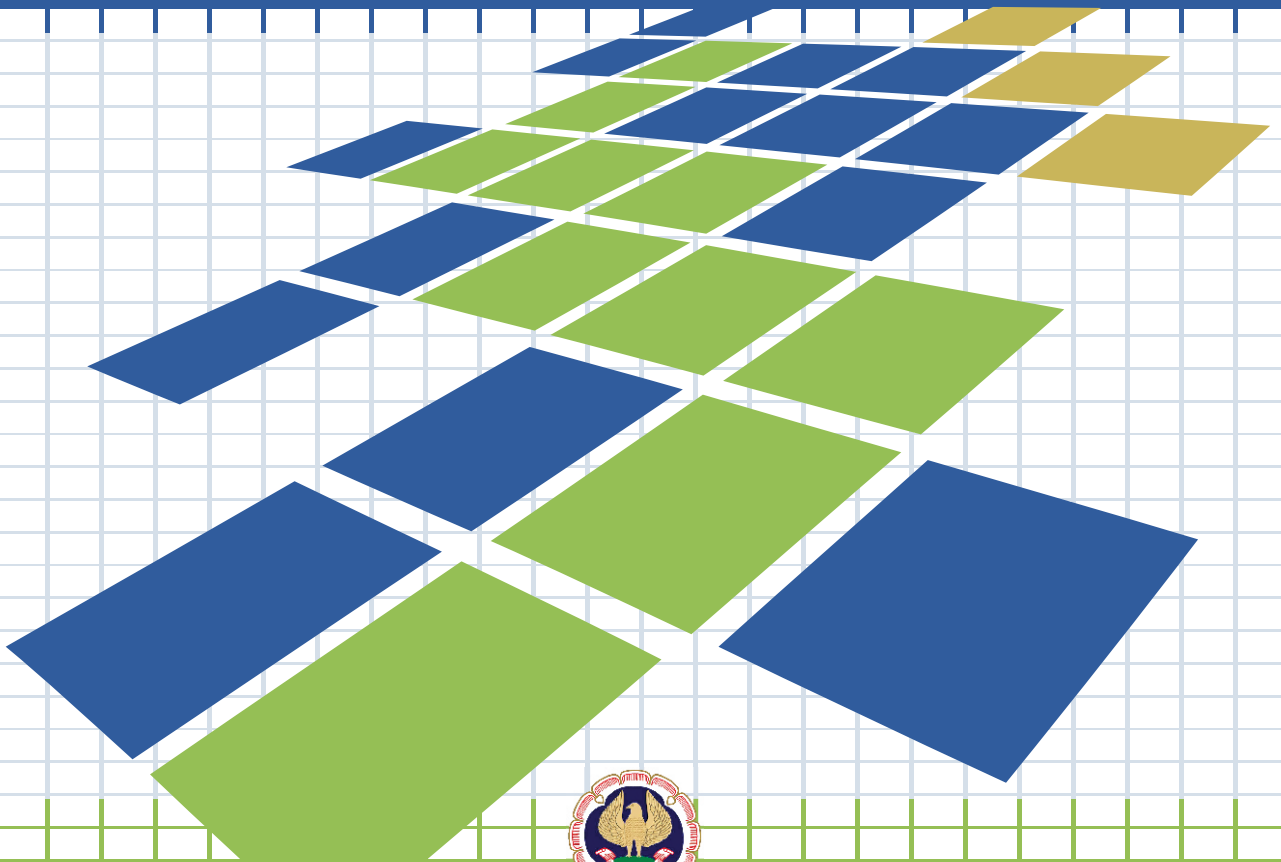


FINAL (NEW) COURSE

# INFORMATION SYSTEMS CONTROL AND AUDIT



Board of Studies  
The Institute of Chartered Accountants of India  
*(Set up by an Act of Parliament)*  
New Delhi

FINAL (NEW) COURSE STUDY MATERIAL

PAPER 6

# Information Systems Control and Audit



BOARD OF STUDIES  
THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

This study material has been prepared by the faculty of the Board of Studies. The objective of the study material is to provide teaching material to the students to enable them to obtain knowledge and skills in the subject. Students should also supplement their study by reference to the recommended text books. In case students need any clarifications or have any suggestions to make for further improvement of the material contained herein, they may write to the Director of Studies.

All care has been taken to provide interpretations and discussions in a manner useful for the students. However, the study material has not been specifically discussed by the Council of the Institute or any of its Committees and the views expressed herein may not be taken to necessarily represent the views of the Council or any of its Committees.

Permission of the Institute is essential for reproduction of any portion of this material.

**© THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA**

All rights reserved. No part of this book may be reproduced, stored in retrieval system, or transmitted, in any form, or by any means, Electronic, Mechanical, photocopying, recording, or otherwise, without prior permission in writing from the publisher.

Revised Edition : March, 2010

Website : [www.icaai.org](http://www.icaai.org)

Department/  
Committee : Board of Studies

E-mail : [bosnoida@icaai.org](mailto:bosnoida@icaai.org)

ISBN No. : 978-81-8441-077-8

Published by : The Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002, India.

Typeset and designed at Board of Studies.

Printed by : Sahitya Bhawan Publications, Hospital Road, Agra- 282 003  
March /2010 /15,000 Copies (Revised)

## PREFACE

This self study material on the subject 'Information Systems Control and Audit' has been prepared for the students of CA Final course.

Today, chartered accountants work in an exciting and complex environment that is constantly changing. Progress in information technology is occurring at an ever-increasing rate. Business organisations are changing their methods of operation and their management structures to meet the demands of an increasingly competitive environment. The economic and legal environment that accountants work in is also changing in unpredictable ways. All of these changes require that today's accounting students be better prepared than ever before to enter the challenging world of the accounting and audit profession.

In today's business world accounting professionals have to interact with computer-based information systems on regular basis. As primary users of information systems in organizations, accountants must participate in their design and understand their operation. Accounting managers must measure and evaluate the performance of information systems. Internal and external auditors must assess the quality of information systems and evaluate the accuracy of information input and output. The major share of the work of accounting consultants is in the design, implementation, evaluation and control of information systems.

The new system of chartered accountancy course recognising the importance of Information Technology has included it as part of the course curriculum both at PCC and Final levels. A paper on Information Systems Control and Audit forming a part of the final syllabus will help the students to understand how to evaluate controls and standards for information systems in an organisational environment. The basic knowledge about Information Technology gained at PCC level is sought to be built up further through this paper.

Chapter 1 of the study material is devoted to the discussion on basic concepts of system and various types of information systems.

Chapter 2 deals with systems development process for an information system. Various stages of systems development life cycle are also discussed. In this chapter, you will also get an idea how computerised business applications are conceived and designed. Various tools and techniques of systems analysis and design and programming are also briefly covered in this Chapter.

Chapter 3 discusses the objectives and functions of various controls for information systems. Understanding of these controls is essential to the Chartered Accountant's ability to audit 'through' the company's information systems.

Chapter 4 discusses various levels of testing for automated controls. Chapter 5 is devoted to the topic of Risk assessment methodologies and their application in information systems.

Chapter 6 outlines Business continuity planning and disaster recovery planning in case such a situation arises in any organization.

Chapter 7 extensively deals with ERP system.

Chapter 8 outlines the framework for Information Systems auditing standards, guidelines and best practices such as BS 7799, COBIT and HIPPA.

Chapter 9 discusses various aspects related with information system security policy, audit policy and audit reporting from practical perspective.

Chapter 10 is devoted to the discussion on Information Technology (Amended) Act, 2008.

At the end of each chapter, a set of self-examination questions is included. You are advised to answer these questions. It will help you in evaluating your understanding of the topic and also generate self-confidence in you. You are advised to leave behind the “spoon-feeding” mentality and digest the subject matter by self-analysis, interpretation and comprehension of various topics under discussion.

Since the level of knowledge required for this paper is “Advanced knowledge”, you are advised to make an early start of the study material and give repeated and intensive readings over a period of time. Information System Control and Audit is very interesting and challenging subject. Try to develop in yourself some interest in this subject and study it for the purpose of learning. You will find that knowledge of this subject will offer you immense opportunities in your career as a chartered accountant.

This study material is developed by Mrs. Indu Arora, Additonal Director of Studies and her team of Faculty members. The Board of Studies acknowledges the contributions made by all these faculty members.

We would welcome suggestions to make this study material more useful to the students. In case of any doubt, students are welcome to write to the Director of Studies, The Institute of Chartered Accountants of India, A-94/4, Sector 58, Noida – 201 301.

# SYLLABUS

---

## PAPER 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

*(One Paper- Three hours - 100 marks)*

**Level of Knowledge:** Advanced knowledge

**Objective:**

To gain application ability of necessary controls, laws and standards in computerized Information system.

**Contents:**

**1. Information Systems Concepts**

General Systems Concepts – Nature and types of systems, nature and types of information, attributes of information.

Management Information System – Role of information within business

Business information systems –various types of information systems – TPC, MIS, DSS, EIS, ES

**2. Systems Development Life Cycle Methodology**

Introduction to SDLC/Basics of SDLC

Requirements analysis and systems design techniques

Strategic considerations : Acquisition decisions and approaches

Software evaluation and selection/development

Alternate development methodologies- RAD, Prototype etc

Hardware evaluation and selection

Systems operations and organization of systems resources

Systems documentation and operation manuals

User procedures, training and end user computing

System testing, assessment, conversion and start-up

Hardware contracts and software licenses

System implementation

Post-implementation review

System maintenance

System safeguards

Brief note on IS Organisation Structure

### 3. Control objectives

#### (a) Information Systems Controls

Need for control

Effect of computers on Internal Audit

Responsibility for control – Management, IT, personnel, auditors

Cost effectiveness of control procedure

Control Objectives for Information and related Technology (COBIT)

#### (b) Information Systems Control Techniques

Control Design: Preventive and detective controls, Computer-dependent control, Audit trails, User Controls (Control balancing, Manual follow up)

Non-computer-dependent (user) controls: Error identification controls, Error investigation controls, Error correction controls, Processing recovery controls

#### (c) Controls over system selection, acquisition/development

Standards and controls applicable to IS development projects

Developed / acquired systems

Vendor evaluation

Structured analysis and design

Role of IS Auditor in System acquisition/selection

#### (d) Controls over system implementation

Acceptance testing methodologies

System conversion methodologies

Post implement review

Monitoring, use and measurement

#### (e) Control over System and program changes

Change management controls

Authorization controls

Documentation controls

Testing and quality controls

Custody, copyright and warranties

Role of IS Auditor in Change Management

- (f) Control over Data integrity, privacy and security
  - Classification of information
  - Logical access controls
  - Physical access controls
  - Environmental controls
  - Security concepts and techniques – Cryptosystems, Data Encryption Standards (DES), Public Key Cryptography & Firewalls
  - Data security and public networks
  - Monitoring and surveillance techniques
  - Data Privacy
  - Unauthorised intrusion, hacking, virus control
  - Role of IS Auditor in Access Control

#### **4. Audit Tests of General and Automated Controls**

- (a) Introduction to basics of testing (reasons for testing);
- (b) Various levels/types of testing such as: (i) Performance testing, (ii) Parallel testing, (iii) Concurrent Audit modules/Embedded audit modules, etc.

#### **5. Risk assessment methodologies and applications:** (a) Meaning of Vulnerabilities, Threats, Risks, Controls, (b) Fraud, error, vandalism, excessive costs, competitive disadvantage, business, interruption, social costs, statutory sanctions, etc. (c) Risk Assessment and Risk Management, (d) Preventive/detective/corrective strategies

#### **6. Business Continuity Planning and Disaster recovery planning:** (a) Fundamentals of BCP/DRP, (b) Threat and risk management, (c) Software and data backup techniques, (d) Alternative processing facility arrangements,(e) Disaster recovery procedural plan, (f) Integration with departmental plans, testing and documentation, (g) Insurance

#### **7. An over view of Enterprise Resource Planning (ERP)**

#### **8. Information Systems Auditing Standards, guidelines, best practices (BS7799, HIPPA, CMM etc.)**

#### **9. Drafting of IS Security Policy, Audit Policy, IS Audit Reporting - a practical perspective**

#### **10. Information Technology (Amended) Act, 2008**



# CONTENTS

## CHAPTER 1 – INFORMATION SYSTEMS CONCEPTS

1.1	Introduction .....	1.1
1.2	Definition of a system.....	1.1
1.3	Types of System .....	1.2
1.4	General Model of a System .....	1.6
1.5	System Environment .....	1.6
1.6	Information .....	1.11
1.7	Information System and its role in Management.....	1.14
1.8	Types of Information Systems at different levels.....	1.19
1.9	Operations Support Systems (OSS) .....	1.20
1.10	Management Support Systems (MSS) .....	1.34
1.11	Office Automation Systems (OAS).....	1.47

## CHAPTER 2 – SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY

2.1	Introduction .....	2.1
2.2	Systems Development Process .....	2.1
2.3	Systems Development Methodology .....	2.4
2.4	System Development Life Cycle (SDLC).....	2.16
2.5	The Preliminary Investigation .....	2.18
2.6	System Requirement Analysis .....	2.25
2.7	Systems Design .....	2.42
2.8	System Acquisition.....	2.48
2.9	Development : Programming Techniques and Languages .....	2.51
2.10	System Testing .....	2.53
2.11	Systems Implementation .....	2.57
2.12	Post Implementation Review and System Maintenance.....	2.60
2.13	Operation Manuals.....	2.63
2.14	Organizational Structure of IT Department.....	2.64

## **CHAPTER 3 – CONTROL OBJECTIVES**

3.1	Information Systems Controls.....	3.1
3.2	Need for Control and Audit of Information Systems.....	3.1
3.3	Effect of Computers on Internal Controls .....	3.3
3.4	Effect of Computers on Audit.....	3.5
3.5	Responsibility for Controls .....	3.7
3.6	The IS Audit Process .....	3.9
3.7	Information Systems Control Techniques.....	3.18
3.8	User Controls.....	3.30
3.9	System Development and Acquisition Controls .....	3.38
3.10	Control Over System and Program Changes.....	3.45
3.11	Quality Control.....	3.52
3.12	Controls Over System Implementation.....	3.57
3.13	System Maintenance.....	3.62
3.14	Post Implementation Review .....	3.65
3.15	Control Over Data Integrity, Privacy and Security .....	3.68
3.16	Security Concepts and Techniques .....	3.73
3.17	Data Security and Public Networks .....	3.76
3.18	Unauthorized Intrusion.....	3.80
3.19	Hacking .....	3.81
3.20	Data Privacy .....	3.85
3.21	Controlling Against Viruses and Other Destructive Programs .....	3.86
3.22	Logical Access Controls .....	3.89
3.23	Physical Access Controls.....	3.104
3.24	Environmental Controls .....	3.115

## **CHAPTER 4 : TESTING – GENERAL AND AUTOMATED CONTROLS**

4.1	Introduction to basics of testing (Reasons for testing).....	4.1
4.2	Software Testing Fundamentals .....	4.1
4.3	Test Plan .....	4.3

4.4	Test Plan Outline .....	4.5
4.5	Types of software testing .....	4.6
4.6	Black box testing .....	4.7
4.7	White box testing .....	4.8
4.8	Unit testing .....	4.10
4.9	Requirement testing .....	4.10
4.10	Regression testing .....	4.11
4.11	Error handling testing.....	4.12
4.12	Manual support testing.....	4.13
4.13	Inter system testing.....	4.13
4.14	Control testing .....	4.14
4.15	Parallel testing.....	4.15
4.16	Volume testing .....	4.15
4.17	Stress testing.....	4.16
4.18	Performance testing.....	4.16
4.19	Concurrent or continuous audit and embedded audit modules.....	4.16
4.20	Hardware testing.....	4.20
4.21	Review of hardware .....	4.21
4.22	Operating system review .....	4.23
4.23	Reviewing the network .....	4.25

## **CHAPTER 5 – RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS**

5.1	Introduction .....	5.1
5.2	Risk, Threat, Exposure and Vulnerability .....	5.1
5.3	Threats to the computerized environment.....	5.3
5.4	Threats due to cyber crimes .....	5.4
5.5	Risk Assessment .....	5.5
5.6	Risk Management .....	5.7
5.7	Risk Identification .....	5.9
5.8	Risk ranking.....	5.12

5.9	Risk mitigation .....	5.14
5.10	Risk and controls .....	5.16
5.11	Risk analysis and assessment form .....	5.16

**CHAPTER 6 – BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING**

6.0	Introduction .....	6.1
6.1	Business Continuity Planning .....	6.1
6.2	Developing a Business Continuity Plan.....	6.3
6.3	Types of Plans .....	6.7
6.4	Test Plan .....	6.9
6.5	Threats and Risk Management .....	6.9
6.6	Software and Data Back-up Techniques .....	6.12
6.7	Alternate Processing Facility Arrangements.....	6.13
6.8	Back-Up Redundancy.....	6.14
6.9	Disaster Recovery Procedural Plan .....	6.17
6.10	Insurance.....	6.18
6.11	Testing Methodology and Checklist .....	6.20
6.12	Audit Tools and Techniques .....	6.23
6.13	Audit of the Disaster Recovery/Business Resumption Plan .....	6.24

**CHAPTER 7 – AN OVERVIEW OF ENTERPRISE RESOURCE PLANNING (ERP)**

7.0	Introduction .....	7.1
7.1	ERP-Definition .....	7.2
7.2	Business Process Reengineering (BPR) .....	7.7
7.3	ERP Implementation .....	7.11
7.4	Post Implementation .....	7.17
7.5	Risk and Governance Issues in an ERP .....	7.18
7.6	How does EPR fit with E-Commerce .....	7.20
7.7	Life after Implementation.....	7.20
7.8	Sample List of ERP Vendors .....	7.22

7.9	ERP Software Package (SAP).....	7.23
7.10	Case Study.....	7.40

**CHAPTER 8 – INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES**

8.0	Introduction .....	8.1
8.1	IS Audit Standards.....	8.2
8.2	AAS-29 Auditing and Assurance Standard on Auditing in a Computer Information Systems Environment .....	8.2
8.3	BS 7799.....	8.3
8.4	CMM- Capability Maturity Model.....	8.12
8.5	COBIT – IT Governance Model.....	8.17
8.6	COCO.....	8.22
8.7	ITIL (IT Infrastructure Library) .....	8.23
8.8	Systrust and Webtrust.....	8.26
8.9	HIPAA .....	8.27
8.10	SAS 70 – Statement of Auditing Standards for Service Organisations .....	8.30

**CHAPTER 9: DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING- A PRACTICAL PERSPECTIVE**

9.0	Introduction .....	9.1
9.1	Important of Information System Security .....	9.2
9.2	Information System Security.....	9.3
9.3	Protecting Computer-held Information Systems .....	9.5
9.4	Information Security Policy.....	9.7
9.5	Types of Information Security Policies and their Hierarchy.....	9.8
9.6	Audit Policy .....	9.15
9.7	Audit Working Papers and Documentation.....	9.19
9.8	IS Audit Reports .....	9.21
	Annexure – I : Sample IS Security Policy.....	9.24

## **CHAPTER 10 – INFORMATION TECHNOLOGY (AMENDED) ACT, 2008**

10.0	Brief History .....	10.1
10.1	The IT Act 2000 and its Objectives .....	10.3
10.2	Preliminary [Chapter I] .....	10.3
10.3	Digital Signature And Electronic Signature (Amended Vide ITAA 2008) Chapter-II] .....	10.8
10.4	Electronic Governance [Chapter III].....	10.9
10.5	Attribution, Acknowledgment And Dispatch Of Electronic Records [Chapter IV] .....	10.14
10.6	Secure Electronic Records And Secure Electronic Signatures [Chapter V] .....	10.16
10.7	Regulation Of Certifying Authorities (Chapter VI).....	10.17
10.8	Electronic Signature Certificates [Chapter VII].....	10.23
10.9	Duties Of Subscribers [Chapter VIII].....	10.26
10.10	Penalties And Adjudication [Chapter IX] .....	10.28
10.11	The Cyber Appellate Tribunal (Amended Vide ITAA-2008) [Chapter X].....	10.32
10.12	Offences [Chapter XI] .....	10.38
10.13	Intermediaries Not To Be Liable In Certain Cases (Substituted Vide ITAA-2008) [Chapter XII] .....	10.50
10.14	Miscellaneous [Chapter XIII] .....	10.51

# INFORMATION SYSTEM CONCEPTS

---

## LEARNING OBJECTIVES :

- To introduce the general concepts of systems, their objective, their elements and their classification.
- To explain the concept of information, its characteristics and its role in Information systems.
- To explain different types of Computer Based Information Systems like DSS, MIS, EIS etc.
- To explain different types of Office Automation Systems.

## 1.1 INTRODUCTION

The term system is in common parlance. People talk of transport system, educational system, solar system and many others. System concepts provide a framework for many organizational phenomenon including features of information system.

## 1.2 DEFINITION OF A SYSTEM

The term system may be defined as an orderly arrangement of a set of interrelated and interdependent elements that operate collectively to accomplish some common purpose or goal. For example - Human body is a system, consisting of various parts such as head, heart, hands, legs and so on. The various body parts are related by means of connecting networks of blood vessels and nerves and the system has a main goal of "living". Thus, a system can be described by specifying its parts, the way in which they are related, and the goals which they are expected to achieve. A business is also a system where economic resources such as people, money, material, machines, etc are transformed by various organizational processes (such as production, marketing, finance etc.) into goods and services. A computer based information system is also a system which is a collection of people, hardware, software, data and procedures that interact to provide timely information to authorized people who need it.

## 1.2 Information Systems Control and Audit

### 1.3 TYPES OF SYSTEM

As shown in Fig. 1.3.1, we can distinguish systems on the basis of following parameters:

- (i) Elements
- (ii) Interactive Behavior
- (iii) Degree of Human Intervention
- (iv) Working / Output

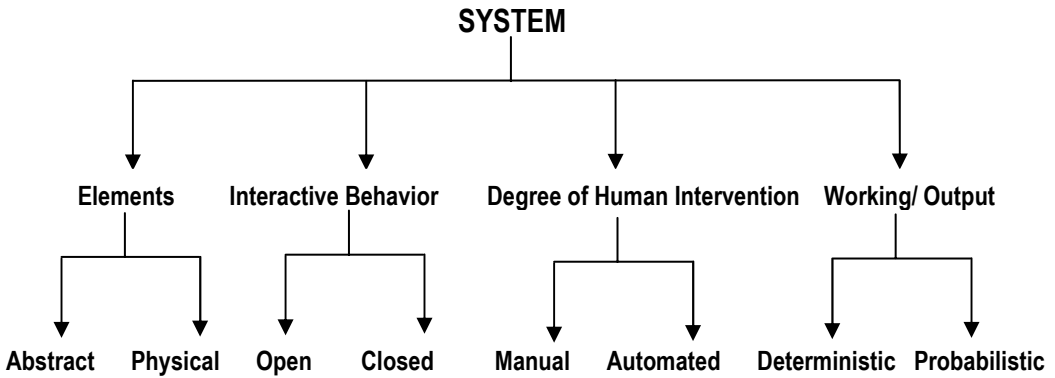


Fig. 1.3.1 : Classification Chart of System

#### 1.3.1 According to Elements

- (i) **Abstract System** : Abstract System also known as Conceptual System or Model can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God.
- (ii) **Physical System** : A physical system is a set of tangible elements which operate together to accomplish an objective. Some of its examples are shown in Table 1.3.1.

Physical System	Description
Circulatory system	The heart and blood vessels which move blood through the body.
Transportation system	The personnel, machines, and organizations which transport goods.
Weapons system	The equipment, procedures, and personnel which make it possible to use a weapon.
School system	The buildings, teachers, administrators, and textbooks that function together to provide education to students.
Computer system	The equipment which function, together to accomplish computer processing.

Table 1.3.1 : Examples of Physical System



The examples illustrate that a system is not a randomly assembled set of elements; it consists of elements, which can be identified as belonging together because of a common purpose, goal, or objective. Physical systems are more than conceptual construct; they display activity or behavior. The parts interact to achieve an objective.

### 1.3.2 According to Interactive Behavior

A system may be composed of a number of components that work together in a cascade to achieve a goal for which the system is designed. All systems work in a specific environment and based on how they perform within an environment, systems can be categorized in two classes:

- (i) **Open System** : A system that interacts freely with its environment by taking input and returning output is termed as an **Open System**. With change of environment, an open system also changes to match itself with the environment. For example, the education system or any business process system will quickly change when the environment changes. To do this, an open system will interact with elements that exist and influence from outside the boundary of the system.

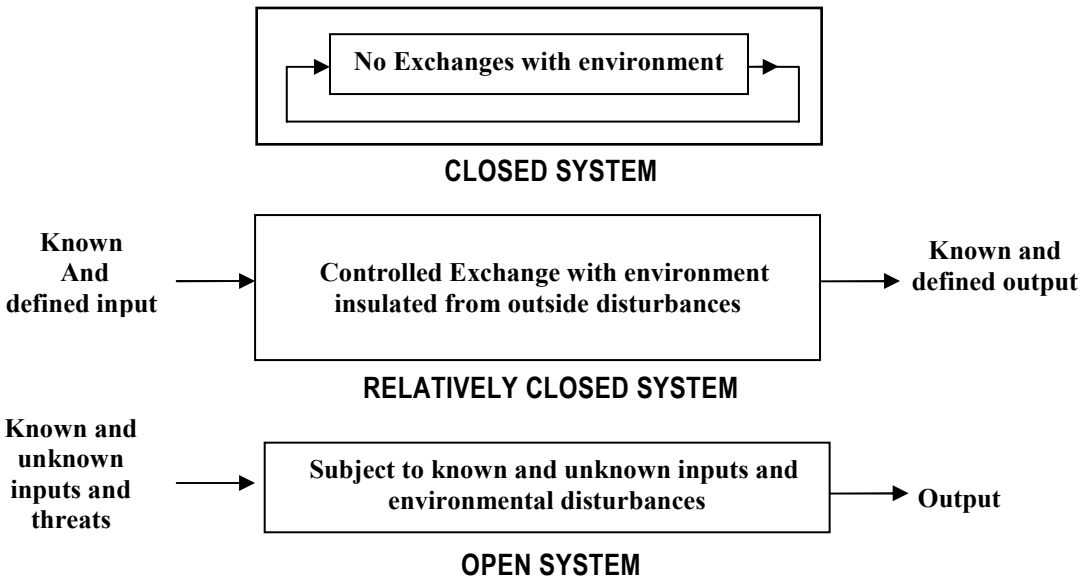
Information systems are open systems because they accept inputs from environment and sends outputs to environment. Also with change of environmental conditions, they adapt themselves to match the changes.

- (ii) **Closed System** : A system that does not interact with the environment nor changes with the change in environment is termed as a **Closed System**. Such systems are insulated from the environment and are not affected with the changes in environment. Closed systems are rare in business area but often available in physical systems that we use in our day to work. For example, consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation. Such closed systems will finally run down or become disorganized. This movement to disorder is termed on increase in entropy.

Organizations are considered to be relatively open systems as they continuously interact with the external environment, by processes or transformation of inputs into useful output. However, organizations behave as a relatively closed system in certain respects so as to preserve their identity and autonomy. They may ignore many opportunities so as to maintain their core-competence.

Organizations perform several operations on these inputs (consisting of finance, physical and mental labor, and raw material) and process out products or services. The process of exchange generates some surplus, in the form of profit, goodwill experience and so on, which can be retained in the organization and can be used for further input output process. Organizations are dependent upon their external environment for the inputs required by them and for disposing of their outputs in a mutually beneficial manner. Fig. 1.3.2 illustrates open system vs closed system.

## 1.4 Information Systems Control and Audit



**Fig. 1.3.2 : Closed System vs Open System**

**Entropy :** Entropy is the quantitative measure of disorder in a system. Systems can run down and decay or can become disordered or disorganized. Presenting or offsetting an increase in entropy requires inputs of matter and energy to repair, replenish and maintain the system. This maintenance input is termed as **Negative Entropy**. Open systems require more negative entropy than relatively closed systems for keeping at a steady state.

In general, the life cycle of a closed system is much shorter compared to that of an open system because it decays faster for not having any input/ interaction from environment.

Open systems require more negative entropy than relatively closed systems for keeping at a steady state of organization and operation, but all the systems described in the text require it. Examples of system maintenance through negative entropy by inputs of matter and energy are shown in Table 1.3.2.

System	Manifestations of entropy	Negative Entropy
Automobile	Engine won't start tyres too thin.	Tune up engine, Replace tires.
Computer program	User dissatisfaction with features and errors.	Program enhancements.
Computer data files	Errors and omissions in data field. Not all relevant entities included.	Review and correct procedures procedure to identify omission and obtain data.

**Table 1.3.2 : Systems and their Entropies**

### 1.3.3 According to Degree of Human Intervention

- (i) **Manual Systems** : Manual Systems are the systems where data collection, manipulation, maintenance and final reporting are carried out absolutely by human efforts.
- (ii) **Automated Systems** : Automated Systems are the systems where computers or microprocessors are used to carry out all the tasks mentioned above. However, none of the business system is 100% automated; rather, to some extent, it depends on manual intervention, may be in a negligible way.

Computers made it possible to carry out processing which would have been either too difficult or too much time-consuming or even impossible to do manually. A system may be even 100% manual. In earlier days, all accounting procedures and transactions, production details or sales data used to be maintained in different ledgers that were created by human efforts only and all these were manual systems. With introduction of computers and complexity in business procedures, these manual jobs were passed to computers in a major way and now a business system inherently involves a close man-machine interaction. The reasons for using computer in business area are as follows:

- Handling huge volume of data that is not manageable by human efforts.
- Storing enormous volume of data for indefinite period without any decay.
- Quick and accurate processing of data to match the competitive environment.
- Quick retrieval of information on query.
- Quick and efficient transportation of data/information to distant places almost at no cost.
- Availability of software tools for quick decision making in a complex situation.

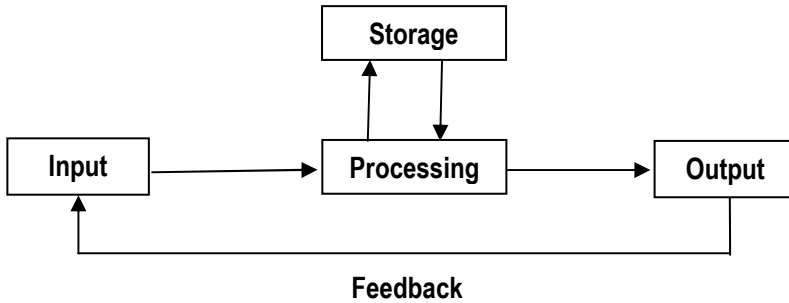
### 1.3.4 According to Working/Output

- (i) **Deterministic System** : A deterministic system operates in a predictable manner wherein the interaction among the parts is known with certainty. If one has a description of the state of the system at a given point in time plus a description of its operation, the next state of the system may be given exactly, without error. An example is a correct computer program, which performs exactly according to a set of instructions.
- (ii) **Probabilistic System** : The probabilistic system can be described in terms of probable behavior, but a certain degree of error is always attached to the prediction of what the system will do. An inventory system is an example of a probabilistic system. The average demand, average time for replenishment, etc, may be defined, but the exact value at any given time is not known. Another example is a set of instructions given to a human who, for a variety of reasons, may not follow the instructions exactly as given.

## 1.6 Information Systems Control and Audit

### 1.4 GENERAL MODEL OF A SYSTEM

A general model of a physical system is input, process and output. This is, of course, very simplified because a system may have several inputs and outputs as shown in Fig. 1.4.1 :



**Fig. 1.4.1 : General Model of a System**

A System may have many inputs and outputs.

- **Input** is the data flowing into the system from outside. For example : A newspaper takes a news feed from a news wire service such as Reuters.
- **Processing** is the action of manipulating the input into a more useful form. For example : The newspaper takes the pure text obtained from the news wire service and creates front page layout using pictures and formatted text.
- **Output** is the information flowing out of a system. For example : The raw news wire information is viewed on your website as a story, all nicely formatted in the company style.
- **Storage** is the means of holding information for use at a later date.
- **Feedback** occurs when the outcome has an influence on the input.

### 1.5 SYSTEM ENVIRONMENT

The external world which is outside the system boundary is known as **System Environment**.

#### 1.5.1 System Boundary

All systems function within some sort of environment, which is a collection of elements. These elements surround the system and often interact with it. For any given problem, there are many types of systems and many types of environments. Thus, it is important to be clear about what constitutes the system and the environment of interest.

For example, a physiologist looking at human system may be interested in studying the entire human body as a system, and not just a part of it (such as the central nervous system only). If the entire human body is the system of interest, the physiologist is likely to define the environment more broadly than he might if the focus was on just the central nervous system.

The features that define and delineate a system form its boundary. The system is inside the boundary; the environment is outside the boundary. In some cases, it is fairly simple to define what is part of the system and what is not; in other cases, the person studying the system may arbitrarily define the boundaries. Some examples of boundaries are discussed in Table 1.5.1.

System	Boundary
Human	Skin, hair, nails, and all parts contained inside form the system; all things outside are environment.
Automobile	The automobile body plus tires and all parts contained within form the system.
Production	Production machines, production inventory of work in process, production employees, production procedures, etc. form the system. The rest of the company is in the environment.

Table 1.5.1 : Examples of Systems and their Boundaries

1.5.2 Subsystem

A subsystem is a part of a larger system. Each system is composed of subsystems, which in turn are made up of other subsystems, each sub-system being delineated by its boundaries.

The interconnections and interactions between the subsystems are termed **Interfaces**. Interfaces occur at the boundary and take the form of inputs and outputs. Fig. 1.5.1 shows examples of subsystems and interfaces at boundaries.

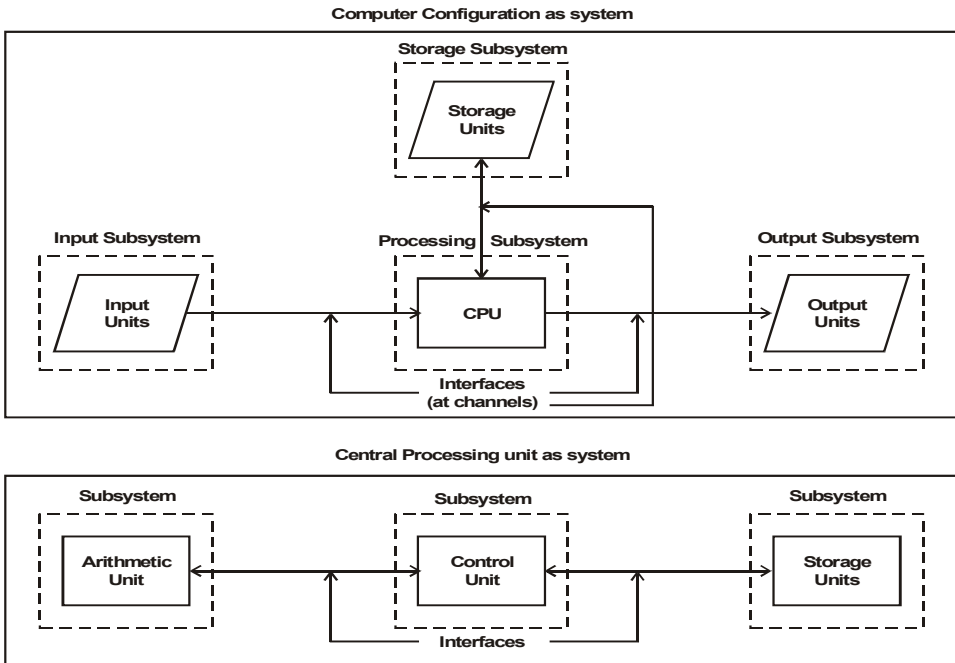


Fig. 1.5.1 : Components of a Computer System

## 1.8 Information Systems Control and Audit

### 1.5.3 Characteristics of Subsystems

The use of subsystems as building blocks is basic to analysis and development. This requires an understanding of the principles, which dictate how systems are built from subsystems.

- (i) **Decomposition** : A complex system is difficult to comprehend when considered as a whole. Therefore the system is decomposed or factored into subsystems. The boundaries and interfaces are defined, so that the sum of the subsystems constitutes the entire system. This process of decomposition is continued with subsystems divided into smaller subsystems until the smallest subsystems are of manageable size. The subsystems resulting from this process generally form hierarchical structures (Fig. 1.5.2). In the hierarchy, a subsystem is one element of supra-system (the system above it).

Decomposition into subsystems is used to analyze an existing system and to design and implement a new system. In both cases, the investigator or designer must decide how to factor, i.e., where to draw the boundaries. The decisions will depend on the objectives of the decomposition and also on individual differences among designers, the latter should be minimized.

An example of decomposition is the factoring of an information processing system into subsystems. One approach to decomposition might proceed as follows:

1. Information system divided into subsystem such as :

- a. Sales and order entry
- b. Inventory
- c. Production
- d. Personnel and payroll
- e. Purchasing
- f. Accounting and control
- g. Planning
- h. Environmental intelligence

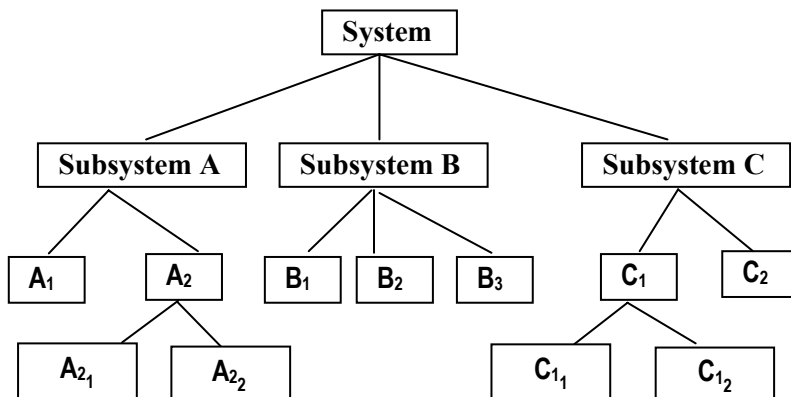
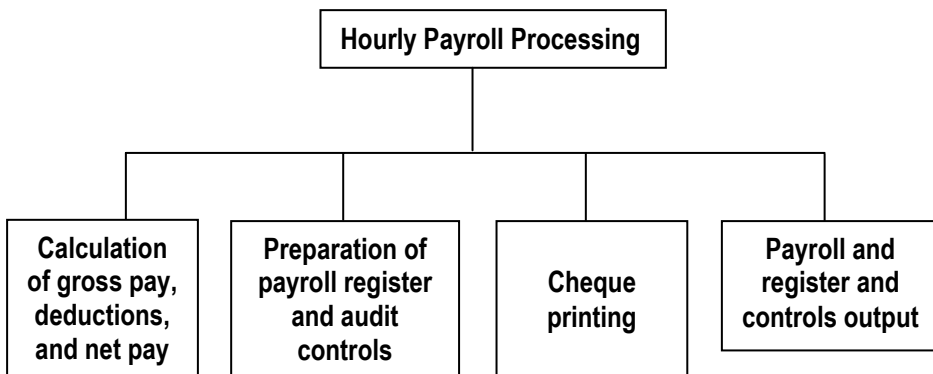


Fig. 1.5.2 : Hierarchical Relations of Subsystems

2. Each subsystem is divided further into subsystems. For example, the personnel and payroll subsystem might be divided into the following smaller subsystems:
  - a. Creation and update of personnel pay-roll records
  - b. Personnel reports
  - c. Payroll data entry and validation
  - d. Hourly payroll processing
  - e. Salaried payroll processing
  - f. Payroll reports for management
  - g. Payroll reports for government
3. If the task is to design and program a new system, the subsystems (major applications) defined in (2) might be further subdivided into smaller subsystems or modules. For example, the hourly payroll processing subsystem might be factored into modules for the calculation of deductions and net pay, payroll register and audit controls preparation, cheque printing, and register and controls output (Fig. 1.5.3).



**Fig. 1.5.3 : Hourly Payroll Processing Subsystem**

- (ii) **Simplification** : Simplification is defined as the process of organizing subsystems so as to reduce the number of interconnections, which is a potential interface for communication among subsystems. The number of interconnections if all the subsystems interact is in general  $\frac{1}{2}n(n-1)$ , where  $n$  is the number of subsystems.
- (iii) **Decoupling** : If two different subsystems are connected very tightly, very close coordination between them is required. For example, if the raw material is put directly into production the moment it arrives at the factory, the raw materials system can be said to be tightly couple. Under these conditions, raw material delivery (input to production system and output from raw material system) must be precisely timed in order to avoid delays in production or to prevent new material from arriving too soon with no place to be stored.

## 1.10 Information Systems Control and Audit

- **Inventories, buffer, or waiting lines** : In the example of the raw material subsystem and production subsystem, a raw material inventory allows the two subsystems to operate somewhat independently (in the short run). Data buffers are used in some computer systems and some communications systems to compensate for different rates of input and output of data.
- **Slack and Flexible resources** : When the output of one subsystem is the input to another, the existence of slack resources allows subsystems to be somewhat independent and yet allows each to respond to the demands of the other subsystem. For example, most data processing systems can provide an extra report or extra analysis because they have slack resources. The ability of an organization to respond can be employed for a variety of purposes. An information systems organization that uses the concept of a combination of systems analyst - programming that an organization with the same number of personnel that uses systems analysts and programming than an organization with the same number of personnel that uses systems analysts only for analysis and design and programmers only for programming.
- **Standards** : Standard allow a subsystem to plan and organize with reduced need to communicate with other subsystems. If, for example, the production department wishes to design a data processing module involving finished goods and a standard product code is used throughout the organization, there is no need to communicate negotiate with other departments about the codes to be used. A standard decoupling mechanisms to reduce to reduce need for communication and close connection among database description maintained by the data administrator (the data dictionary) allows use of the database without tedious and time-consuming checking with other subsystems also using the database.

### 1.5.3 Supra-System

A **Supra-System** refers to the entity formed by a system and other equivalent systems with which it interacts. For example, an organization may be subdivided into numerous functional areas such as marketing, finance, manufacturing, research and development, and so on. Each of these functional areas can be viewed as a subsystem of a larger organizational system because each could be considered to be a system in and of itself. For example, marketing may be viewed as a system that consists of elements such as market research, advertising, sales, and so on. Collectively, these elements in the marketing area may be viewed as making up the marketing Supra-System. Similarly the various functional areas (subsystems) of an organization are elements in the same supra- system within the organization.

### 1.5.4 System Stress and System Change

Systems whether living or artificial systems like organizational systems, information systems, change because they undergo stress. A stress is a force transmitted by a system's supra-system that causes a system to change, so that the supra-system can better achieve its goals. In trying to accommodate the stress, the system may impose stress on its subsystems and so on.



When a supra-system exerts stress on a system, the system will change to accommodate the stress, or it will become pathological; that is, it will decay and terminate.

A Supra-system enforces compliance by the system through its control over the supply of resources and information input to the system. If the system does not accommodate the stress, the supra-system decreases or terminates the supply of matter energy and information input to the system. If the system does not accommodate the stress, the supra-system decreases or terminates the supply of matter energy and information input.

Systems accommodate stress through a change in the form; there can be structural changes or process changes. For example - a computer system under stress for more share-ability of data may be changed through the installation of terminals in remote locations - a structural change. Demands for greater efficiency may be met by changing the way in which it sorts the data - a process change.

## 1.6 INFORMATION

Information is data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as - "Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision". For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel. This information is of vital importance to a marketing manager who is trying to plan for future sales.

The term "data" and 'information' are often used interchangeably. However, the relation of data to information is that of raw material to finished product. A data processing system processes data to generate information on which business decisions are based. Therefore, the quality of information determines the quality of action or decision. The management plays the part of converting the information into action through the familiar process of decision-making. Therefore, Information plays a vital role in the survival of a business.

### 1.6.1 Attributes of Information

Some of the important attributes of useful and effective information are as follows :

- (i) **Availability** : Availability or Timeliness is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.
- (ii) **Purpose** : Information must have purposes at the time it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.

## 1.12 Information Systems Control and Audit

It helps in creating new concepts, identifying problems, solving problems, decision making, planning, initiating, and controlling. These are just some of the purposes to which information is directed to human activity in business organizations.

- (iii) **Mode and format** : The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are either visual, verbal or in written form.

Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching. Therefore, all the statistical rules of compiling statistical tables and presenting information by means of diagram, graphs, curves, etc., should be considered. Format of information dissemination is a matter of imagination and perception. It should be simple, relevant and should highlight important points but should not be too cluttered up.

- (iv) **Decay** : Value of information usually decays with time and usage and so it should be refreshed from time to time. For example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the state. Similarly, in highly fluctuating share market a broker is always interested about the latest information of a particular stock/s.
- (v) **Rate** : The rate of transmission/reception of information may be represented by the time required to understand a particular situation. A useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive, Quantitatively, the rate for humans may be measure by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines the rate may be based on the number of bits of information per character (sign) per unit of time.
- (vi) **Frequency** : The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.
- (vii) **Completeness** : The information should be as complete as possible. For example - Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.
- (viii) **Reliability** : It is just not authenticity or correctness of information; rather technically it is a measure of failure or success of using information for decision-making. If an information leads to correct decision on many occasions, we say the information is reliable.
- (ix) **Validity** : It measures the closeness of the information to the purpose which it purports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity. The measure suiting the organization may have to be carefully selected or evolved.

- (x) **Quality** : Quality refers to the correctness of information. Information is likely to be spoiled by personal bias. For example, an over-optimistic salesman may give rather too high estimates of the sales. This problem, however, can be circumvented by maintaining records of salesman's estimates and actual sales and deflating or inflating the estimates in the light of this.
- (xi) **Transparency** : If information does not reveal directly what we want to know for decision-making, it is not transparent. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- (xii) **Value of information** : It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.
- (xiii) **Adequacy** : To be useful, an information must be adequate so that the desired actions can be initiated. Required information should flow on different directions within the organization and to and from its environment. Further, the type of information that flows within the organization or across, it should have adequate and relevant contents.

### 1.6.2 Types of Information

Information, broadly, can be divided into two different types : **Internal Information** and **External Information** in the context of business organizations.

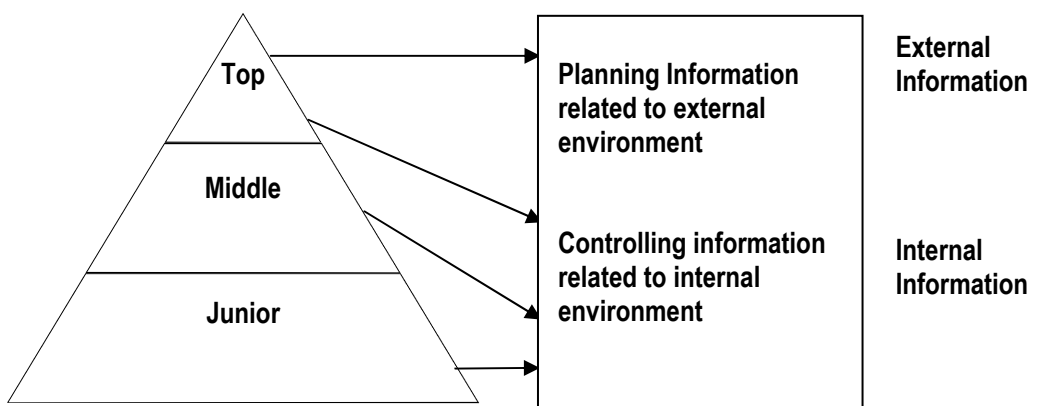


Fig. 1.6.1 : External and Internal Information

**Internal information** : The internal information can be defined as an information that has been generated from the operations of the organization at various functional areas. The internal information gets processed and summarized from junior to top most level of

## 1.14 Information Systems Control and Audit

management. The internal information always pertains to the various operational units of the organization. Examples of internal information would be production figures, sales figures, information about personnel, accounts, material etc.

**External information :** The external information is collected from the external environment of the business organization. External information is considered to affect the organizational performance from outside the organization.

For example - Information such as Govt. policies, competition, economic status etc. are considered to be external information. Access to internal and external information by different levels of management is shown in Fig. 1.6.1.

## 1.7 INFORMATION SYSTEM AND ITS ROLE IN MANAGEMENT

An Information System can be considered as an arrangement of a number of elements that provides effective information for decision-making and/or control of some functionalities of an organization. Information is an entity that reduces uncertainty about an event or situation. For example, correct information about demand of products in the market will reduce the uncertainty of production schedule. Enterprises use information system to reduce costs, control wastes or generate revenue. Computer Based Information System are complementary networks of hardware/software that people and organizations use to collect, filter, process, create and distribute data. Hence onwards, the chapter focuses only to CBIS.

In modern business perspective, the information system has far reaching effects for smooth and efficient operations. Some of important implications of information system in business are as follows:

- Information system helps managers in effective decision-making to achieve the organizational goal.
- Based on well-designed Information system, an organization will gain edge in the competitive environment.
- Information systems help take right decision at the right time.
- Innovative ideas for solving critical problems may come out from good Information system.
- Knowledge gathered through Information system may be utilized by managers in unusual situations.
- Information system is viewed as a process, it can be integrated to formulate a strategy of action or operation.

### 1.7.1 Factors on which Information Requirements depend

The factors on which information requirements of executives depend are as follows :

1. Operational function
2. Type of decision making
3. Level of management activity

**(1) Operational function :** The grouping or clustering of several functional units on the basis of related activities into a sub-systems is termed as **Operational function**. For example, in a business enterprise, marketing is an operational function, as it is the clustering of several functional units like market research, advertising, sales analysis and so on. Likewise, production finance, personnel etc. can all be considered as operational functions.

Information requirement depends upon operational function. The information requirement of different operational functions vary not only in content but also in characteristics. In fact, the content of information depends upon the activities performed under an operational function. For example, in the case of production, the information required may be about the production targets to be achieved, resources available and so on. Whereas in the case of marketing functions, the content of information may be about the consumer behavior, new product impact in the market etc.

**(2) Type of decision making :** Organizational decisions can be categorized as **Programmed and Non-programmed ones**.

**Programmed Decisions :** Programmed decisions or structured decisions refer to decisions made on problems and situations by reference to a predetermined set of precedents, procedures, techniques and rules. These are well-structured in advance and are time-tested for their validity. As a problem or issue for decision-making emerges, the relevant pre-decided rule or procedure is applied to arrive at the decision. For example, in many organizations, there is a set procedure for receipt of materials, payment of bills, employment of clerical personnel, release of budgeted funds, and so on.

Programmed decisions are made with respect to familiar, routine, recurring problems which are amenable for structured solution by application of known and well-defined operating procedures and processes. Not much judgment and discretion is needed in finding solutions to such problems. It is a matter of identifying the problem and applying the rule, thus simplifying the process of decision making.

**Non-programmed Decisions :** Non-programmed decisions or unstructured decisions are those which are made on situations and problems which are novel and non-repetitive and about which not much knowledge and information are available. They are non-programmed in the sense that they are made not by reference to any pre-determined guidelines, standard operating procedures, precedents and rules but by application of managerial intelligence, experience, judgment and vision to tackling problems and situations, which arise infrequently and about which not much is known. There is no simple or single best way of making

## 1.16 Information Systems Control and Audit

decisions on unstructured problems, which change their character from time to time, which are surrounded by uncertainty and enigma and which defy quick understanding. Solutions and decisions on them tend to be unique or unusual. For example - problems such as a sudden major change in government policy badly affecting a particular industry, the departure of a top level key executive, drastic decline in demand for a particular high profile product, competitive rivalry from a previously little known manufacturer etc. do not have ready-made solutions.

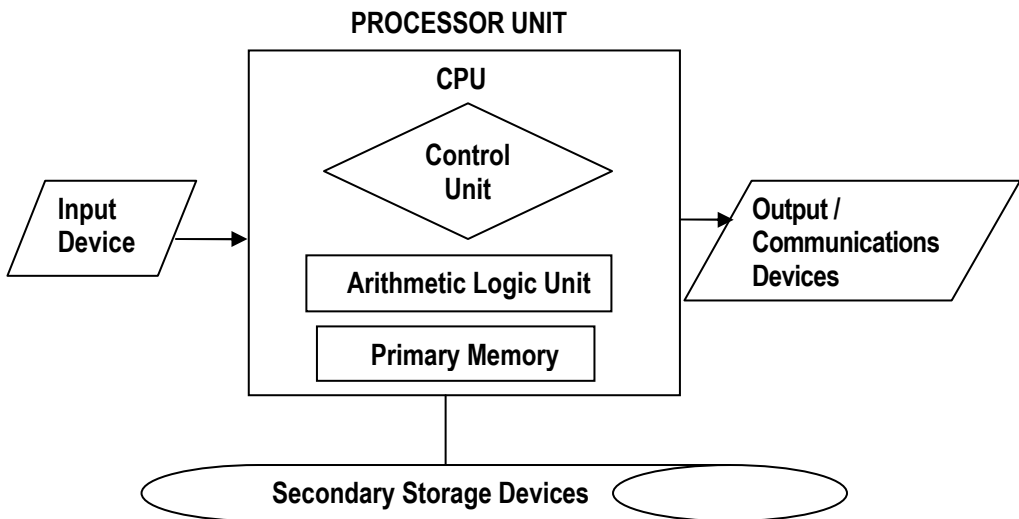
**(3) Level of management activity :** Different levels of management activities in management planning and control hierarchy are Strategic level, Tactical level and Operational level.

- **Strategic Level or Top level :** Strategic level management is concerned with the developing of organizational mission, objectives and strategies. Decisions made at this level of organization in order to handle problems critical to the survival and success of the organization are called **Strategic Decisions**. They have a vital impact on the direction and functioning of the organization. For example - decisions on plant location, introduction of new products, making major new fund-raising and investment operations, adoption of new technology, acquisition of outside enterprises and so on go into making strategic decisions.
- **Tactical Level or Middle level :** Tactical level lies in middle of managerial hierarchy where managers plan, organize, lead and control the activities of other managers. Decisions made at this level called the **Tactical decisions** (which are also called operational decisions) are made to implement strategic decisions. A single strategic decision calls for a series of tactical decisions, which are of a relatively structured nature. Tactical decisions are relatively short, step-like spot solutions to breakdown strategic decisions into implemental packages. Tactical decisions are specific and functional; made in a relatively closed setting; more easily available and digestible; and less surrounded by uncertainty and complexity.
- **Operational level or Supervisory Level :** This is the lowest level in managerial hierarchy wherein the managers coordinate the work of others who are not themselves managers. They ensure that specific tasks are carried out effectively and efficiently.

### 1.7.2 Components of Computer Based Information System

A **Computer-based Information System (CBIS)** is an information system in which the computer plays a major role. Such a system consists of the following elements as shown in Fig 1.7.1.

**Hardware :** The term hardware refers to machinery including the computer itself, which is often referred as Central Processing Unit (CPU) and all of its support equipment. Among the support equipment are input and output devices, storage devices, and communications devices.



**Fig 1.7.1 : The Hardware Components of CBIS**

**Software** : The term software refers to the computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the CBIS to function in ways that produce useful information from data.

**Data** : Data are facts that are used by programs to produce useful information. Like programs, data are generally stored in machine-readable form on disk or tape until the computer needs them.

**Procedures** : Procedures are the policies that govern the operation of a computer system. For instance, the steps that must be taken to enter a password and log onto computer terminal are a procedure. The actions needed to restore the computer system to its operational state after a major failure are another example of a procedure. Procedures often specify the actions that people should take in a step-by-step manner.

**People** : Every CBIS needs people if it is to be made useful. People are probably the components that influence the success or failure of information systems the most. Users, programmers, system analysts, and database administrators are just some of the people associated with the computer-based information systems.

Some of the characteristics of Computer Based Information Systems are as follows:

- 1) All systems work for predetermined objectives and the system is designed and developed accordingly.
- 2) In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.

## 1.18 Information Systems Control and Audit

- 3) If one subsystem or component of a system fails, in most cases the whole system does not work. However, it depends on how the subsystems are interrelated.
- 4) The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system
- 5) The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

Major areas of computer-based applications are finance and accounting, marketing and sales, manufacturing, inventory/stock management, human resource management etc.

- **Finance and Accounting**

The main goal of this subsystem (considering Business functions as whole system) is to ensure financial viability of the organization, enforce financial discipline and plan and monitor the financial budget. Also it helps forecasting revenues, determining the best resources and uses of funds and managing other financial resources. Typical sub-application areas in finance and accounting are - Financial accounting; General ledger; Accounts receivable/payable; Asset accounting; Investment management; Cash management; Treasury management; Fund management and Balance sheet.

- **Marketing and Sales**

Marketing and sales activities have great importance in running a business successfully in a competitive environment. The objective of this subsystem is to maximize sales and ensure customer satisfaction. The marketing system facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products.

The sales department may use an order processing system to keep status and track of orders, generate bills for the orders executed and delivered to the customer, strategies for rendering services during warranty period and beyond, analyzing the sales data by category such as by region, product, salesman or sales value. The system may also be used to compute commissions for dealers or salesmen and thus helps the corporate managers to take decisions in many crucial areas.

- **Production or Manufacturing**

The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service. The system generates production schedules and schedules of material requirements, monitors the product quality, plans for replacement or overhauling the machinery and also helps in overhead cost control and waste control.

- **Inventory /Stores Management**

The inventory management system is designed with a view to keeping track of materials in the stores. The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials with optimal re-order quantity and facilitate various queries about inventory like total inventory value at any



time, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc.

Similarly well-designed inventory management system for finished goods and semi-finished goods provides important information for production schedule and marketing/sales strategy.

- **Human Resource Management**

Human resource is the most valuable asset for an organization. Utilization of this resource in most effective and efficient way is an important function for any enterprise. Less disputes, right utilization of manpower and quiet environment in this functional area will ensure smooth sailing in business. Human resource management system aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included HRM system. An HRM system may have the following modules – Personnel administration; Recruitment management; Travel management; Benefit administration; Salary administration; Promotion management etc.

## **1.8 TYPES OF INFORMATION SYSTEMS AT DIFFERENT LEVELS**

It is a fact that much of management is primarily concerned with decision- making and so the importance of information system is further emphasized in this matter.

Management at different levels take decisions matching to their position or hierarchy in the organization and different types of information systems are designed and developed for them i.e. an information system for a departmental manager will be characteristically different from one designed for a corporate manager.

If we consider an organization having a pyramidal management structure with the corporate level managers at the top and operational managers at the bottom, typical categories of data are manipulated at different levels.

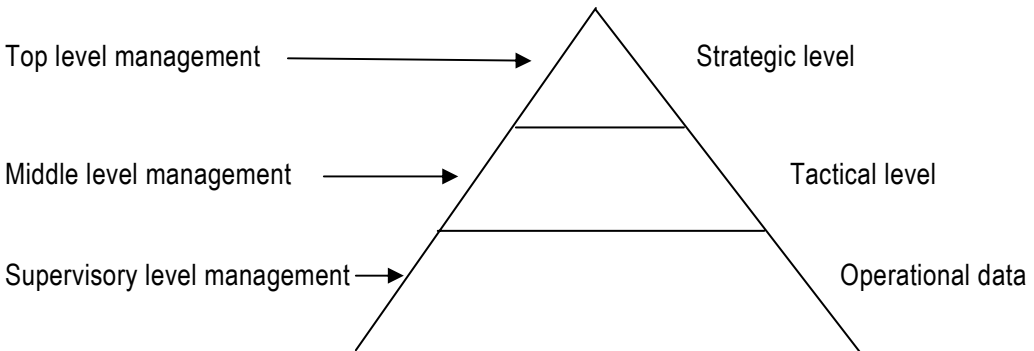
The Fig. 1.8.1 exhibits data available at different functional areas of an organization for management.

- At the lowest level, that is managed by operational level managers (like supervisor, section in-charge), all types of inputs available from various sources are collected. The routine office work, like maintaining inward register and public interaction are mostly done at this level. However, no decision-making process is carried out at this level. But proper organization of data for further processing is an important task to be completed at this level. So sufficiently trained manpower will be deployed at this stage.
- At the middle level of management the decision making-process starts. Inputs from different internal and external information sources are collected (normally passed from operational level managers) and processed for strategic decisions. Middle level managers who are expected to contribute significantly towards development of the

## 1.20 Information Systems Control and Audit

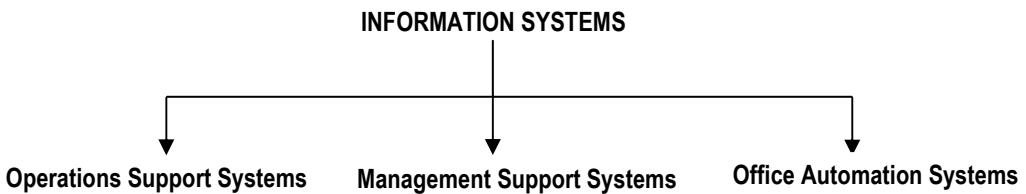
organization will be the key personnel to carry out the processing activities of the strategic data. They will use various tools of analysis and typical software products to report to the higher level with options and possible effects.

- At the top level, the decisions are taken on the basis of the information passed from middle management.



**Fig. 1.8.1 : Information systems at different Levels**

Primarily, Information systems can be classified into three broad categories upon their focus on the kind of activities in a business enterprise. These categories are shown in Fig. 1.8.2.



**Fig. 1.8.2 : Categories of Information Systems**

## 1.9 OPERATIONS SUPPORT SYSTEMS (OSS)

The objective of **Operation Support System** is to improve the operational efficiency of the enterprise. As these systems primarily are concerned with the operations, they use internal data primarily for managers at the lower levels. These are further classified into three categories:

- Transaction Processing Systems
- Management Information Systems
- Enterprise Resource Planning Systems

### 1.9.1 Transaction Processing Systems (TPS)

**Transaction Processing System (TPS)** at the lowest level of management is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use. For example, selling of a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance. Transaction processing system will thus record and manipulate transaction data into usable information.

Typically, a TPS involves the following activities :

- (i) Capturing data to organize in files or databases;
- (ii) Processing of files / databases using application software;
- (iii) Generating information in the form of reports;
- (iv) Processing of queries from various quarters of the organization.

A TPS may follow periodic data preparation and batch processing (as in payroll application) or on-line processing (as in inventory control application). However in industries and business houses now-a-days on-line approach is preferred in many applications as it provides information with up-to-date status. However, the people involved in TPS usually are not in a position to take any management decision.

#### (I) TPS Components

The principal components of a TPS include inputs, processing, storage and outputs. The components or elements are part of both manual and computerized systems.

- **Inputs** : Source documents, such as customer orders, sales, slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs into the Transaction Processing System. They serve several purposes like - capturing data, facilitating operations by communicating data and authorizing another operation in the process, standardizing operations by indicating which data require recording and what actions need to be taken, and providing a permanent file for future analysis, if the documents are retained etc.
- **Processing** : This involves the use of journals and registers to provide a permanent and chronological record of inputs. Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting. Some of the more common special journals are – sales journal, purchase journal, cash receipts journal etc.
- **Storage** : Ledgers and files provide storage of data on both manual and computerized systems. The general ledger, the accounts/vouchers payable ledgers, and the accounts

## 1.22 Information Systems Control and Audit

receivable ledger are the records of final account that provide summaries of a firm's financial accounting transactions.

- **Outputs** : Any document generated in the system is output. Some documents are both output and input. For example - a customer invoice is an output from the order-entry application system and also an input document to the customer. The trial balance lists the balances of all the accounts on the general ledger and tests the accuracy of the record keeping. Financial reports summarize the results of transaction processing and express these results in accordance with the principles of financial reporting.

### (II) Features of TPS

- (i) **Large volume of data** : As TPS is transaction – oriented, it generally consists large volumes of data and thus require greater storage capacity. Their major concern is to ensure that the data regarding the economic events in the organizations are captured quickly and correctly.
- (ii) **Automation of basic operations** : Any TPS aims at automating the basic operations of a business enterprise and plays a critical role in the day-to-day functioning of the enterprise. Any failure in the TPS for a short period of time can play havoc with the functioning of the enterprise. Thus, TPS is an important source of up-to-date information regarding the operations in the enterprise.
- (iii) **Benefits are easily measurable** : TPS reduces the workload of the people associated with the operations and improves their efficiency by automating some of the operations. Most of these benefits of the TPS are tangible and easily measurable. Therefore, cost benefit analysis regarding the desirability of TPS is easy to conduct. As the benefits from TPS are mainly tangible, the user acceptance is easy to obtain.
- (iv) **Source of input for other systems** : TPS is the basic source of internal information for other information systems. Heavy reliance by other information systems on TPS for this purpose makes TPS important for tactical and strategic decisions as well.

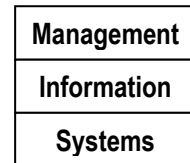
## 1.9.2 Management Information Systems (MIS)

**Management Information Systems (MIS)** assist managers in decision making and problem solving in contrast to TPS, which is operations oriented. They use results produced by the TPS, but they may also use other information. In any organization, decisions must be made on many issues that recur regularly and require a certain amount of information. Because the decision making process is well understood, the manager can identify the information that will be needed for the purpose. In turn, the information systems can be developed so that reports are prepared regularly to support these recurring decisions.

**(I) Definition of Management Information System (MIS)** : Many experts have defined MIS in different languages. A Management Information System has been defined by Davis and Olson as “**An integrated user-machine system designed for providing information to**

**support operational control, management control and decision making functions in an organization”.**

The information system makes use of resources such as hardware, software, personnel, procedure and supplies as well. MIS is designed to provide accurate, relevant and timely information to managers at different levels and in different functional areas throughout the organization for decision-making purpose. MIS support the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals. Nature of MIS at different levels has different flavors and they are available in the form of reports, tables, graphs and charts or in presentation format using some tools. MIS at the top level is much more comprehensive and condensed or summarized compared to that existing in the middle level management. In order to understand MIS, its constituent components (Fig. 1.9.1) must be well understood.



**Fig. 1.9.1 : MIS Components**

**Management** : A manager may be required to perform following activities in an organization:

- (i) Determination of organizational objectives and developing plans to achieve them.
- (ii) Securing and organizing the human and physical resources so that these objectives could be accomplished.
- (iii) Exercising adequate controls over the functions.
- (iv) Monitoring the results to ensure that accomplishments are proceeding according to plan.

Thus, management comprises the processes or activities that describe what managers do in the operation of their organization : plan, organize, initiate, and control operations. In other words, Management refers to a set of functions and processes designed to initiate and co-ordinate group efforts in an organized setting directed towards promotion of certain interest, preserving certain values and pursuing certain goals. It involves mobilization, combination, allocation and utilization of physical, human and other needed resources in a judicious manner by employing appropriate skills, approaches and techniques.

**Information (as referred to MIS)** : Information could be defined as sets of facts, figures and symbols processed for the current decision-making situation. The information is considered to be of significance in a particular situation.

**System** : A system is defined as a set of related components, activities, process and human beings interacting together so as to accomplish some common objective.

Putting all these three components together, MIS can be defined as set of related processes, activities individuals or entities interacting together to provide processed data to managers at various levels and functional areas.

The functions of MIS can be shown with the help of Fig. 1.9.2. For example, in a competitive market for products manufactured by an enterprise, its management needs information on the

## 1.24 Information Systems Control and Audit

pricing policy of the competitors, specially of competing products, sales techniques etc., to effectively combat the effect of the competition.

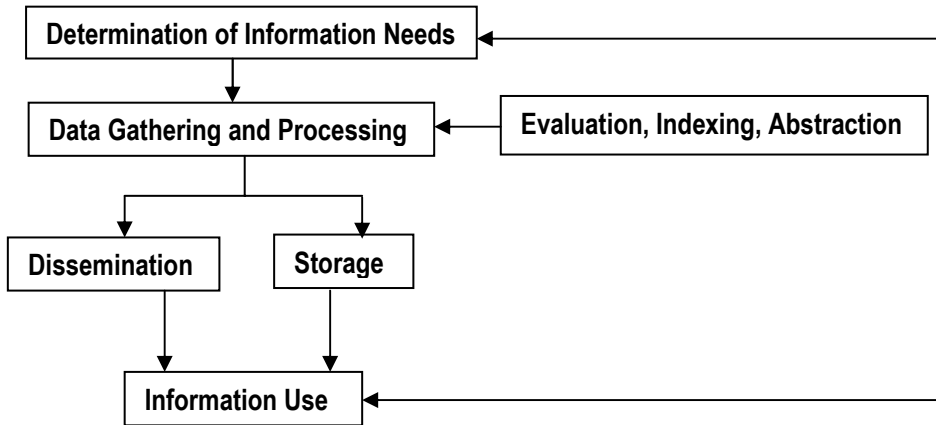


Fig. 1.9.2 : Functions of MIS

(II) **Characteristics of an effective MIS** : Some of the important characteristic for an effective MIS are eight in number and are briefly discussed below:

- (i) **Management Oriented** : It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only, it may also meet the information requirements of middle level or operating levels of management as well.
- (ii) **Management Directed** : Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- (iii) **Integrated** : Development of information should be an integrated one which means that all the functional and operational information sub-system should be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management by taking a comprehensive view or a complete look at the inter locking sub-systems that operate within a company.
- (iv) **Common Data Flows** : It means the use of common input, processing and output procedures and media whenever required. Data is captured by system analysts only once and as close to its original source as possible. They, then, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.

- (v) **Heavy Planning Element** : An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development who should keep in view future objectives and requirements of firm's information in mind.
  - (vi) **Sub System Concept** : Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
  - (vii) **Common Database** : Database is the mortar that holds the functional systems together. It is defined as a "super-file" which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
  - (viii) **Computerized** : Though MIS can be implemented without using a computer, the use of computers increases the effectiveness of the system. In fact, its use equip the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.
- (III) Misconceptions about MIS** : Some of the myths about MIS are as follows :
- (i) The study of MIS is about the use of computers. This statement is not true. MIS may or may not be computer based, computer is just a tool, just like any other machine. Installing a MIS depends largely on several factors such as – how critical is the response time required for getting an information; how big is the organization; and how complex are the needs of the information processing.
  - (ii) More data in reports means more information for managers. This is a misapprehension. It is not the quantity of data, but its relevance, which is important to managers in process of decision-making. Data provided in reports should meet information requirements of managers. It is the form of data and its manner of presentation that is of importance to business managers. Unorganized mass of data creates confusion.
  - (iii) Accuracy in reporting is of vital importance. The popular belief is that accuracy in reporting should be of high order. At the operating level, it is true. Other examples, where accuracy is really important, can be the dispensing of medicine; the control of aircraft; the design of a bridge etc. Accuracy, however, is a relevant but not an absolute ideal. Higher levels of accuracy involve higher cost. At higher decision levels, great accuracy may not be required. The degree of accuracy is closely related to the decision problem. Higher management is concerned with broad decisions on principles and objectives. A fairly correct presentation of relevant data often is adequate for top management decisions. For a decision on a new project proposal, top management is not interested in knowing the project cost in precise rupee terms. A project cost estimated at a fairly correct figure is all what it wants.

## 1.26 Information Systems Control and Audit

**(IV) Pre-requisites of an effective MIS :** The main pre-requisites of an effective MIS are as follows :

(i) **Database :** It can be defined as a “super-file” which consolidates data records formerly stored in many data files. The data in database is organized in such a way that access to the data is improved and redundancy is reduced. Normally, the database is sub-divided into the major information sub-sets needed to run a business. The main characteristic of database is that each sub-system utilizes same data and information kept in the same file to satisfy its information needs. The other important characteristics of database are as follows :

- It is user-oriented.
- It is capable of being used as a common data source, to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.
- It is available to authorized persons only.
- It is controlled by a separate authority established for the purpose, known as Data Base Management System (DBMS).

The maintenance of data in database requires computer hardware, software and experienced computer professionals. In addition, it requires a good data collection system equipped with experts having first-hand knowledge of the operations of the company and its information needs.

(ii) **Qualified system and management staff :** The second pre-requisite of effective MIS is that it should be manned by qualified officers. These officers who are expert in the field should understand clearly the views of their fellow officers. For this, the organizational management base should comprise of two categories of officers Systems and Computer experts and Management experts.

- Systems and Computer experts in addition to their expertise in their subject area should also be capable of understanding management concepts to facilitate the understanding of problems faced by the concern. They should also be clear about the process of decision making and information requirements for planning and control functions.
- Management experts should also understand quite clearly the concepts and operations of a computer. This basic knowledge of computers will be useful to place them in a comfortable position, while working with systems technicians in designing or otherwise of the information system.

(iii) **Support of Top Management :** The management information system to become effective, should receive the full support of top management. The reasons for this are as follows :

- Subordinate managers are usually lethargic about activities, which do not receive the support of their superiors (top management).



- The resources involved in computer-based information systems are large and are growing larger in view of importance gained by management information system.

To gain the support of top management, the officers should place before top management all the supporting facts and state clearly the benefits, which will accrue from it to the concern. This step will certainly enlighten management, and will change their attitude towards MIS. Their wholehearted support and cooperation will help in making MIS an effective one.

- (iv) **Control and maintenance of MIS** : Control of the MIS means the operation of the system as it was designed to operate. Some time, users develop their own procedures or short cut methods to use the system, which reduce its effectiveness. To check such habits of users, the management at each level in the organization should devise checks for the information system control.

Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.

- (v) **Evaluation of MIS** : An effective MIS should be capable of meeting the information requirements of its executives in future as well. This capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points.
- Examining whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future.
  - Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.
  - Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

**(V) Constraints in operating a MIS** : Major constraints which come in the way of operating an information system are the following :

- (i) Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- (ii) Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts depend upon the need and importance of a function for which MIS can be installed first.
- (iii) Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
- (iv) Non-availability of cooperation from staff is a crucial problem which should be handled tactfully. This task should be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

## 1.28 Information Systems Control and Audit

**(VI) Effects of using Computer for MIS :** The effect of applying computer technology to information system can be listed as below :

- (i) **Speed of processing and retrieval of data increases :** Modern business situations are characterized by high degree of complexity, keen competition and high risk and reward factors. This invariably calls for systems capable for providing relevant information with minimum loss of time. Manual systems, howsoever well organized, often fail to match the demand for information for decision making. Computer with its unbelievably fast computational capability and systematic storage of information with random access facility has accounted as a major factor in inducing MIS development.
- (ii) **Scope of analysis widened :** The use of computer can provide multiple type of information accurately and in no time to decision makers. Such information equips an executive to carry out a thorough analysis of the problems and to arrive at the final decision. Computer is capable of providing various types of sales reports for example; area wise sales commission of each salesman, product-wise sales, etc. Which are quite useful in analyzing the sales department working and to ascertain their weaknesses so that adequate measures may be taken in time. In this way, the use of computer has widened the scope of analysis.
- (iii) **Complexity of system design and operation increased :** The need for highly processed and sophisticated information based on multitudes of variables has made the designing of the system quite complex. The computer manufacturers have developed some important programs (software) that can perform the task of developing programs to cater to the specialized needs of their customers, either on consultancy basis or on contract.
- (iv) **Integrates the working of different information sub-system :** A suitable structure of MIS may be a federation of information sub-system, viz., production, material, marketing, finance, engineering and personnel. Each of these sub-systems are required to provide information to support operational control, management control and strategic planning. Such information may be made available from a common-data-base that meet out the information requirements of different information sub-system by utilizing the services of computers for storing, processing, analyzing and providing such information as and when required.
- (v) **Increases the effectiveness of Information system :** Information received in time is of immense value and importance to a concern. Prior to the use of computer technology for information purposes, it was difficult to provide the relevant information to business executives in time even after incurring huge expenses. But now with the use of computer technology, it is not difficult to provide timely, accurate and desired information for the purpose of decision making.
- (vi) **More comprehensive information :** The use of computer for MIS enabled systems expert to provide more comprehensive information to executives on business matters.

**(VII) Limitations of MIS :** The main limitations of MIS are as follows :

- (i) The quality of the outputs of MIS is basically governed by the quantity of input and processes.

- (ii) MIS is not a substitute for effective management which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- (iii) MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- (iv) MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- (v) MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives.
- (vi) MIS is less useful for making non-programmed decisions. Such type of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- (vii) The effectiveness of MIS is reduced in organizations, where the culture of hoarding information and not sharing with other holds.
- (viii) MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

### 1.9.3 Enterprise Resource Planning (ERP) Systems

**Enterprise Resource Planning (ERP)** is one of the latest high-end solutions that seek to streamline and integrate operation processes and information flows in the company to synergize the five major resources of an organization namely men, money, machine, materials and market. Formally, ERP can be defined as follows :

“An ERP system is a fully integrated business management system that integrates the core business and management processes to provide an organization a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable real-time information.”

- (I) **Objectives** : The major objectives of ERP are to
- provide support for adopting best business practices
  - implement these practices with a view towards enhancing productivity and
  - empower the customers and suppliers to modify the implemented business processes to suit their needs.

An ERP system integrates various business processes as shown in Fig. 1.9.3.

- (a) **Business System** : It includes the following aspects - Business Forecasting for product/market groups; Target fixing and allocation by key parameters; Strategy formulation and implementation; Resource allocation to key result areas; Strategy monitoring and control and Information-based management for management applications.

### 1.30 Information Systems Control and Audit

- (b) **Production** : It includes the following aspects - Production planning and control; Work processes; Purchasing and procurement system; Inventory management; Inventory analysis and valuation; Excise/ custom interface; and Production information systems for production applications.
- (c) **Maintenance** : It includes the following aspects - Plant maintenance planning; Breakdown, preventive, and conditional maintenance; Maintenance management – initiation, execution, control and costing; Monitoring performance of maintenance action; Maintenance contract management; and Maintenance information systems for maintenance applications.
- (d) **Quality Control** : It includes the following aspects - Quality assessment against standards; Quality assessment by process, materials, and work center location; Analysis of quality by reasons and actions taken; Building quality assurance data for equipment/process/ technology selection; Monitoring quality across the organization from input to output for operating decisions and business decisions; and Quality control information systems for quality control applications.

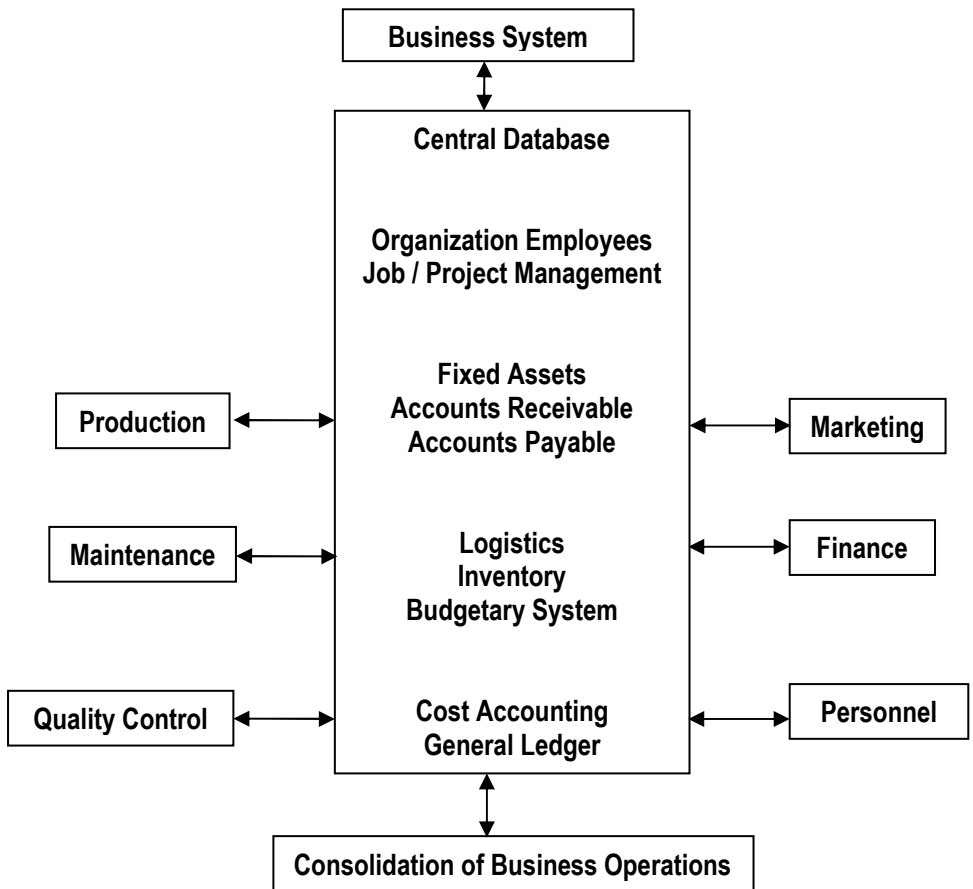


Fig. 1.9.3 : Enterprise Resource Planning Model

- (e) **Marketing** : It includes the following aspects - Market/customer/product analysis; Sales forecasting and budgeting; Marketing research information; Distribution and channel management; Order processing and analysis; Finished good store management; Dispatching and invoicing; Accounts receivable analysis and management; and Marketing information systems for marketing applications.
- (f) **Finance** : It includes the following aspects - Financial planning and control; Management of long-term funds and working capital management; Ledgers, payables and receivables; Financial statement analysis; Cost accounting – cost center accounting and product / process costing; Cost analysis for management decisions; Tax management; Finance information systems for finance applications.
- (g) **Personnel** : It includes the following aspects - Human resource planning, recruitment, and training; Employee performance appraisal and upgradation; Job evaluation and compensation management; Employee benefits and incentives; Employee health and safety; Disciplinary measures; Maintaining industrial peace; Personnel information systems for personnel applications.
- (h) **Consolidation of Business Operations** : It includes the following aspects - Accounting by units and divisions with local focus; Consolidation by accounts in corporate functions; Comprehensive reporting systems for business decisions.
- (II) **Myths of ERP System** : Some of the misconceptions about ERP System are as follows :
  - (i) There is a misconception that ERP is a computer system. Even though computers and Information technology are integral parts of an ERP system, ERP is primarily an enterprise-wide system which encompasses corporate mission; objectives; attitudes; beliefs; values; operating style; and people who make the organization.
  - (ii) There is a misconception that ERP is relevant for manufacturing organizations only. In contrast, ERP system is not limited to any particular industry segment but is relevant for all types of business activities which include manufacturing as well as services.
- (III) **Characteristics of ERP System** : Some of the characteristics of ERP System are as follows :
  - (i) **Flexible** : ERP is a flexible system which may cover different languages, currencies, and accounting standards etc. Functions that comprehensively manage multiple locations of an organization can be packaged and implemented automatically.
  - (ii) **Modular and Open** : ERP system is modular and open which implies that any module can be interfaced or detached, whenever required, without affecting the other modules. It supports multiple hardware platforms for the organizations having heterogeneous collection of systems and also supports third party add-ons also by providing access to open database connectivity through the use of client/ server technology.
  - (iii) **Integrated** : ERP is an integrated system as it provides data automation – automatic data exchange among different applications - that takes place between related business components. The data of related business functions are automatically updated at the

### 1.32 Information Systems Control and Audit

time a transaction occurs. Due to this feature, one is able to grasp business details in real time, and carry out various types of management decisions in a timely manner.

- (iv) **Best Business Practices** : ERP aims at adopting best business practices applicable worldwide and imposes its own logic on an organization's strategy and its implementation. Best business practices available worldwide can also be adopted by an organization through benchmarking which is the process of identifying, understanding, and adapting outstanding practices from other organizations to help improve performance.

**(IV) Features of ERP** : Some of the major features of ERP and what ERP can do for the business system are as follows:

- (i) ERP provides multi-platform, multi-facility, multi-code manufacturing, multi currency, and multi-lingual facilities.
- (ii) It supports strategic and business planning activities, operational planning and execution activities and creation of resources. All these functions are effectively integrated for flow and updation of information immediately upon entry of any information.
- (iii) It has end-to-end Supply Chain Management (SCM) to optimize the overall demand and supply of data.
- (iv) It facilitates organization-wide integrated information system covering all functional areas like – production, marketing, finance and accounting and human resources.
- (v) It performs core activities and increases customer service, thereby augmenting the corporate image.
- (vi) It bridges the information gap across organizations.
- (vii) It provides complete integration of system not only across departments but also across companies under the same management.
- (viii) It allows automatic introduction of the latest technologies like electronic funds transfer (EFT), Electronic Data Interchange (EDI), Internet, Video conferencing, Electronic commerce (E-Commerce) etc.
- (ix) It eliminates most of the business problems like material shortage, productivity enhancement, customer service, cash management, inventory management, quality management, prompt delivery etc.

It provides intelligent business tools like decision support systems, executive information systems, data mining and easy working systems to enable better decision making.

**(V) Benefits of ERP** : There are numerous benefits of ERP which can be categorized into following groups:

- (i) **Better use of Organizational Resources** : ERP enables an organization to make better use of its resources which are scarce by their nature. Making better use of these resources is possible because ERP offers a model which indicates where the resources

find best usage and how resources can be managed in that particular usage to produce the best result. Thus, through the application of ERP, organizational resources are put at a place where they have their optimum utilization.

- (ii) **Lower Operating Costs** : ERP results into lower operating costs to the organization. Lowering operating costs is possible because of improved business performance through cycle time reduction, inventory reduction, order fulfillment improvement, increased business agility, etc. Lower operating costs mean improved profitability for the organization.
  - (iii) **Proactive Decision Making** : In today's competitive and dynamic environment, there is a need for proactive decision making rather than the reactive decision making. A proactive decision-making process emphasizes that decisions must be made in advance of likely environmental changes and anticipated competitive moves by competitors.
  - (iv) **Decentralized Decision Making** : ERP enables an organization to decentralize its decision-making process. Thus, decisions are made at those points at which these are relevant for execution. Due to faster processing technology and structured query language (SQL), managers can see the information in their own perspective. Further, with intelligent ERP downloads, decisions can be made even at lower management levels. Thereby releasing the burden on higher management levels and freeing them for strategic thinking.
  - (v) **Enhanced customer Satisfaction** : To compete effectively in today's marketplace, organizations must focus on their customers. Customers have become increasingly aggressive in demanding quality and service because they have a wide range of choices. This requires organizations to define end-to-end approach for managing customers' requests. ERP provides the way for this in the form of efficient and effective processing of requests and emphasizing customer relationship management.
  - (vi) **Flexibility in Business Operations** : ERP provides flexibility in business operations, which is required to adjust according to environmental needs. In order to take care of changing needs, an organization has to design its business operations in such a way that enables these operations to change according to environmental needs. ERP provides flexibility in business operations because different languages, currencies, accounting standards, etc. can be covered in one system.
- (VI) Limitations of ERP** : Though ERP system has many benefits, it has some limitations which are as follows :
- (i) An ERP system provides current status only, such as open orders, Managers often need to look at past along with the current status to identify trends and patterns that aid better decision making.
  - (ii) The methods used in the ERP applications are not integrated with other organizational or divisional systems. Further, they do not include external intelligence.

## 1.34 Information Systems Control and Audit

ERP packages are integrated software packages, covering all business finances that support the ERP operations. An ERP software is designed to model and automate many of the basic processes of a company with the objective of integrating information across the company. Some major ERP packages available in Indian market are as SAP, Oracle Applications, Ramco Marshals, eBPCs, Activera and Baan ERP.

### 1.10 MANAGEMENT SUPPORT SYSTEMS (MSS)

**Management Support Systems (MSS)** focus on the managerial uses of information resources and provide information to managers for planning and decision making. The information provided by these systems is based on both the internal and external data using various data analysis tools. There are three types of MSS, namely :

- Decision Support Systems (DSS)
- Executive Information (Support) System (EIS)
- Expert Systems

#### 1.10.1 Decision Support Systems (DSS)

##### (I) What is a DSS?

**Decision Support Systems (DSS)** are a specific class of computerized information system that supports business and organizational decision-making activities. A properly-designed DSS is an interactive software-based system intended to help decision makers compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions.

Typical information that a decision support application might gather and present would be

- an inventory of all the current information assets (including legacy and relational data sources, cubes, data warehouses, and data marts) of an organization;
- comparative sales figures between one week and the next,
- projected revenue figures based on new product sales assumptions;
- the consequences of different decision alternatives, given past experience in a context that is described.

In other words, a Decision Support System (DSS) can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own, somewhat personalized, way. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enable them to generate the information required by them in making decisions. In other words, a DSS supports the human decision-making process, rather than providing a means to replace it.

**Programmed Decision Systems** : Systems that replace human decision making rather than support it are sometimes called **Programmed Decision Systems**. These systems are used to



make routine, structured decisions, such as approving loans or credit, reordering inventory, triggering reminder notices, and selecting audit samples. In programmed decision systems, the focus is on doing something more efficiently, whereas in DSS, the focus is on helping decision makers become more effective.

(II) **Characteristics of DSS** : The DSS are characterized by at least three properties:

- They support semi-structured or unstructured decision-making.
- They are flexible enough to respond to the changing needs of decision makers, and
- They are easy to use.

(i) **Semi-structured and Unstructured Decisions** : Structured decisions are those that are easily made from a given set of inputs. These types of decisions such as deciding to issue a reminder notice if a bill is overdue or deciding to sell a stock under a given set of market conditions can be programmed fairly easily. Unstructured decisions and semi-structured decisions, however, are decisions for which information obtained from a computer system is only a portion of the total knowledge needed to make the decision.

The DSS is particularly well adapted to help with semi-structured and unstructured decisions. However, it can be designed to support structured decision making as well. A manager, for instance, can browse through data at will (perhaps at a display terminal). When enough information is gathered from this process to supplement other information (perhaps some of it may be non computer-based), a decision can be reached.

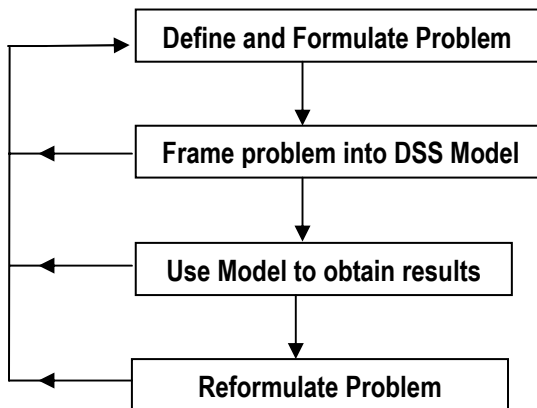


Fig. 1.10.1 : Steps in solving a problem with DSS

In Fig. 1.10.1, it is shown how a semi-structured problem might be solved by using a DSS.

- Firstly, the problem is defined and formulated.
- It is then modeled with DSS software.
- Next, the model is run on the computer to provide results. The modeler, in reviewing these results, might decide to completely reformulate the problem, refine the model, or use the model to obtain other results.

### 1.36 Information Systems Control and Audit

For example, a user might define a problem that involves simulating cash flows under a variety of business conditions by using financial modeling software. The DSS model is then run, providing results. Depending on what the results of the model indicate about cash flow, the user might decide to completely remodel the problem, make small modifications to the current model, run the model under a number of new assumptions, or accept the results. For instance, if the model revealed inadequate cash flows to support organizational operations, model modifications should be developed and run. The modification process might continue for several interactions until an acceptable cash flow is identified.

- (ii) **Flexibility to adapt to changing needs** : Semi-structured and unstructured decisions often do not conform to a predefined set of decision-making rules. Because of this, their DSS must provide for enough flexibility to enable users to model their own information needs and should also be capable of adapting to changing information needs.

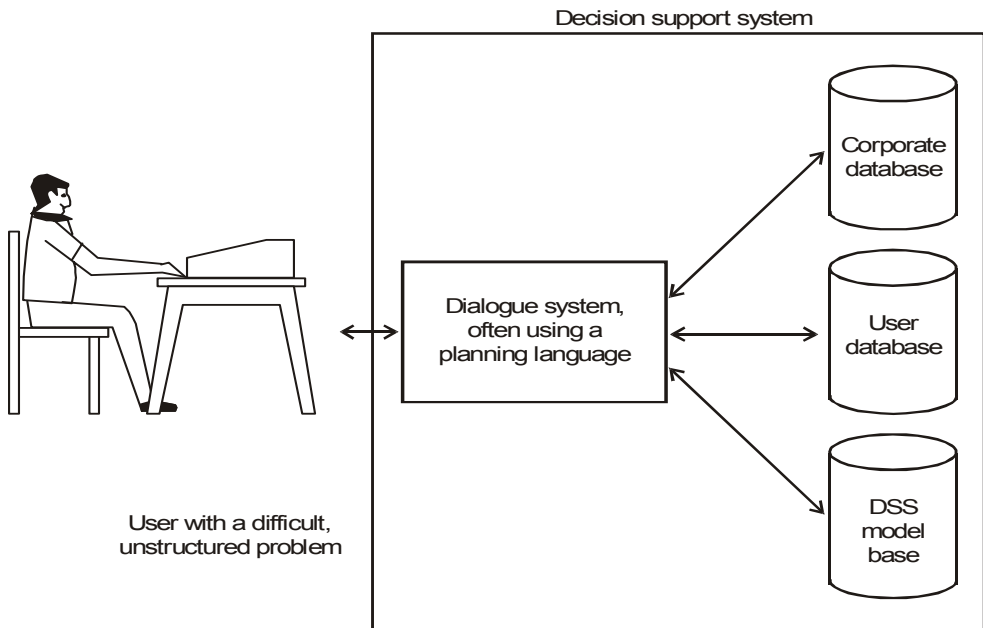
The DSS designer understands that managers usually do not know in advance what information they need and, even if they do, those information needs keep changing constantly. Thus, rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

- (iii) **Ease of Learning and Use** : Since DSS are often built and operated by users rather than by computer professionals, the tools that accompany them should be relatively easy to learn and use. Such software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth – generation languages (4GL), natural English, and easily read documentation, thus making it easier for users to conceptualize and perform the decision-making process.

(III) **Components of DSS (see Fig. 1.10.2)** A decision support system has four basic components listed below :

- (i) **The user** : The user of a Decision Support System is usually a manager with an unstructured or semi-structured problem to solve. Manager and staff specialist (analyst) are the two broad classes of users. Typically, users do not need a computer background to use a decision support system for problem solving. The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution.
- **Manager** : These are the users who have basic computer knowledge and want the DSS to be very user friendly. The manager may be at any level of authority in the organization (e.g., either top management or operating management).
  - **Staff Specialist (Analysts)** : These are the people who are more details oriented and willing to use complex system in their day to day work.

- (ii) **Databases** : Decision Support Systems include one or more databases that contain both routine and non-routine data from both internal and external sources. The data from external sources include data about the operating environment surrounding an organization – for example, data about economic conditions, market demand for the organization's goods or services, and industry competition.



**Fig. 1.10.2 : DSS Components**

Decision Support System users may construct additional databases themselves. Some of the data may come from internal sources. An organization often generates this type of data in the normal course of operations – for example, data from the financial and managerial accounting systems such as account, transaction, and planning data. The database may also capture data from other subsystems such as marketing, production, and personnel. External data include assumptions about such variables as interest rates, vacancy rates, market prices, and levels of competition.

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

- (a) **Physical level** : It involves the implementation of the database on the hard disk i.e. storage of data in the hard disk. The management of storage and access is controlled by operating system.
- (b) **Logical Level** : It is designed by professional programs, who have complete knowledge of DBMS. It deals with the nature of data stored, the scheme of the data. Storage which is logically divided into various tables having rows and columns and the techniques for defining relationships with indexes.

### 1.38 Information Systems Control and Audit

- (c) **External level** : The logical level defines schema which is divided into smaller units known as sub-schemas and given to the managers each sub-schema containing all relevant data needed by one manager.
- (iii) **Planning languages** : Two types of planning languages that are commonly used in Decision Support Systems are – **General-purpose planning languages** and **Special-purpose planning languages**.
- General-purpose planning languages that allow users to perform many routine tasks – for example, retrieving various data from a database or performing statistical analyses. The languages in most electronic spreadsheets are good examples of general-purpose planning languages. These languages enable user to tackle a broad range of budgeting, forecasting, and other worksheet-oriented problems.
  - Special-purpose planning languages are more limited in what they can do, but they usually do certain jobs better than the general-purpose planning languages. Some statistical languages, such as SAS and SPSS, are examples of special purpose planning languages.
- (iv) **Model base** : The planning language in a DSS allows the user to maintain a dialogue with the model base which is the “brain” of DSS because it performs data manipulations and computations with the data provided to it by the user and the database. There are many types of model bases, but most of them are custom-developed models that do some types of mathematical functions - for example, cross tabulation, regression analysis, time series analysis, linear programming and financial computations. The analysis provided by the routines in the model base is the key to supporting the user’s decision.

#### (IV) Examples of Decision Support Systems in Accounting

Many DSS are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations of these systems.

- **Cost Accounting System** : The health care industry is well known for its cost complexity. Managing costs in this industry require controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care organizations calculate product costs for individual procedures or services. One health care organization, for example, combines a variety of DSS applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.
- **Capital Budgeting System** : Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One DSS designed to support decisions about investments in automated manufacturing technology is **AutoMan**, which allows decision makers to consider financial, nonfinancial,

quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. They can then evaluate up to seven investment alternatives at once.

- **Budget Variance Analysis System** : Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized DSS to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
- **General Decision Support System** : As mentioned earlier, some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker's tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called **Expert Choice** which supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert Choice analyzes these judgments and presents the decision maker with the best alternative.

### 1.10.2 Executive Information Systems (EIS)

An **Executive Information System (EIS)** – sometimes referred to as an Executive Support System (ESS) – is a DSS that is designed to meet the special needs of top-level managers. Some people use the terms “EIS” and “ESS” interchangeably, but others do not. Any distinction between the two usually is because Executive Support Systems are likely to incorporate additional capabilities such as electronic mail. In this section, we first cover those people in organizations that are considered to be executives and examine the types of decisions they make.

**Executives** : An executive can probably best be described as a manager at or near the top of the organizational hierarchy who exerts a strong influence on the course taken by the organization. The slots in a firm considered to be executive positions vary from company to company. For example, in many firms, the Chief Information Officer (CIO) is usually an executive who participates in key strategic decisions. In other firms, the CIO is a middle manager (who often has a title other than CIO). And sometimes, the person in charge of an organization's CBIS is basically a data processing director.

## 1.40 Information Systems Control and Audit

(I) **Characteristics of EIS** : Some of the characteristics of EIS are as follows :

- (i) EIS is a Computer-based-information system that serves the information need of top executives.
- (ii) EIS enables users to extract summary data and model complex, problems without the need to learn query languages statistical formulas or high computing skills.
- (iii) EIS provides rapid access to timely information and direct access to management reports.
- (iv) EIS is capable of accessing both internal and external data.
- (v) EIS provides extensive online analysis tool like trend analysis, market conditions etc.
- (vi) EIS can easily be given a DSS support for decision making.

(II) **Executive Roles and Decision Making** : Most executive decisions fall into one of three classes : **Strategic planning, Tactical planning, and “Fire-fighting” activities** (see Fig. 1.10.3). Also, executives need a certain degree of control to ensure that these activities are carried out properly.

- **Strategic Planning** : Strategic planning involves determining the general, long-range direction of the organization. Typically, the CEO is ultimately responsible for the development of strategic plans.

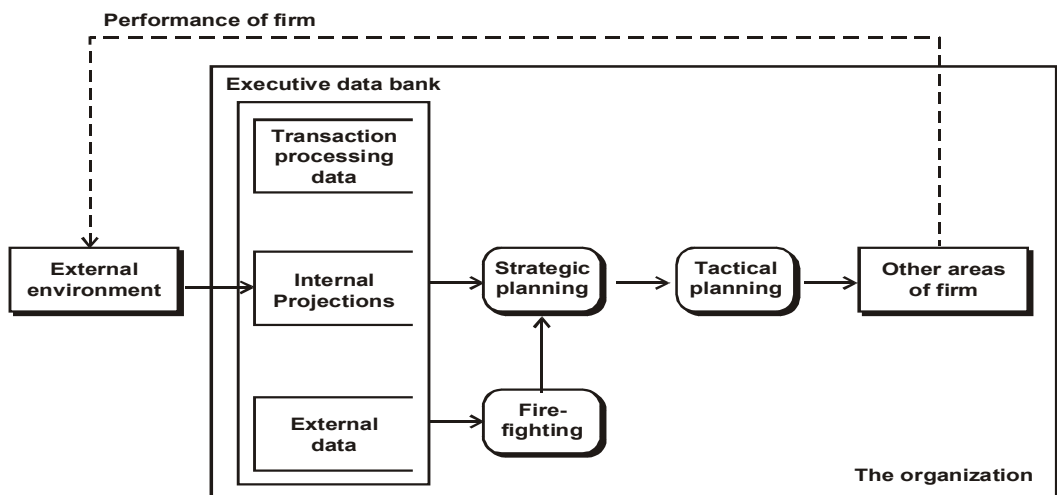


Fig. 1.10.3 : A data flow representation of the executive decision-planning environment.

- **Tactical Planning** : Whereas strategic planning addresses the general concerns of the firm, tactical planning refers to the how, when, where, and what issues involved with carrying out the strategic plan. Although executives will not normally be concerned with tactical details, they do need to worry about general tactics. For example, the vice-president of finance must address how the firm can best achieve a balance between debt

and equity financing. And the marketing vice-president will need to consider which classes of products the company should produce to be successful in the marketplace.

- **Fire Fighting** : Major problems arise sometimes that must be resolved by someone at an executive level. For example, if a company is involved in a big lawsuit that threatens its financial solvency, an executive must get involved. Other possible fire-fighting activities include damage caused to a major facility, the announcement of an important product by a competitor, a strike, and a sharp reversal of the economy. Many of these events will call for key alterations in plans.

In addition to planning and fire-fighting, executive management also needs to exert some general control over the organization. For example, if the strategic plan calls for a 20 percent increase in profitability, feedback is needed to ensure that certain actions taken within the organization are accomplishing that objective. Thus, executives will also periodically review key performance data to see how they compare against planned amounts.

**(III) The Executive Decision-Making Environment** : The type of decisions that executives must make is broad. Often, executives make these decisions based on a vision they have regarding what it will take to make their companies successful. To a large extent, executives rely much more on their own intuition than on the sophisticated analytical skills. The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives. Five characteristics of the types of information used in executive decision making are-lack of structure, high degree of uncertainty, future orientation, informal source, and low level of detail. These are discussed below:

- **Lack of structure** : Many of the decisions made by executives are relatively unstructured. These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data when reaching a decision.
- **High degree of uncertainty** : Executives work in a decision space that is often characterized by a lack of precedent. For example, when the Arab oil embargo hit in mid-1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions. If prices are lowered, for instance, product demand will not automatically increase.
- **Future orientation** : Strategic-planning decisions are made in order to shape future events. As conditions change, organizations must change also. It is the executive's responsibility to make sure that the organization keeps pointed toward the future. Some key questions about the future include : "How will future technologies affect what the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now?" As one can see, the answers to all of these questions about the future external environment are vital.
- **Informal Source** : Executives, more than other types of managers, rely heavily on informal source for key information. For example, lunch with a colleague in another firm

## 1.42 Information Systems Control and Audit

might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company’s database or in scheduled computer reports.

- **Low level of detail** : Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overview than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

Dimensions of Difference	Executive Information System	Traditional Information System
Level of management	For top or near top executives.	For lower staff.
Nature of Information Access	Specific issues/problems and aggregate reports	Status reporting
Nature of information provided	Online tools and analysis.	Offline status reporting.
Information Sources	More external, less internal	Internal
Drill down facility to go through details at successive	Available.	Not available
Information format	Text with graphics	Tabular
Nature of interface	User-friendly	Computer-operator generated.

**Table 1.10.1 : EIS vs Traditional Information Systems**

As shown in Table 1.10.1, Executive Information Systems differ from Traditional Information Systems in the following ways :

- Information tends to be presented by pictorial or graphical means.
- Information is presented in summary format, e.g. sales for the whole company. There is, however, the facility to ‘drill down’ to other levels of information to see how the sale figure were arrived at -by geographical location, by product group etc.

The powerful focus of an EIS is due to the saying “what gets measured gets done.” Managers are particularly attentive to concrete information about their performance when it is available to their superiors. This focus is very valuable to an organization if the information reported is actually important and represents a balanced view of the organization’s objectives.

Misaligned reporting systems can result in inordinate management attention to things that are not important or to things which are important but to the exclusion of other equally important things. For example, a production reporting system might lead managers to emphasize volume



of work done rather than quality of work. Worse yet, productivity might have little to do with the organization's overriding customer service objectives.

**(IV) Contents of EIS :** A general answer to the question of what data is appropriate for inclusion in an Executive Information System is "whatever is interesting to executives".

EIS implementations begin with just a few measures that are clearly of interest to senior managers, and then expand in response to questions asked by those managers as they use the system. Over time, the presentation of this information becomes stale, and the information diverges from what is strategically important for the organization.

While the above indicates that selection of data for inclusion in an EIS is difficult, there are several guidelines that help to make that assessment. A practical set of principles to guide the design of measures and indicators to be included in an EIS is presented below :

- (i) EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.
- (ii) EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.
- (iii) Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.
- (iv) EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
- (v) EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
- (vi) EIS measures must evolve to meet the changing needs of the organization.

### 1.10.3 Expert Systems

An **Expert System** is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert System are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities? And so on.

A characteristic of expert systems is the ability to declare or explain the reasoning process that was used to make decisions.

## 1.44 Information Systems Control and Audit

Some of the business applications of Expert Systems are as follows :

- (i) **Accounting and Finance** : It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, Providing investment advice.
- (ii) **Marketing** : It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
- (iii) **Manufacturing** : It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.
- (iv) **Personnel** : It is useful in assessing applicant qualifications, giving employees assisting at filling out forms
- (v) **General Business** : It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

### (I) Need for Expert Systems

- (i) Expert labor is expensive and scarce. Knowledge workers employee who routinely work with data and information to carry out their day to day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.
- (ii) Moreover, no matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.

Both these limitations imposed by human information processing capability and the rushed pace at which business is conducted today put a practical limit on the quality of human decision making this putting a need for expert systems.

### (II) Benefits of Expert Systems

- (i) Expert Systems preserve knowledge that might be lost through retirement resignation or death of an acknowledged company expert.
- (ii) Expert Systems put information into an active-form so it can be summoned almost as a real-life expert might be summoned.
- (iii) Expert Systems assist novices in thinking the way experienced professional do.
- (iv) Expert Systems are not subject to such human fallings as fatigue, being too busy, or being emotional.
- (v) Expert Systems can be effectively used as a strategic tool is the areas of marketing products, cutting costs and improving products.

Still Expert Systems are not always the answer to managerial or organizational problems. Some of the properties that potential applications should posses to qualify for Expert System development are as follows:

- (i) **Availability** : One or more experts are capable of communicating how they go about solving the problems to which the Expert System will be applied.
- (ii) **Complexity** : Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
- (iii) **Domain** : The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.
- (iv) **Expertise** : Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- (v) **Structure** : The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

### (III) Components of Expert Systems

An Expert System provides tools, information and methods for decision making in specific areas such as systems which generate competitive bids, systems to support loan approved, systems to support draining in specialized areas where experts are in scarcity and so on.

An Expert System is typically composed of the **Knowledge Base**, **Inference Engine**, the **Knowledge Acquisition Subsystem** and the **User Interface**.

#### (i) Knowledge Base (KB)

The knowledge base stores the rules data and relationships that are used to solve problems and contains specific facts about the expert area. For instance, the example where an insurance agent needs both expert tax and financial advice is a good candidate for an Expert System with two knowledge bases. With such a system, a set of rules must be developed to bridge the knowledge bases and resolve any conflicts.

The knowledge acquired from the expert has to be represented formally that deals with the structuring of the information, how to manipulate it to infer additional data, and knowledge acquisition. The power of a system tends to be related to the depth and breadth of the knowledge in the knowledge base. There are several types of representation techniques, like - Production Rule Systems, a Structured Object and Predicate Calculus or Logic.

#### (ii) Inference Engine

The inference engine is the main processing element consisting of system of programs that requests data from the user, manipulates the knowledge base and provides a decision to the user. It performs this task in order to deduce new facts, which are then used to draw further conclusions. The inference engine is the active component of an expert system since it steers through knowledge and progresses the whole interaction. The inference engine chooses rules from the agenda to fire.

There are, in fact, various techniques which model different reasoning methods; these include backward and forward chaining; some operate with both.

## 1.46 Information Systems Control and Audit

- A **forward-chaining mechanism** first examines the KB and the problem at hand; then, it attempts to discover a solution. For instance, a medical Expert System may be used to examine a patient's symptoms and provide a diagnosis based on the symptomology, the Expert System might locate several diseases that the patient may have.
- With **backward chaining**, on the other hand, the Inference Engine starts with a hypothesis or goal, which it then checks against the facts and rules in the knowledge base for consistency. So, for instance, the Expert System might be given the goal to "find this patient's disease(s) and would work back from there, asking questions as necessary to confirm or a refute candidate diagnoses".

### (iii) Knowledge Acquisition Subsystem (KAS)

The Knowledge Acquisition Subsystem is the software component of an Expert System that enables the Knowledge Engineer (KE) a specialized systems analyst responsible for designing and maintaining the expert System to build and refine an expert systems knowledge base. The KE works with the knowledge acquisition subsystem to model decision logic, derive industries and update the knowledge base.

Knowledge base development and maintenance can be done using special, reasonably user-friendly software. This software provides a convenient and efficient means of capturing and storing the contents of the knowledge base. Users are often presented with easy-to-operate menus and templates for entering rules, facts and relationship among facts. Once these are entered the software correctly stores the information in the knowledge base. Such software notes it much easier and less expensive to develop, update and refine the KB.

### (iv) User Interface

A user interface is the method by which an expert system interacts with a user. These can be through dialog boxes, command prompts, forms, or other input methods. Some expert systems interact with other computer applications, and do not interact directly with a human. In these cases, the expert system will have an interaction mechanism for transactions with the other application, and will not have a user interface.

In most instances, the Expert System prompts the user to supply information about the problem and the user types in the requested data. The data entered are examined by the interface engine and compared to the facts, rules and relationships in the knowledge base. This examination and comparison process results in the system continuing to prompt the user for more information until the system has enough data about the current problem so that it can reach a conclusion. Thus the user interface for an Expert System is highly interactive.

## 1.11 OFFICE AUTOMATION SYSTEMS (OAS)

**Office Automation System (OAS)** are among the newest and most rapidly expanding computer based information systems. Different office activities can be broadly grouped into the following types of operations:

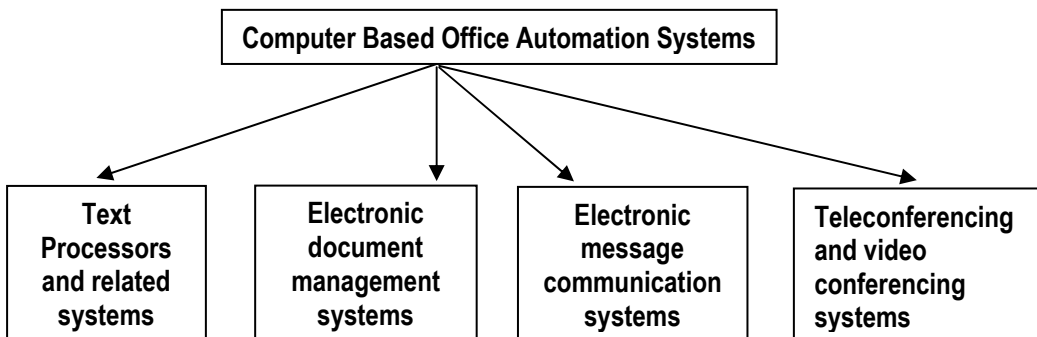
- (i) **Document Capture** : Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- (ii) **Document Creation** : This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- (iii) **Receipts and Distribution** : This basically includes distribution of correspondence to designated recipients.
- (iv) **Filling, Search, Retrieval and Follow up** : This is related to filling, indexing, searching of documents, which takes up significant time.
- (v) **Calculations** : These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- (vi) **Recording Utilization of Resources** : This includes, where necessary, record keeping in respect to specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

**Benefits of Office Automation Systems**

- (i) Office Automation Systems improve communication within an organization and between organizations.
- (ii) Office Automation Systems reduce the cycle time between preparation of messages and receipt of messages at the recipients' end.
- (iii) Office Automation Systems reduce the costs of office communication both in terms of time spent by executives and cost of communication links.
- (iv) Office Automation Systems ensure accuracy of communication flows.

Fig. 1.11.1 depicts categories of Computer based Office Automation systems.



**Fig 1.11.1 : Building Blocks of Office Automation Systems**

Each of these Office Automation Systems are briefly described as follows:

## **1.48 Information Systems Control and Audit**

### **1.11.1 Text Processing Systems**

- Text processing systems are the most commonly used components of the OAS. This is so because a large proportion of the office communication takes place in writing using words of a natural language.
- Text processing systems automate the process of development of documents such as letters, reports, memos etc. They permit use of standard stored information to produce personalized documents. Such automation reduces keying effort and minimizes the chances of errors in the document.
- The text processor may be simple word processing systems or desktop publishing systems. The desktop publishing systems help in quick production of multiple copies of the document with quality printing.
- The desktop publishing systems are often supported with laser printers, inkjet printers, scanners and other such devices for producing good quality documents.

### **1.11.2 Electronic Document Management Systems**

- The computer based document management systems are at capturing the information contained in documents, stored for future reference and communicate the relevant parts to the users as and when required. These systems are linked to the office automation systems such as text processors, electronic message communication systems etc.
- These systems are very useful in remote access of documents that is almost impossible with manual document management systems, For example, a customer may have a complaint concerning delivery of goods not being in accordance with the delivery instructions in the order. The computer based document management system would enable the executive to access the document through his notebook computer connected to any telephone line and show it to the customer, his order document in the office.
- In the case of internal communication document management systems can prove to be very useful. For example, the loan application form filed in a branch of a bank can be accessed by the sanctioning officer for scrutiny at the head office or any office for scrutiny of loan proposals.
- With computer based document management systems, location of the executive becomes irrelevant for access to documents. Thus, these systems can be very useful in an office environment where traveling executives share work space in the office.

### **1.11.3 Electronic Message Communication Systems**

Business enterprises have been using a variety of communication systems for finding and receiving messages. These include telephone, mail and facsimile (Fax), etc. The computer based message communication systems offer a lot of economy not only in terms of reduced time in sending or receiving the message but also in terms of reliability of the message and cost of communication.

## Components of Message Communication Systems

The three basic components based message communication systems are as follows :

(i) **Electronic Mail** : Various features of electronic mail are stated below :

- **Electronic transmission** : The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.
- **Online development and editing** : The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- **Broadcasting and Rerouting** : Email permits sending a message to a large number of target recipients. Thus it is easy to send a circular to all branches of a bank using Email resulting in a lot of saving of paper. The email could be rerouted to people having direct interest in the message with or without changing or and appending related information to the message.
- **Integration with other information systems** : The E-mail has the advantage of being integrated with the other information systems. Such an integration helps in ensuring that the message is accurate and the information required for the message is accessed quickly.
- **Portability** : Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal computer equipped with the relevant communication hardware, software and link facilities.
- **Economical** : The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode of sending messages. Since the speed of transmission is increasing, the time cost on communication media per page is falling further, adding to the popularity of email. The email is proving to be very helpful not only for formal communication but also for informal communication within the business enterprise.

(ii) **Facsimile (Fax)**

**Facsimile (Fax)** is electronic communication of images of documents over telephone lines. The computer based fax technology automates fax communication and permits sharing of fax facilities. It 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, similarly, the managers in an enterprise can leave the fax messages to the server which will send it to the intended recipient automatically.

## 1.50 Information Systems Control and Audit

### (iii) Voice Mail

**Voice mail** a variation of the email in which messages are transmitted as digitized voice. The recipient of the voice mail has to dial a voice mail service or access the e-mail box using the specified equipment and he can hear the spoken message in the voice of the sender. The secured type of voice mail service may require the recipient to enter identification code before the access is granted to the stored information.

### 1.11.4 Teleconferencing and Video-conferencing Systems

Teleconferencing is conducted a business meeting involving more than two persons located at two or more different places. The teleconferencing helps in reducing the time and cost of meeting as the participants do not have to travel to attend the meeting. Teleconferencing may be audio or video conferencing with or without use of computer systems.

The computer based teleconferencing has the advantage of flexibility in terms of pre-recorded presentations and integration with other information systems. These systems are based on Personal computers featuring a digital camera and run on a visual communication software. The communication links are still quite expensive making the desktop video conferencing useful only for selected applications.

### References :

1. Davis Olson, Second Edition, Management Information Systems, Mcgraw Hill.
2. Charles Parker & Thomas Case, Management Information System Strategy & Action, II<sup>nd</sup> Edition, Mcgraw Hill, 1993.

### Self - Examination Questions

1. Define following terms :
  - (i) System
  - (ii) System Boundary
  - (iii) Subsystem
  - (iv) System Environment
  - (v) Entropy
2. Differentiate between the following :
  - (i) Deterministic and Probabilistic systems
  - (ii) Open and Closed systems
  - (iii) Sub-system and Supra-system
  - (iv) Manual System and Automated System.
  - (v) Executive Information System and Traditional Information systems



- (vi) Internal Information and External Information
  - (vii) Programmed Decisions and non-programmed decisions
3. Explain the concept of decomposition with the help of an example.
  4. What do you mean by Information? Discuss various attributes of information.
  5. Explain various types of information systems at various levels of management.
  6. What is Decision Support System? Explain, in brief, various characteristics of a DSS.
  7. What are the four basic components of a DSS? Explain them.
  8. Discuss ERP systems, its model and limitations.
  9. What is an Executive Information System?
  10. What role do executives play in decision making?
  11. Discuss the characteristics of the information used in decision making?
  12. What purposes are served by an EIS?
  13. What are Office Automation Systems and its categories. Explain in detail.
  14. Discuss Expert systems in detail.
  15. What do you understand by Operations Support Systems. Discuss its categories in detail.
  16. Discuss Computer based information System and its components in detail with example.
  17. What do you understand by Transaction Processing System (TPS)? Discuss in detail.
  18. Define Management Information System (MIS) Discuss characteristics of MIS.
  19. What are the various misconceptions or myths about MIS.
  20. What are the pre-requisites of an effective MIS.
  21. How does use of computers in MIS effect an organizations performance.
  22. How do you categorize Management Support Systems.

# SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY

---

## LEARNING OBJECTIVES :

- To introduce the general concepts of various approaches of systems development, their framework, advantages and disadvantages.
- To explain in detail the phases involved in Systems Development Life Cycle.
- To understand the key issues while acquiring or developing system for achieving goals set.
- To discuss in detail various System Development Tools like – DFD, Decision Tree, Flowcharts etc.
- To understand an organizational structure of an IT Department.

## 2.1 INTRODUCTION

Computer information systems serve many different purposes, ranging from the processing of business transactions - to provide information needed to decide recurring issues, assisting senior officials with difficult strategy formulation, and linking office information and corporate data. But how do such complex information systems come into existence? Of course, through people. Technology has developed at a rapid pace but the most important aspect of any system is human know-how and the use of ideas to harness the computer so that it performs the required tasks. This process is essentially what system development is all about. To be of any use, a computer-based information system must function properly, be easy to use, and suit the organization for which it has been designed. If a system helps people to work more efficiently they will use it. If not, they will surely avoid it.

## 2.2 SYSTEMS DEVELOPMENT PROCESS

In business, systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods. System development can generally be thought of as having two major components : **System Analysis** and **System Design**.

- **System Analysis** is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.

## 2.2 Information Systems Control and Audit

- **System Design** is the process of planning a new business system or one to replace or complement an existing system.

But before planning can be done, one must thoroughly understand the old system and determine how computers can be used (if at all) to make its operation more effective.

**Example :** Consider stockroom operations of a clothing store. What measures can be taken to control its inventory and gain access to more up-to-date information about stock levels and reordering in a better way.

**Solution :** The Stores Manager asks a System Analyst to organize the stockroom operations.

Before an analyst can design a system to capture data, update files and produce reports, he needs to know more about :

- how the store currently operates,
- what forms are being used to store information manually, such as requisitions, purchase orders and invoices etc,
- what reports are being produced and how they are being used, etc.

To proceed, an analyst seeks information about lists of reorder notices, outstanding purchase orders, records of stock on hand, and other reports. He tries to understand how the existing system works and more specifically what the flow of information through the system looks like and assesses as carefully as possible, what the future need of the system will be and what changes should be considered to meet these needs. He may recommend alternatives for improving the situation which then management decides to accept or reject. The plan includes all system design features, file specifications, operating procedures, and design features, and equipment and personnel requirements. The system design is like the blue print for a building, it specifies all the features that should be there in the finished product.

### 2.2.1 Achieving System Development Objectives

There are many reasons why organizations fail to achieve their systems development objectives. Some of them are as follows :

- *Lack of senior management support and involvement in information systems development.* Developers and users of information systems watch senior management to determine which systems development projects are important and act accordingly by shifting their efforts away from any project which is not receiving management attention. In addition, management can see that adequate resources, as well as budgetary control over use of those resources, are dedicated to the project.
- *Shifting user needs.* User requirements for information technology are constantly changing. As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purposes might change since the development process began.

- *Development of strategic systems.* Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.
- *New technologies.* When an organization tries to create a competitive advantage by applying advance Information technology, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.
- *Lack of standard project management and systems development methodologies.* Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- *Overworked or under-trained development staff.* In many cases, systems developers often lack sufficient education background. Furthermore, many companies do little to help their development personnel stay technically sound. Currently in these organizations, a training plan and training budget do not exist.
- *Resistance to change.* People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- *Lack of user participation.* Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps reduce user resistance to change.
- *Inadequate testing and user training.* New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.

To overcome these and other problems, organizations must execute the systems development process efficiently and effectively.

### 2.2.2 System Development Team

Several people in the organization are responsible for systems development. In large systems, the worth of a particular project is typically decided by a top management level steering committee, usually consisting of a group of key Information Systems services users that acts as a review body for Information Systems plans and applications development. The steering committee ensures that ongoing systems development activities are consistently aimed at satisfying the information requirements of managers and users within the organization. A project management team generally consists of both computer professionals and key users. System analysts are subsequently assigned to determine user requirements, design the system and assist in development and implementation activities. In any systems organization, however, systems designers take a lead role during the design, development and implementation stages.

## 2.4 Information Systems Control and Audit

In end-user developed systems, the end-user is ultimately responsible for the system. Generally, the end-user seeks guidance from information centre personnel while developing the system.

### 2.2.3 Accountants' involvement in Development work

Most accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization who can combine knowledge of IT, business, accounting, and internal control, as well as behavior and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

## 2.3 SYSTEMS DEVELOPMENT METHODOLOGY

A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations. The methodology is characterized by the following:

- The project is divided into a number of identifiable processes, and each process has a starting point and an ending point. Each process comprises several activities, one or more deliverables, and several management control points. The division of the project into these small, manageable steps facilitates both project planning and project control.
- Specific reports and other documentation, called **Deliverables** must be produced periodically during system development to make development personnel accountable for faithful execution of system development tasks.
- Users, managers, and auditors are required to participate in the project which generally provide approvals, often called signoffs, at pre-established management control points. Signoffs signify approval of the development process and the system being developed.
- The system must be tested thoroughly prior to implementation to ensure that it meets users' needs.
- A training plan is developed for those who will operate and use the new system.
- Formal program change controls are established to preclude unauthorized changes to computer programs.
- A post-implementation review of all developed systems must be performed to assess the effectiveness and efficiency of the new system and of the development process.

**Approaches to System Development** : Since organizations vary significantly in the way they automate their business procedures, and since each new type of system usually differs from any other, several different system development approaches are often used within an organization.

All these approaches are not mutually exclusive, which means that it is possible to perform some prototyping while applying the traditional approach. These approaches are as follows :

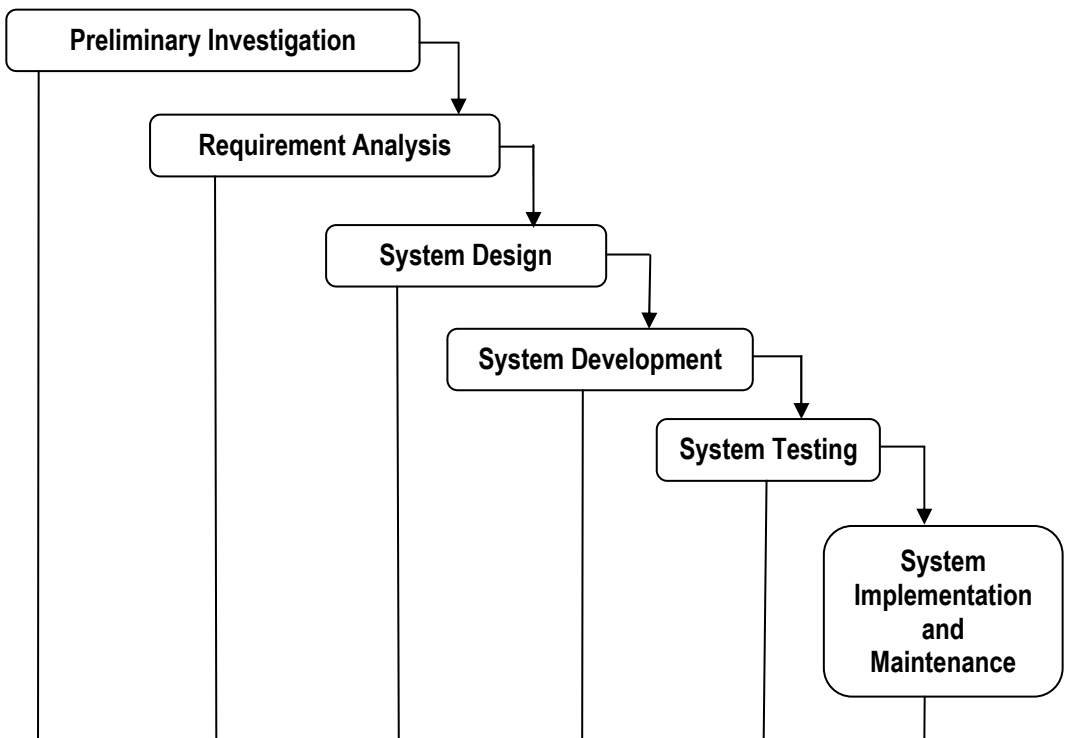
- (i) **Waterfall** : Linear framework type
- (ii) **Prototyping** : Iterative framework type
- (iii) **Incremental** : Combination of linear and iterative framework type
- (iv) **Spiral** : Combination linear and iterative framework type
- (v) **Rapid Application Development (RAD)** : Iterative Framework Type
- (vi) **Agile Methodologies**

**2.3.1 The Traditional / Waterfall Approach / Sequential Approach**

The waterfall approach is a traditional development approach in which each developer in a development team works in different phases. These phases include requirement analysis, specifications and design requirements, coding, final testing, and release. The waterfall approach is used on small projects because it eliminates testing to identify problems early in the process.

In the traditional approach of system development, activities are performed in sequence. Fig. 2.3.1 shows examples of the tasks performed during each phase of the traditional approach. When the traditional approach is applied, an activity is undertaken only when the prior step is fully completed.

**Overview of WaterFall Model**



**Fig. 2.3.1 : Steps in Traditional Approach**

## 2.6 Information Systems Control and Audit

**Framework type :** Linear

### **Basic Principles**

- (i) Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- (ii) Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- (iii) Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

### **Strengths**

- (i) Ideal for supporting less experienced project teams and project managers or project teams whose composition fluctuates.
- (ii) An orderly sequence of development steps and design reviews help ensure the quality, reliability, adequacy and maintainability of the developed software.
- (iii) Progress of system development is measurable.
- (iv) Conserves resources.

### **Weaknesses**

- (i) Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- (ii) Project progresses forward, with only slight movement backward.
- (iii) Little room for use of iteration, which can reduce manageability if used.
- (iv) Depends upon early identification and specification of requirements, yet users may not be able to clearly define what they need early in the project.
- (v) Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- (vi) Problems are often not discovered until system testing.
- (vii) System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- (viii) Difficult to respond to changes. Changes that occur later in the life cycle are more costly and are thus discouraged.
- (ix) Produces excessive documentation and keeping it updated as the project progresses is time-consuming.
- (x) Written specifications are often difficult for users to read and thoroughly appreciate.
- (xi) Promotes the gap between users and developers with clear vision of responsibility.

### 2.3.2 The Prototyping Model

The traditional approach sometimes may take years to analyze, design and implement a system. In order to avoid such delays, organizations are increasingly using prototyping techniques to develop smaller systems such as DSS, MIS and Expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system. As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

**Framework type :** Iterative.

**Basic Principles :** Prototyping can be viewed as a series of four steps, depicted in Fig. 2.3.2 wherein Implementation and Maintenance phases take place once the prototype model is tested and found to be meet uses' requirements.

**Step 1 - Identify Information System Requirements :** In traditional approach, the system requirements have to be identified before the development process starts. However, under prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis.

**Step 2 - Develop the Initial Prototype :** In this step, the designers create an initial base model and give little or no consideration to internal controls, but instead emphasize such system characteristics such as simplicity, flexibility, and ease of use. These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents. The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.

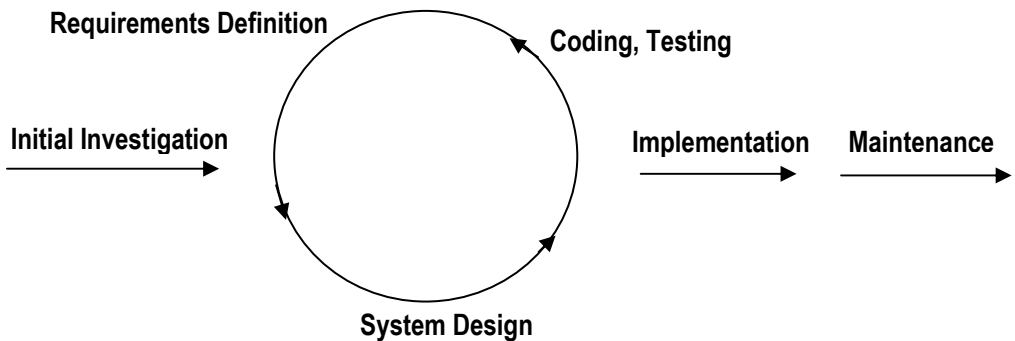
**Step 3 - Test and Revise :** After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system users for reevaluation. Thus iterative process of modification and reevaluation continues until the users are satisfied.

**Step 4 - Obtain User Signoff of the Approved Prototype :** At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide.

Prototyping is not commonly used for developing traditional applications such as accounts receivable, accounts payable, payroll, or inventory management, where the inputs, processing, and outputs are well known and clearly defined.



## 2.8 Information Systems Control and Audit



**Fig. 2.3.2 : Prototyping Model**

### Strengths

- (i) Improves both user participation in system development and communication among project stakeholders.
- (ii) Especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
- (iii) Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- (iv) Helps to easily identify confusing or difficult functions and missing functionality.
- (v) May generate specifications for a production application.
- (vi) Encourages innovation and flexible designs.
- (vii) Provides quick implementation of an incomplete, but functional, application.
- (viii) Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
- (ix) A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- (x) Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

### Weaknesses

- (i) Approval process and control are not strict.
- (ii) Incomplete or inadequate problem analysis may occur whereby only the most obvious and superficial needs will be addressed, resulting in current inefficient practices being easily built into the new system.

- (iii) Requirements may frequently change significantly.
- (iv) Identification of non-functional elements is difficult to document.
- (v) Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design with narrow focus that limits future system potential.
- (vi) Prototype may not have sufficient checks and balances incorporated.
- (vii) Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system developers with change suggestions. The users may not be able or willing to spend the amount of time required under the prototyping approach.
- (viii) The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
- (ix) Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by users when they have to go through too many interactions of the prototype.

In spite of above listed limitations, to some extent, systems analysis and development has been greatly improved by the introduction of prototyping. Prototyping enables the user to take an active part in the systems design, with the analyst acting in an advisory role. Prototyping makes use of the expertise of both the user and the analyst, thus ensuring better analysis and design, and prototyping is a crucial tool in that process.

### 2.3.3 The Incremental Model

**Framework Type :** Combination Linear and Iterative.

**Basic Principles :** The Incremental build model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is defined as finished when it satisfies all of its requirements. This model combines the elements of the waterfall model with the iterative philosophy of prototyping.

The product is decomposed into a number of components, each of which are designed and built separately (termed as builds). Each component is delivered to the client when it is complete. This allows partial utilization of product and avoids a long development time. It also creates a large initial capital outlay with the subsequent long wait avoided. This model of development also helps ease the traumatic effect of introducing completely new system all at once.

- (i) A series of mini-waterfalls are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.

## 2.10 Information Systems Control and Audit

or

- (ii) Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.

or

- (iii) The initial software concept, requirement analysis, and design of architecture and system core are defined using the Waterfall approach, followed by iterative Prototyping, which culminates in installation of the final prototype (ie. Working system).

Fig. 2.3.3 depicts the Incremental Model.

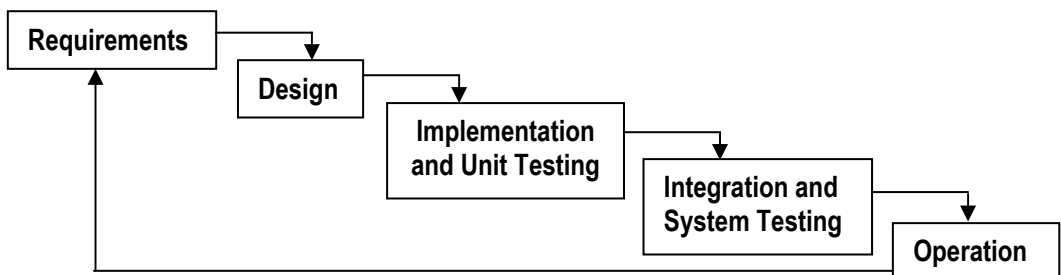


Fig. 2.3.3 : Incremental Model

### Strengths

- (i) Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
- (ii) Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval/signoff by the user and information technology management at designated major milestones.
- (iii) Stakeholders can be given concrete evidence of project status throughout the life cycle.
- (iv) More flexible – less costly to change scope and requirements.
- (v) Helps to mitigate integration and architectural risks earlier in the project.
- (vi) Allows delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
- (vii) Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organization is negatively impacted.

### Weaknesses

- (i) When utilizing a series of mini-waterfalls for a small part of the system before moving onto the next increment, there is usually a lack of overall consideration of the business problem and technical requirements for the overall system.
- (ii) Each phase of an iteration is rigid and do not overlap each other.

- (iii) Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
- (iv) Since some modules will be completed much earlier than others, well-defined interfaces are required.
- (v) Difficult problems tend to be purchased to the future to demonstrate early success to management.

#### **2.3.4 Spiral Model**

**Framework Type :** Combination Linear and Iterative.

**Basic Principles :** The Spiral model is a software development process combining elements of both design and prototyping-in-stages, in an effort to combine advantages of top-down and bottom-up concepts. Also known as the Spiral Lifecycle, it is a Systems Development Method (SDM) which combines the features of the prototyping model and the waterfall model. The spiral model is intended for large, expensive and complicated projects.

- (i) The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.
- (ii) A preliminary design is created for the new system. This phase is the most important part of "Spiral Model" in which all possible alternatives, that can help in developing a cost effective project are analyzed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.
- (iii) A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
- (iv) A second prototype is evolved by a fourfold procedure :
  - evaluating the first prototype in terms of its strengths, weaknesses, and risks;
  - defining the requirements of the second prototype;
  - planning and designing the second prototype;
  - constructing and testing the second prototype.

Game development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

## 2.12 Information Systems Control and Audit

### Strengths

- (i) Enhance risk avoidance.
- (ii) Useful in helping to select the best methodology to follow for development of a given software iteration based on project risk.
- (iii) Can incorporate Waterfall, Prototyping, and Incremental methodologies as special cases in the framework, and provide guidance as to which combination of these models best fits a given software iteration, based upon the type of project risk. For example, a project with low risk of not meeting user requirements but high risk of missing budget or schedule targets would essentially follow a linear Waterfall approach for a given software iteration. Conversely, if the risk factors were reversed, the Spiral methodology could yield an iterative prototyping approach.

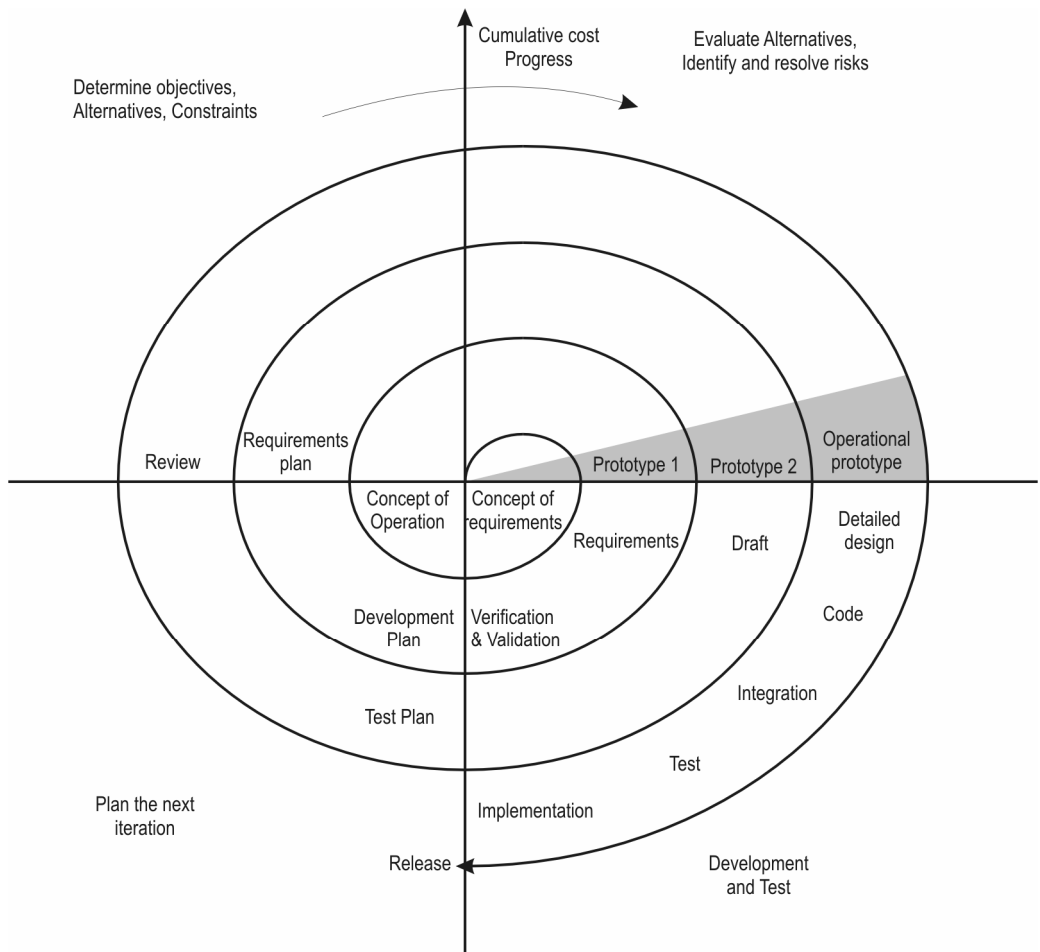


Fig. 2.3.4 : Spiral Model( Boehm 1988)

## Weaknesses

- (i) Challenges to determine the exact composition of development methodologies to use for each iteration around the Spiral.
- (ii) Highly customized to each project, and thus is quite complex, limiting reusability.
- (iii) A skilled and experienced project manager required to determine how to apply it to any given project.
- (iv) No established controls for moving from one cycle to another cycle. Without controls, each cycle may generate more work for the next cycle.
- (v) No firm deadlines - cycles continue with no clear termination condition, so there is an inherent risk of not meeting budget or schedule.

### 2.3.5 Rapid Application Development (RAD)

**Framework Type :** Iterative.

**Basic Principles :** Rapid Application Development (RAD) refers to a type of software development methodology which uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements.

- (i) Key objective is for fast development and delivery of a high quality system at a relatively low investment cost,
- (ii) Attempts to reduce inherent project risk by breaking a project into smaller segments and providing more ease-of-change during the development process.
- (iii) Aims to produce high quality systems quickly, primarily through the use of iterative Prototyping (at any stage of development), active user involvement, and computerized development tools. Graphical User Interface(GUI) builders, Computer Aided Software Engineering (CASE) tools, Database Management Systems (DBMS), Fourth generation programming languages, Code generators and object-oriented techniques etc.
- (iv) Key emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.
- (v) Project control involves prioritizing development and defining delivery deadlines or "timeboxes." If the project starts to slip, emphasis is on reducing requirements to fit the timebox, not in increasing the deadline.
- (vi) Generally includes **Joint Application Development (JAD)**, where users are intensely involved in system design, either through consensus building in structured workshops, or through electronically facilitated interaction.
- (vii) Active user involvement is imperative.
- (viii) Iteratively produces production software, as opposed to a throwaway prototype.

## 2.14 Information Systems Control and Audit

- (ix) Produces documentation necessary to facilitate future development and maintenance.
- (x) Standard systems analysis and design techniques can be fitted into this framework.

### Strengths

- (i) The operational version of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks.
- (ii) Because RAD produces systems more quickly and to a business focus, this approach tends to produce systems at lower cost.
- (iii) Quick initial reviews are possible.
- (iv) Constant integration isolate problems and encourage customer feedback.
- (v) Holds a great level of commitment from stakeholders, both business and technical, than Waterfall, Incremental, or spiral frameworks. Users are seen as gaining more of a sense of ownership of a system, while developer are seen as gaining more satisfaction from producing successful systems quickly.
- (vi) Concentrates on essential system elements from user viewpoint.
- (vii) Provides the ability to rapidly change system design as demanded by users.
- (viii) Produces a tighter fit between user requirements and system specifications.
- (ix) Generally produces a dramatic savings in time, money and human effort.

### Weaknesses

- (i) More speed and lower cost may lead to a lower overall system quality.
- (ii) Danger of misalignment of developed system with the business due to missing information.
- (iii) Project may end up with more requirements than needed (gold-plating).
- (iv) Potential for feature creep where more and more features are added to the system over the course of development.
- (v) Potential for inconsistent designs within and across systems.
- (vi) Potential for violation of programming standards related to inconsistent naming conventions and inconsistent documentation,
- (vii) Difficulty with module reuse for future systems.
- (viii) Potential for designed system to lack scalability.
- (ix) Potential for lack of attention to later system administration needs built into system.
- (x) High cost of commitment on the part if key user personnel.
- (xi) Formal reviews and audits are more difficult to implement than for a complete system.

- (xii) Tendency for difficult problems to be pushed to the future to demonstrate early success to management.
- (xiii) Since some modules will be completed much earlier than others, well –defined interfaces are required.

### 2.3.6 Agile Methodologies

All the methodologies described before are based on the premise that any software development process should be predictable and repeatable. One of the criticisms against these methodologies is that there is more emphasis on following procedures and preparing documentation. They are considered to be heavyweight or rigorous and are also criticized for their excessive emphasis on structure. There is a movement called **Agile Software Movement**, which provides a conceptual framework for undertaking software engineering projects.

Most agile methods attempt to minimize risk by developing software in short time boxes called **Iterations**. Software development being essentially a human activity, will always have variations in processes and inputs and the model should be flexible enough to handle the variations. Each iteration is like a miniature software project of its own, and includes all of the tasks necessary to release the mini-increment of new functionality : planning, requirements analysis, design, coding testing and documentation. While an iteration may not add enough functionality to warrant releasing the product, an agile software project intends to be capable of releasing new software at the end of every iteration.

For example - The entire set of software requirements cannot be known at the beginning of the project nor do they remain static. If the model cannot handle this dynamism, then there can be lot of wastage of effort or the final product may not meet the customer's needs. Hence the agile methodologies advocate the principle "**Build Short, Build Often**". That is, the given project is broken up into subprojects and each subproject is developed and integrated in to the already delivered system. This way the customer gets continuous delivery of useful and usable systems. The subprojects are chosen so that they have short delivery cycles, usually of the order of 3 to 4 weeks. The development team also gets continuous feedback.

Some of the Characteristics of Agile Methodology are as follows :

- Iterative with short cycles enabling fast verifications and corrections.
- Time bound iterative cycles.
- Modularity at development process level.
- People oriented.
- Collaborative and communicative working style.
- Incremental and convergent approach that minimizes risks and facilitates functional additions.

Some of the popular agile methodologies are - Scrum, FDD (Feature –Driven Development), Crystal and XP (Extreme Programming).



## 2.16 Information Systems Control and Audit

### 2.4 SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

The **System Development Life Cycle (SDLC)** framework provides system designers and developers to follow a sequence of activities. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.

The SDLC is document driven which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred to as deliverables. A deliverable may be a substantial written document, a software artifact, a system test plan or even a physical object such as a new piece of technology that has been ordered and delivered. This feature of the SDLC is critical to the successful management of an IS project.

The SDLC can also be viewed from a more process oriented perspective. This emphasizes the parallel nature of some of the activities and presents activities such as system maintenance as an alternative to a complete re-design of an existing system. The advantages of this system are as follows :

- Better planning and control by project managers.
- Compliance to prescribed standards ensuring better quality.
- Documentation that SDLC stresses on is an important measure of communication and control.
- The phases are important milestones and help the project manager and the user for review and signoff.

From the perspective of the IS Audit, the following are the possible advantages:

- (i) The IS auditor can have clear understanding of the various phases if the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- (ii) The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
- (iii) The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
- (iv) The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

#### **Risks Associated with SDLC**

Some of the shortcomings of the SDLC are as follows:

- (i) The development team may find it cumbersome.
- (ii) The users may find that the end product is not visible for a long time.
- (iii) The rigidity of the approach may prolong the duration of many projects.
- (iv) IT may not be suitable for small and medium sized projects.

The process of system development starts when management or sometimes system development personnel realize that a particular business system needs improvement. The System Development Life Cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system. In most business situations, these activities are all closely related, usually inseparable and even the order of the steps in these activities may be difficult to determine. Different parts of a project can be in various phases at the same time, with some components undergoing analysis while others are at advanced design stages.

Table 2.4.1 list all the phases involved in the System Development Life Cycle.

<b>PHASE NO.</b>	<b>PHASE NAME</b>	<b>NATURE OF ACTIVITY</b>
1.	Preliminary Investigation	Determining and evaluating the strategic benefits of the system and ensure that the solution fits the business strategy. Includes cost-benefit analysis of the proposed system.
2.	Systems Requirements Analysis	Analyzing the type of the system on the basis of the users requirements.
3.	Systems Design	Designing the system in terms of user interface data storage and data processing functions on the basis of the requirement phase by developing the system flowcharts, system and data flow diagrams, screens and reports.
4.	Systems Development/Programming	Programming the system as designed and conduct the continuous testing and debugging.
5.	Systems Testing	Various kinds of testing is conducted before the developed system is implemented. This includes Unit Testing, Integration Testing and System Testing etc.
6.	Systems Implementation	Final Testing and quality of controls audit, acceptance by management and user before migration of the system to the live environment and data conversion from legacy system to the new system.
7.	Post Implementation Review and Maintenance	Continuous evaluation of the system as it functions in the live environment and its updation. Maintenance includes continuous evaluation of the system as it functions in the live environment and its updation.

**Table 2.4.1 : Phases in System Development Life Cycle**

## 2.18 Information Systems Control and Audit

### 2.5 THE PRELIMINARY INVESTIGATION

**Objective :** To determine and analyze the strategic benefits in implementing the system through evaluation and quantification of - productivity gains; future cost avoidance; cost savings, and Intangible benefits like improvement in morale of employees.

A preliminary investigation is normally initiated by some sort of system request. The steps involved in the preliminary investigation phase are as follows :

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

The following issues are typically addressed in the Feasibility Study:

- (i) Determine whether the solution is as per the business strategy.
- (ii) Determine whether the existing system can rectify the situation without a major modification.
- (iii) Define the time frame for which the solution is required.
- (iv) Determine the approximate cost to develop the system.
- (v) Determine whether the vendor product offers a solution to the problem.

**Document / Deliverable :** A preliminary investigation report/ feasibility study for management.

#### 2.5.1 Identification of Problem

The first step in an application development is to define the problem clearly and precisely which is done only after several rounds of discussions with the user group. Then its prevalence within the organization has to be assessed. A problem that has a considerable impact on the organization is likely to receive immediate management attention. User involvement will also be high, if they are convinced that the proposed solution will resolve the problem.

For instance, personnel in a functional area may feel that an existing system is outdated or a manager might want access to specific new information that he claims will lead to better decisions. Shifting business requirements, changing organizational environments, and evolving information technology may render systems ineffective or inefficient. Whatever may be the reason, managers and users may feel compelled to submit a request for a new system to the IS department. If the need seems genuine, a system analyst is assigned to make a preliminary investigation who submits all proposals to the steering committee for evaluation to identify those projects that are most beneficial to the organization.

Thus it can be concluded that the purpose of the preliminary investigation is to evaluate the project request. It is neither a designed study, nor it includes the collection of details to completely describe the business system. Rather it relates to collection of information that

permits committee members to evaluate the merits of the project request and make an informed judgment about the feasibility of the proposed project.

The analyst working on the preliminary investigation should accomplish the following objectives:

- Clarify and understand the project request.
- Determine the size of the project.
- Determine the technical and operational feasibility of alternative approaches.
- Assess costs and benefits of alternative approaches.
- Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.

### 2.5.2 Identification of Objective

After the identification of the problem, it is easy to work out the objectives of the proposed solution. For instance, inability to provide a convenient reservation system, for a large number of intending passengers was the problem of the Railways. So its objective was “to introduce a system wherein intending passengers could book a ticket from source to destination, faster than in real-time.”

### 2.5.3 Delineation of Scope

The scope of a solution defines its boundaries. It should be clear and comprehensible to the user management stating what will be addressed by the solution and what will not. Often the scope becomes a contentious issue between development and user organizations. Hence, outlining the scope in the beginning is essential.

The following questions should be answered while stating the scope:

- Functionality requirements** : What functionalities will be delivered through the solution?
- Data to be processed** : What data is required to achieve these functionalities?
- Control requirements** : What are the control requirements for this application?
- Performance requirements** : What level of response time, execution time and throughput is required?
- Constraints** : What are the conditions the input data has to conform to? For example, what is the maximum number of characters that a name can have in a database?
- Interfaces** : Is there any special hardware/software that the application has to interface with? For example-Payroll application may have to capture from the attendance monitoring system that the company has already installed. Then the solution developer has to understand the format of data, frequency mode of data transfer and other aspects of the software.
- Reliability requirements** : Reliability of an application is measured by its ability to remain uncorrupted in the face of inadvertent / deliberate misuse. The reliability required for an application depends on its criticality and the user profile.

## 2.20 Information Systems Control and Audit

While eliciting information to delineate the scope, few aspects need to be kept in mind:

- Different users will represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project, addressing his concerns should be the basis of the scope.
- While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
- While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. For example - when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.
- It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities. Solutions which have a wide impact are likely to meet with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle this have had a very poor ERP implementation record, with disastrous consequences.
- While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weight-age too. These factors have to be considered from the perspective of the user management and resolved. For example- in a security system, how foolproof it is, may be a critical a factor like the economic benefits that entail.

The two primary methods with the help of which the scope of the project can be analyzed are as follows :

- (i) **Reviewing internal documents** : The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, the analyst will try to know how the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
- (ii) **Conducting Interviews** : Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.

### 2.5.4 Feasibility Study

After possible solution options are identified, project feasibility - the likelihood that these systems will be useful for the organization – is determined. A feasibility study is carried out by the system analysts which refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The Feasibility Study of a system is evaluated under following dimensions :

- **Technical** : Is the technology needed available?
  - **Financial** : Is the solution viable financially?
  - **Economic** : Return on Investment?
  - **Schedule / Time** : Can the system be delivered on time?
  - **Resources** : Are human resources reluctant for the solution?
  - **Operational** : How will the solution work?
  - **Behavioral** : Is the solution going to bring any adverse effect on quality of work life?
  - **Legal** : Is the solution valid in legal terms?
- (i) **Technical Feasibility** : It is concerned with issues pertaining to hardware and software. Essentially, an analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:
- Does the necessary technology exist to do what is suggested (and can it be acquired)?
  - Does the proposed equipment have the technical capacity to hold the data required to use the new system?
  - Can the proposed application be implemented with existing technology?
  - Will the proposed system provide adequate responses to inquires, regardless of the number or location of users?
  - Can the system be expanded if developed?
  - Are there technical guarantees of accuracy, reliability, ease of access, and data security?

## 2.22 Information Systems Control and Audit

Some of the technical issues to be considered are given in the Table 2.5.1 below.

Design Considerations	Design Alternatives
• Communications channel configuration	• Point to point, multidrop, or line sharing
• Communications channels	• Telephone lines, coaxial cable, fiber optics, microwave, or satellite
• Communications network	• Centralized, decentralized, distributed, or local area
• Computer programs	• Independent vendor or in-house
• Data storage medium	• Tape, floppy disk, hard disk, or hard copy
• Data storage structure	• Files or database
• File organization and access	• Direct access or sequential files
• Input medium	• Keying, OCR, MICR, POS, EDI, or voice recognition
• Operations	• In-house or outsourcing
• Output frequency	• Instantaneous, hourly, daily, weekly, or monthly
• Output medium	• CRT, hard copy, voice, or turn-around document
• Output scheduling	• Pre-determined times or on demand
• Printed output	• Pre-printed forms or system-generated forms
• Processor	• Micro, mini, or mainframe
• Transaction processing	• Batch or online
• Update frequency	• Instantaneous, hourly, daily, weekly, or monthly

**Table 2.5.1 : Technical issues while Systems Design**

- (ii) **Financial Feasibility** : The solution proposed may be prohibitively costly for the user organization. For example – Monitoring the stock through VSAT network connecting multiple locations may be acceptable for an organization with high turnover. But this may not be a viable solution for smaller ones.
- (iii) **Economic Feasibility/Cost-Benefit Analysis** : It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. After problems or opportunities are identified, the analysts must determine the scale of

response needed to meet the user's requests for a new system, as well as the approximate amount of time and money that will be required in the effort. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- (i) The cost of conducting a full systems investigation.
- (ii) The cost of hardware and software for the class of applications being considered.
- (iii) The benefits in the form of reduced costs or fewer costly errors.
- (iv) The cost if nothing changes (i.e., the proposed system is not developed)

**Estimating costs and benefits :** After possible solution options are identified, an analyst should make a primary estimate of each solution's costs and benefits.

**Cost :** System costs can be sub divided into **Development, Operational and Intangible costs.**

- **Development costs** for a computer based information system include costs of the system development process such as - salaries of the system analysts and computer programmers who design and program the system; cost of converting and preparing data files and preparing systems manual and other supportive documents; cost of preparing new or expanded computer facilities; cost of testing and documenting the system, training employees, and other start up costs.
- **Operating costs** of a computer based information system include - hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel who will operate the new system; salaries of system analysts and computer programmers who perform the system maintenance function; cost of input data preparation and control; cost of data processing supplies; and Cost of maintaining proper physical facilities including power, light, heat, air conditioning, building rental or other facility charges and equipment and building maintenance charges, overhead charges of the business firm.
- **Intangible costs** are costs that cannot be easily measured. For example, the development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale. Customer sales and goodwill may be lost by errors made during the installation of a new system. Such costs are difficult to measure in rupees but are directly related to the introduction and operation of information system.

**Benefits :** The benefits which result from developing new or improved information systems that utilize EDP can be subdivided into tangible and intangible benefits. Tangible benefits are those that can be accurately measured and are directly related to the introduction of a new system, such as decrease in data processing cost. Intangible benefits such as improved business image are harder to measure and define.

- (iv) **Schedule or Time Feasibility :** Schedule feasibility involves the design team's estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee. For example, if a design team projects that it will take 16 months for a particular system design to become fully functional, the steering committee may reject the proposal in favor of a simpler alternative that the company can implement in a shorter time frame.



## 2.24 Information Systems Control and Audit

- (v) **Resources Feasibility** : This focuses on human resources. Implementing sophisticated software solutions becomes difficult in non-metro locations because of the reluctance of skilled personnel to move to such locations.
- (vi) **Operational Feasibility** : It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems. Some of the questions which help in testing the operational feasibility of a project are stated below :
- Is there sufficient support for the system from management and from users?
  - Are current business methods acceptable to users?
  - Have the users been involved in planning and development of the project?
  - Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control result in any areas? Will accessibility of information be lost?
  - Will individual performance be poorer after implementation than before?

This analysis may involve a subjective assessment of the political and managerial environment in which the system will be implemented. In general, the greater the requirements for change in the user environment in which the system will be installed, the greater the risk of implementation failure.

- (vii) **Behavioral Feasibility** : It refers to the systems which will be designed to process data and produce the desired outputs. However, if the data input for the system is not readily available or collectable, then the system may not be successful.
- (viii) **Legal Feasibility** : Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations. Any system, which violates the local legal requirements should also be rejected. For example, a revised system should comply with all applicable federal and state statutes about financial reporting requirements, as well as the company's contractual obligations.

**2.5.5 Reporting Results to Management** : After the analyst articulates the problem and its scope, he provides one or more solution alternatives and estimates the cost and benefits of each alternative, and reports these results to the management. The report should be accompanied by a short cover letter that summarizes the results and makes the recommendation regarding further procedures. From the analyst's report, management should determine what to do next. Not all projects submitted for evaluation and review are accepted. Requests that fail to pass feasibility test are not pursued further unless they are reworked and resubmitted as new proposals. In some cases, only a part of the project is actually unworkable and the steering committee may decide to combine the workable part of the project with another feasible proposal. In certain other cases, primary investigation produces new information to suggest that improvements in management and supervision, and not the development of information systems are the actual solutions to the reported problems.

## 2.6 SYSTEM REQUIREMENT ANALYSIS

**Objectives :** This phase includes a thorough and detailed understanding of the current system, identifies the areas that need modification to solve the problem, the determination of user/managerial requirements and to have fair idea about various systems development tools.

The following activities are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts.
- To analyze requirements to detect and correct conflicts and determine priorities.
- To verify the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.
- To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation.
- To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams.
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

**Document/Deliverable :** A systems requirements report.

### 2.6.1 Fact finding Techniques

Every system is built to meet some set of needs, for example, the need of the organization for lower operational costs, better information for managers, smooth operations for users or better levels of service to customers. To assess these needs, the analysts often interact extensively with the people, who will be benefited from the system, in order to determine what are their actual requirements. Various fact-finding techniques, which are used by the system analyst for determining these needs/ requirements, are briefly discussed below :

- (i) **Documents :** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
- (ii) **Questionnaires :** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.
- (iii) **Interviews :** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide systems developer with a

## 2.26 Information Systems Control and Audit

complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.

- (iv) **Observation** : In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed.

### 2.6.2 Analysis of the Present System

Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. There should be enough information assembled so that a qualified person can understand the present system without visiting any of the operating departments. Survey of existing methods, procedures, data flow, outputs, files, input and internal controls should be intensive in order to fully understand the present system and its related problems.

The following areas should be studied in depth:

- (i) **Review historical aspects** : A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate what system changes have occurred in the past including operations that have been successful or unsuccessful with computer equipments and techniques.
- (ii) **Analyze inputs** : A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, he will be able to determine how these inputs fit into the framework of the present system.
- (iii) **Review data files maintained** : The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all on-line and off-line files which are maintained in the organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
- (iv) **Review methods, procedures and data communications** : Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure review is

an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. A system analyst also needs to review and understand the present data communications used by the organization. He must review the types of data communication equipments including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must understand how the data-communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

- (v) **Analyze outputs** : The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting is used, how long it is kept on file, etc. must be investigated. Often many reports are a carry-over from earlier days and have little relevance to current operations. Attempt should be made to eliminate all such reports in the new system.
- (vi) **Review internal controls** : A detailed investigation of the present information system is not complete until internal control is reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.
- (vii) **Model the existing physical system and logical system** : As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the process must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- (viii) **Undertake overall analysis of present system** : Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of - the present work volume; the current personnel requirements; the present benefits and costs and each of these must be investigated thoroughly.

### 2.6.3 Systems Analysis of Proposed Systems

After each functional area of the present information system has been carefully analyzed, the proposed system specifications must be clearly defined which are determined from the desired objectives set forth at the first stage of the study. Likewise consideration should be given to the strengths and short comings of the present system. The required systems specifications which should be in conformity with the project's objectives are as follows :

- Outputs produced with great emphasis on timely managerial reports that utilize the management by exception' principle.

## 2.28 Information Systems Control and Audit

- Database maintained with great accent on online processing capabilities.
- Input data prepared directly from original source documents for processing by the computer system.
- Methods and procedures that show the relationship of inputs and outputs to the database, utilizing data communications where deemed appropriate.
- Work volumes and timings carefully considered for present and future periods including peak periods.

The starting point for compiling these specifications is output. After outputs have been determined, it is possible to infer what inputs, database, methods, procedures and data communications must be employed. The output-to-input process is recommended since outputs are related directly to the objectives of the organization. The future workload of the system must be defined for inputs, database and outputs in terms of average and peak loads, cycles and trends.

### 2.6.4 System Development Tools

Many tools and techniques have been developed to improve current information systems and to develop new ones. Such tools help end users and systems analysts to -

- conceptualize, clarify, document and communicate the activities and resources involved in the organization and its information systems.;
- analyze present business operations, management decision making and information processing activities of the organization;
- Propose and design new or improved information systems to solve business problems or pursue business opportunities that have been identified.

Many systems development tools take the form of diagrams and other graphic representations. The major tools used for system development can be grouped into four categories based on the systems features. These are as follows :

**(I) System components and flows :** These tools help the system analysts to document the data flow among the major resources and activities of an information system. System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities. A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements. A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by an information system.

**(II) User interface :** Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system. Layout forms and screens are used to construct the formats and contents of input/output media and methods. Dialogue flow diagrams analyze the flow of dialogue between computers and people. They document the flows among different display screens generated by alternative end user responses to menus and prompts.

**(III) Data attributes and relationships :** The data resources in information system are defined, catalogued and designed by this category of tools.

- A Data Dictionary catalogs the description of the attributes (characteristics) of all data elements and their relationships to each other as well as to external systems.
- Entity-relationship diagrams are used to document the number and type of relationship among the entities in a system.
- File layout forms document the type, size and names of the data elements in a system.
- Grid charts help in identifying the use of each type of data element in input/output or storage media of a system.

**(IV) Detailed system process :** These tools are used to help the programmer develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system. Structure charts document the purpose, structure and hierarchical relationships of the modules in a program.

We will now describe some of these tools in detail.

(a) **Structured English : Structured English**, also known as **Program Design Language (PDL)** or **Pseudo Code**, is the use of the English language with the syntax of structured programming. Thus, Structured English aims at getting the benefits of both the programming logic and natural language. Program logic that helps to attain precision and natural language that helps in getting the convenience of spoken languages.

**Structured English consists of the following elements:**

- (i) Operation statements written as English phrases executed from the top down.
- (ii) Conditional blocks indicated by keywords such as IF, THEN, and ELSE.
- (iii) Repetition blocks indicated by keywords such as DO, WHILE, and UNTIL.

**Some of the keywords that may be used are as follows :**

START, BEGIN, END, STOP, DO, WHILE, DO WHILE, FOR, UNTIL, DO UNTIL, REPEAT, END WHILE, END UNTIL, END REPEAT, IF, IF THEN, ELSE, IF ELSE, END IF, THEN, ELSE THEN, ELSE IF, SO, CASE, EQUAL, LT, LE, GT, GE, NOT, TRUE, FALSE, AND, OR, XOR, GET, WRITE, PUT, UPDATE, CLOSE, OPEN, CREATE, DELETE, EXIT, FILE, READ, EOF, EOT.

**Example 2.6.1 :** A bank will grant loan under the following conditions:

1. If a customer has an account with the bank and had no loan outstanding, loan will be granted.
2. If a customer has an account with the bank but some amount is outstanding from previous loans then loan will be granted if special approval is needed.
3. Reject all loan applications in all other cases.

Write the above conditions in structured language.

**Solution :** IF customer has a Bank Account THEN

IF Customer has no dues from previous account THEN

## 2.30 Information Systems Control and Audit

Allow loan facility

**ELSE**

**IF** Management Approval is obtained **THEN**

Allow loan facility

**ELSE**

Reject

**ENDIF**

**ENDIF**

**ELSE**

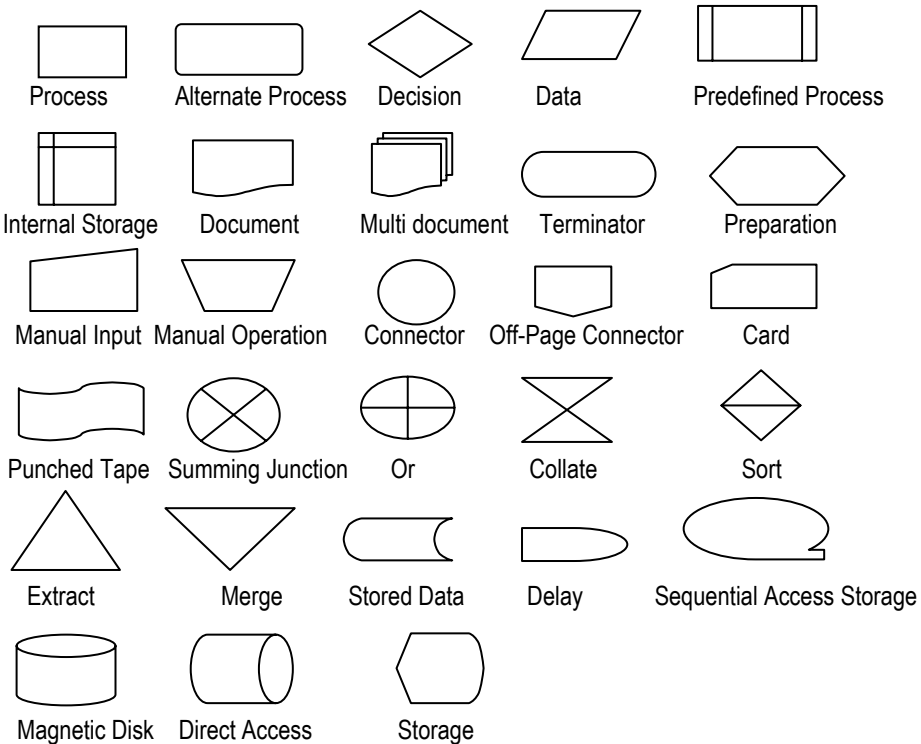
Reject

**ENDIF**

(b) **Flowcharts** : **Flowcharting** is a graphic technique that can be used by analysts to represent the inputs, outputs and processes of a business in a pictorial form. It is a common type of chart, that represents an algorithm or process showing the steps as boxes of various kinds, and their order by connecting these with arrows. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

### Symbols used in Flow charts

A typical flowchart may have the following kinds of symbols as shown in Fig. 2.6.1 :



**Fig . 2.6.1 : Standard Flowchart Symbols**

## Types of Flow charts

Generally, flowcharts are divided into four major categories:

- **Document flowchart**, showing a document flow through systems.
- **Data flowchart**, showing data flows in a system.
- **System flowchart**, showing controls at a physical or resource level.
- **Program flowchart**, showing the controls in a program within a system.

## Benefits of Flowchart

- **Communication** : Flowcharts are better way of communicating the logic of a system to all concerned.
- **Effective analysis** : With the help of flowchart, problem can be analyzed in more effective way.
- **Proper documentation** : Program flowcharts serve as a good program documentation, which is needed for various purposes.
- **Efficient Coding** : The flowcharts act as a guide or blueprint during the systems analysis and program development phase.
- **Proper Debugging** : The flowchart helps in debugging process.
- **Efficient Program Maintenance** : The maintenance of operating program becomes easy with the help of flowchart. It helps the programmer to put efforts more efficiently on that part.

## Limitations of Using Flowcharts

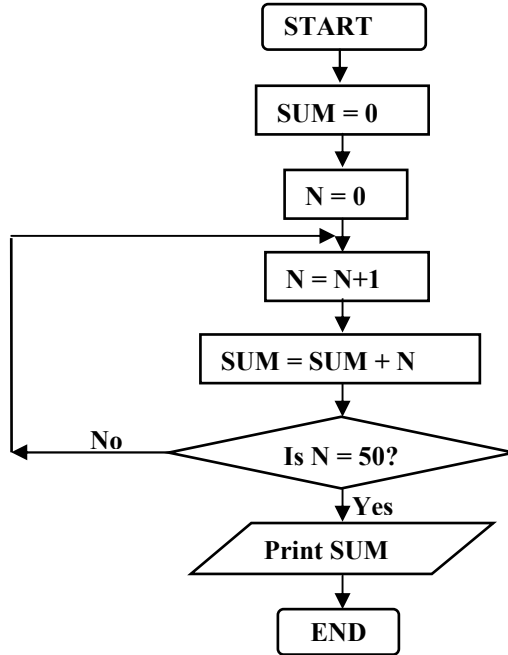
- **Complex logic** : Sometimes, the program logic is quite complicated. In that case, flowchart becomes complex and clumsy.
- **Alterations and Modifications** : If alterations are required the flowchart may require re-drawing completely.
- **Reproduction** : As the flowchart symbols cannot be typed, reproduction of flowchart becomes a problem.
- The essentials of what is done can easily be lost in the technical details of how it is done.



### 2.32 Information Systems Control and Audit

**Example 2.6.2 :** Draw a flowchart to find the sum of first 50 natural numbers.

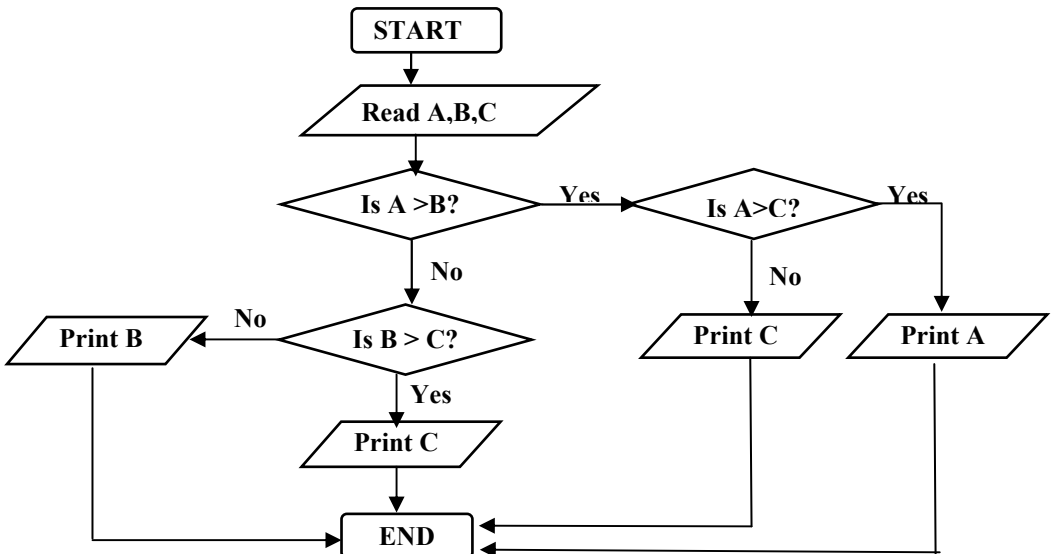
**Solution :** The required flowchart is given in Fig. 2.6.2.



**Fig. 2.6.2 :** Sum of first 50 natural numbers

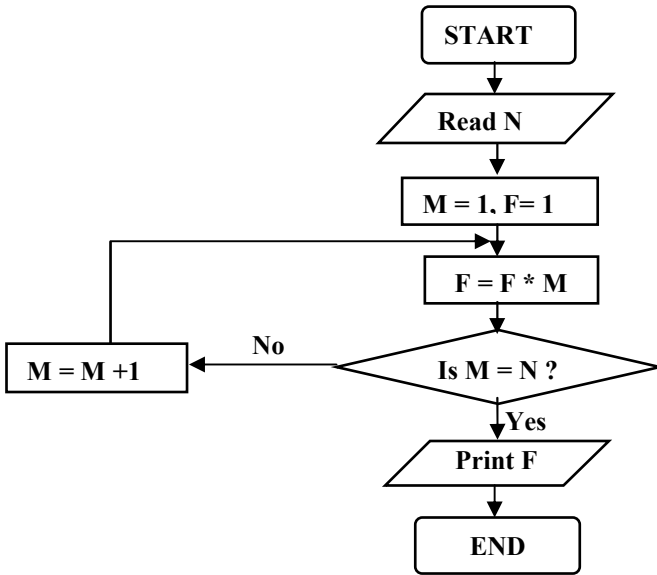
**Example 2.6.2 :** Draw a flowchart to find the largest of three numbers A, B and C.

**Solution :** The required flowchart is shown in Fig. 2.6.3.





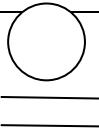

**Fig. 2.6.3 :** Flowchart for finding out the largest of three numbers

**Example 2.6.4 :** Draw a flowchart for computing factorial N (N!) where  $N! = 1 * 2 * 3 * \dots * N$ .  
**Solution :** The required flowchart has been shown in Fig. 2.6.4.



**Fig. 2.6.4 : Flowchart for computing factorial N**

(c) **Data Flow Diagrams :** A **Data Flow Diagram** uses few simple symbols to illustrate the flow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements. A DFD is composed of four basic elements : Data Sources and Destinations, Data Flows, Transformation processes, and Data stores shown in Table 2.6.1. These four symbols are combined to show how data are processed.

Symbol	Name	Explanation
	Data Sources and destinations	The people and organizations that send data to and receive data from the system are represented by square boxes called Data destinations or Data Sinks.
	Data flows	The flow of data into or out of a process is represented by curved or straight lines with arrows.
	Transformation process	The processes that transform data from inputs to outputs are represented by circles, often referred to as bubbles.
	Data stores	The storage of data is represented by two horizontal lines.

**Table 2.6.1 : Data Flow Diagram Symbols**

### 2.34 Information Systems Control and Audit

(d) **Decision Tree** : A **Decision Tree** (or tree diagram) is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. Decision tree is commonly used in operations research, specifically in decision analysis, to help identify a strategy most likely to reach a goal and to calculate conditional probabilities.

**Example 2.6.5** : David, a manager of a famous golf club is having some trouble with his customer attendance. There are days when everyone wants to play golf and the staff are overworked. On other days, for no apparent reason, no one comes to play golf. David's objective is to optimize staff availability by trying to predict when people will play golf. To accomplish that he needs to understand the reason people decide to play and if there is any explanation for that. He assumes that weather must be an important underlying factor, so he decides to use the weather forecast for the upcoming week. So during two weeks he has been recording:

- The outlook, whether it was sunny, overcast or raining.
- The temperature (in degrees Fahrenheit).
- The relative humidity in percent.
- Whether it was windy or not.
- Whether people attended the golf club on that day.

David compiled this dataset into a table containing 14 rows and 5 columns as shown in Table 2.6.2 below:

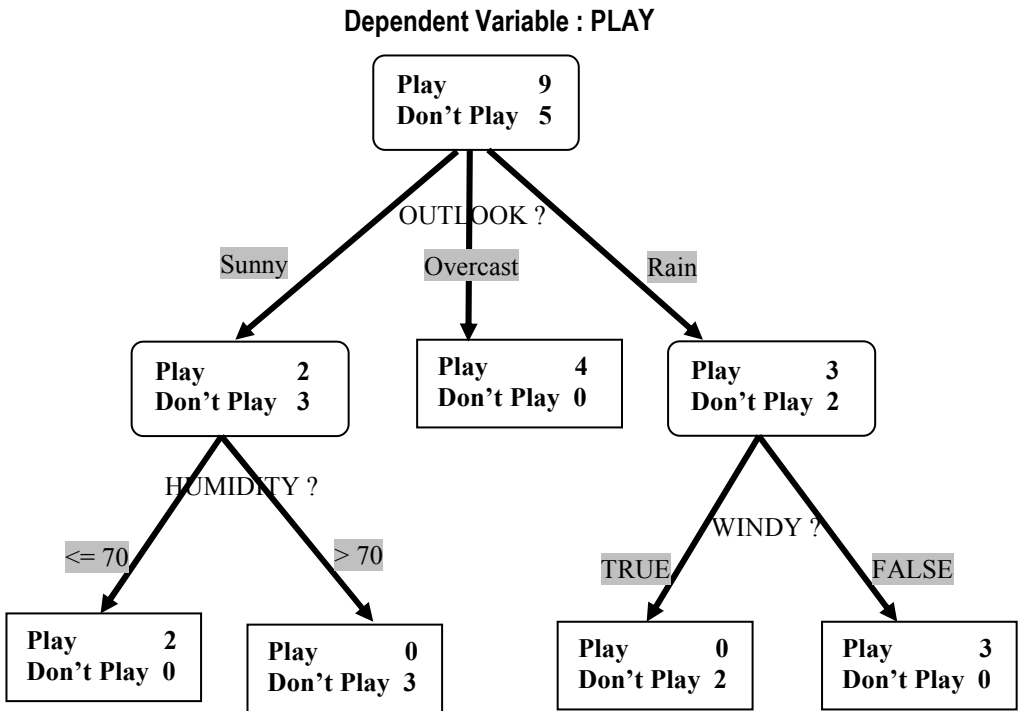
INDEPENDENT VARIABLES				DEPENDENT VARIABLES
OUTLOOK	TEMPERATURE	HUMIDITY	WINDY	PLAY
Sunny	85	85	False	Don't Play
Sunny	80	90	True	Don't Play
Overcast	83	78	False	Play
Rain	70	96	False	Play
Rain	68	80	False	Play
Rain	65	70	True	Don't Play
Overcast	64	65	True	Play
Sunny	72	95	False	Don't Play
Sunny	69	70	False	Play
Rain	75	80	False	Play
Sunny	75	70	True	Play
Overcast	72	90	True	Play
Overcast	81	75	False	Play
Rain	71	80	True	Don't Play

**Table 2.6.2 : PLAY GOLF DATASET**

He then applied a decision tree model to solve this problem as depicted in Fig. 2.6.5.

In the decision tree, the top node represents all the data. The classification tree algorithm concludes that the best way to explain the dependent variable, **Play**, is by using the variable **Outlook**. Using the categories of the variable outlook, three different groups were found:

- One that plays golf when the weather is sunny,
- One that plays when the weather is cloudy, and
- One that plays when it's raining.



**Fig. 2.6.5 : Decision Tree Model of Play Golf Dataset**

**David's first conclusion :** If the outlook is overcast people always play golf, and there are some fanatics who play golf even in the rain. Then he divided the sunny group in two. He realized that people don't like to play golf if the humidity is higher than seventy percent. Finally, he divided the rain category in two and found that people will also not play golf if it is windy.

And lastly, here is the short solution of the problem given by the classification tree : David dismisses most of the staff on days that are sunny and humid or on rainy days that are windy, because almost no one is going to play golf on those days. On days when lot of people will play golf, he hires extra staff. The conclusion is that the decision tree helped David turn a complex data representation into a much easier structure.

**2.36 Information Systems Control and Audit**

(e) **Decision Table** : A **Decision Table** is a table which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency. Decision tables are necessitated by the fact that branches of the flowchart multiply at each diamond (comparison symbol) and may easily run into scores and even hundreds. If, therefore, the programmer attempts to draw a flowchart directly, he is liable to miss some of the branches. The four parts of the decision table are as follows :

- (i) **Condition Stub** - which comprehensively lists the comparisons or conditions;
- (ii) **Action Stub** - which comprehensively lists the actions to be taken along the various program branches;
- (iii) **Condition entries** - which list in its various columns the possible permutations of answer to the questions in the conditions stub); and
- (iv) **Action entries** - which lists, in its columns corresponding to the condition entries the actions contingent upon the set of answers to questions of that column.

**Example 2.6.6** : No charges are reimbursed to the patient until the deductible has been met. After the deductible has been met, reimburse 50% for Doctor's Office visits or 80% for Hospital visits. There will be 4 rules:

- (i) The first condition (Is the deductible met?) has two possible outcomes – yes or no.
- (ii) The second condition (type of visit) has two possible outcomes - Doctor's office visit (D) or Hospital visit (H). Two times two is four.

**Solution** : Table 2.6.3 shows the Decision Table of the problem.

<b>Conditions</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
1. Deductible met?	Y	Y	N	N
2. Type of visit	D	H	D	H
<b>Actions</b>				
1. Reimburse 50 %	X			
2. Reimburse 80 %		X		
3. No reimbursement			X	X

**Table 2.6.3 : Decision Table of Example 2.6.6**

**Example 2.6.7** : No charges are reimbursed to the patient until the deductible has been met. After the deductible has been met, the amount to be reimbursed depends on whether or not the doctor or hospital is a "Preferred Provider." For preferred providers Doctor's office visits are reimbursed at 65% and Hospital visits are reimbursed at 95%. For other providers reimburse 50% for Doctor's Office visits or 80% for Hospital visits. There will be 8 rules.

- (i) The first condition (Is the deductible met?) has two possible outcomes - yes or no.
- (ii) The second condition (Is it a Preferred Provider?) has two possible outcomes - yes or no.
- (iii) The third condition (type of visit) has two possible outcomes - Doctor's office visit (D) or Hospital visit (H). Two times two times two is 8.

**Solution :** Table 2.6.4 shows the Decision table of the problem.

<b>Conditions</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>
1. Deductible met?	Y	Y	Y	Y	N	N	N	N
2. Preferred Provider?	Y	Y	N	N	Y	Y	N	N
3. Type of visit	D	H	D	H	D	H	D	H
<b>Actions</b>								
1. Reimburse 65 %	X							
2. Reimburse 95 %		X						
3. Reimburse 50 %			X					
4. Reimburse 80 %				X				
5. No Reimbursement					X	X	X	X

**Table 2.6.4 : Decision Table of Example 2.6.7**

(f) **CASE Tools** : The data flow diagram and system flow charts that users review are commonly generated by systems developers using the on-screen drawing modules found in **CASE** (Computer-Aided-Software Engineering) software packages. CASE refers to the automation of anything that humans do to develop systems and support virtually all phases of traditional system development process. For example, these packages can be used to create complete and internally consistent requirements specifications with graphic generators and specifications languages.

An ideal CASE system would have an integrated set of tools and features to perform all aspects in the life cycle. Some of the features that various CASE products possess are - Repository / Data Dictionary; Computer aided Diagramming Tools; Word Processing; Screen and Report generator; Prototyping; Project Management; Code Generation; and Reverse Engineering.

(g) **System Components matrix** : A **System Component Matrix** provides a matrix framework to document the resources used, the activities performed and the information produced by an information system. It can be used as an information system framework for both systems analysis and system design and views the information system as a matrix of components that highlights how the basic activities of input, processing, output, storage and controls are accomplished in an information system, and how the use of hardware, software and people resources can convert data resources into information products.

Table 2.6.5 illustrates the use of a system component matrix to document the basic components of a sales processing and analysis system in an organization.

## 2.38 Information Systems Control and Audit

Information system Activities	Hardware Resources		Software Resources		People Resources		Data Resources	Information Products
	Machines	Media	Programs	Procedures	Specialists	Users		
<b>Input</b>	POS Terminals	Bar tags, Mag Stripe Cards	Data Entry program	Data Entry procedures		Sales clerks customers	Customer data, product data	Data entry displays
<b>Processing</b>	Mainframe Computer		Sales processing program, sales analysis program	Sales transaction procedures	Computer operators	Sales clerks managers	Customer inventory and sales databases	Processing status displays
<b>Output</b>	POS Terminals, Management Workstations	Paper reports and receipts	Report generator program, Graphic program	Output use and distribution procedures		Sales clerks managers, customers		Sales receipts, sales analysis reports and displays
<b>Storage</b>	Magnetic Disk Drives	Magnetic disk packs	Database management system program		Computer operators		Customer, inventory and sales databases	
<b>Control</b>	POS terminals, Management workstations	Paper documents and control reports	Performance monitor program, security monitor program	Correction procedures	Computer operators control clerks	Sales clerks managers customers	Customer, inventory and sales database	Data entry display, sales receipts, Error display and signals


**Table 2.6.5 : An example of a system component matrix for a sales processing and analysis system. Note how it emphasizes the basic activities needed, resources used and products produced by this information system.**

(h) **Data Dictionary** : A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include - the identity of the source document(s) used to create the data item; the names of the computer files that store the data item; the names of the computer programs that modify the data item; the identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry; the identity of the computer programs or individuals not permitted to access the data item etc.

As new data fields are added to the record structure of a business file, information about each new data item is used to create a new computer record in the data dictionary. Similarly, when new computer programs are created those access data items in existing files, the data dictionary is updated to indicate the data items these new programs access. Finally, when data fields are deleted from the structure of file records, their corresponding records in the data dictionary are dropped.

Fig. 2.6.6 shows a sample record from a data dictionary which is basically a file about data. Each file record contains information about one data field used in other files.

Name of data field	File in which stored	Source document	Size in bytes	Type
Inventory quantity on hand	Inventory master file	Form number ABC 123	4	Numeric



**Fig. 2.6.6 : Example of Data Dictionary**

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help establish an audit trail because it can identify the input sources of data items, the computer programs that modify particular data items, and the managerial reports on which the data items are output. When an accountant is participating in the design of a new system, a data dictionary can also be used to plan the flow of transaction data through the system.

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

**Layout form and Screen Generator :** They are for printed report used to format or “paint” the desired layouts and contact without having to enter complex formatting information. Fig. 2.6.7 shows a Layout screen for the design for a customer order report.

**Menu Generator :** Menu generator outlines the functions which the system is aimed to accomplish. Menu may be linked to other submenus that will enable the user to understand how the screens and sub-screens will be used for data entry or inquiry.

**Report Generator :** Report generator has capacity of performing similar functions as found in screen generators. In addition, it can also indicate totals, paging, sequencing and control breaks in creating samples of the desired report.

**Code Generator :** Code generator allows the analyst to generate modular units of source code from the high level specifications provided by the system analyst and play significant role in systems development process.



## 2.40 Information Systems Control and Audit

Customer Order Report				
Date MM/DD/YY				
Order Number	9999			
Customer Name	XXXXXXXXXXXXXXXXXXXXXXXXXX			
Catalog Number	Available	Location	Cost	Stock Level
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	99999
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	99999
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	99999
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	99999
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	99999
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	99999
	3 Exit	1.8 Column	8 Repeat	10 Field

Fig. 2.6.7 : Layout screen for the design of a display for a customer order report.

### 2.6.5 System Specification

At the end of the analysis phase, the systems analyst prepares a document called “**Systems Requirement Specifications (SRS)**”. A SRS contains the following :

- **Introduction** : Goals and Objectives of the software context of the computer-based system; Information description
- **Information Description** : Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
- **Functional Description**: Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
- **Behavioral Description** : Response to external events and internal controls
- **Validation Criteria** : Classes of tests to be performed to validate functions, performance and constraints.
- **Appendix** : Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review** : It contains the following :
  - The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
  - The review reflects the development team’s understanding of the existing processes. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.

### 2.6.6 Roles Involved in SDLC

#### (i) Steering Committee

Some of the functions of Steering Committee are as follows :

- To provide overall direction and ensures appropriate representation of affected parties.
- To be responsible for all cost and timetables.
- To conduct a regular review of progress of the project in the meetings of steering committee which may involve co-ordination and advisory functions.
- Taking corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

#### (ii) Project Manager

A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. He is responsible for delivery of the project within the time and budget. and periodically reviews the progress of the project with the project leader and his team.

#### (iii) Project Leader

The project leader is dedicated to a project who has to ensure its completion and fulfillment of objectives. He reviews the project position more frequently than a Project Manager and the entire project team reports to him.

#### (iv) Systems Analyst / Business Analyst

The systems analysts' main responsibility is to conduct interviews with users and understand their requirements. He is a link between the users and the programmers who converts the users requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.

#### (v) Module Leader / Team Leader

A project is divided into several manageable modules, and the development responsibility for each module is assigned to Module Leaders. For example, while developing a financial accounting application – Treasury, Accounts payable, Accounts receivable can be identified as separate modules and can be assigned to different module leaders. Module leaders are responsible for the delivery of tested modules within the stipulated time and cost.

#### (vi) Programmer / Coder / Developer

Programmers is a mason of the software industry who converts design into programs by coding using programming language. Apart from developing the application in a programming language, he also tested the program for debugging activity.

## 2.42 Information Systems Control and Audit

### (vii) Database Administrator (DBA)

The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.

### (viii) Quality Assurance

This team sets the standards for development, and checks compliance with these standards by project teams on a periodic basis. Any quality assurance person who has participated in the development process shall not be viewed as “independent” to carry out quality audits.

### (ix) Tester

Tester is a junior level quality assurance personnel attached to a project who tests programs and subprograms as per the plan given by the module / project leaders and prepare test reports.

### (x) Domain Specialist

Whenever a project team has to develop an application in a field that's new to them, they take the help of a domain specialist. For example, if a team undertakes application development in Insurance, about which they have little knowledge, they may seek the assistance of an Insurance expert at different stages. This makes it easier to anticipate or interpret user needs. A domain specialist need not have knowledge of software systems.

### (xi) IS Auditor

As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. He should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.

## 2.7 SYSTEMS DESIGN

After the completion of requirements analysis for a system, systems design activity takes place for the alternative which is selected by management.

**Objective** : Designs an Information System that best satisfies the user / managerial requirements. It describes the parts of the system and their interaction, sets out how the system shall be implemented using the chosen hardware, software and network facilities, specifies the program and the database specifications and the security plan and further specify the change control mechanism to prevent uncontrolled entry of new requirements.

**Activities** : Key design phase activities include - describing inputs and outputs, such as screen design and reports; Determining the processing steps and computation rules for the

new solution; Determining data file or database system file design; Preparing the program specifications for the various types of requirements or information criteria defined; and Internal / external controls.

**Document / Deliverable** : Creates a 'blueprint' for the design with the necessary specifications for the hardware, software, people and data resources.

System design involves first logical design and then physical construction of a system. The logical design of an information system is like an engineering blueprint; it shows major features of the system and how they are related to one another. Physical construction, the activity following logical design, produces program software, files and a working system. Design specifications instruct programmers about what the system should do. The programmers, in turn, write the programs that accept input from users, process data, produce the reports, and store data in the files.

Once the detailed design is completed, the design is then distributed to the system developers for coding. The design phase involves following steps :

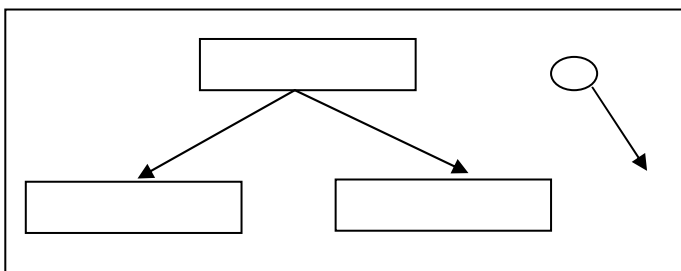
- (i) Architectural Design;
- (ii) Design of the Data / Information Flow;
- (iii) Design of the Database;
- (iv) Design of the User-interface;
- (v) Physical Design; and
- (vi) Design and acquisition of the hardware/system software platform.

**2.7.1 Architectural Design**

Architectural design deals with the organization of applications in terms of hierarchy of modules and sub-modules. At this stage, we identify - major modules; function and scope of each module; interface features of each module; modules that each module can call directly or indirectly and Data received from / sent to / modified in other modules.

The architectural design is made with the help of a tool called Functional Decomposition which can be used to represent hierarchies as shown in Fig. 2.7.1. It has three elements – Module; Connection; and Couple

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.



**Fig. 2.7.1 : Functional Decomposition Tool**

## 2.44 Information Systems Control and Audit

### 2.7.2 Design of Data / Information flow

The design of the data and information flows is a major step in the conceptual design of the new system. In designing the data / information flow for the proposed system, the inputs that are required are - existing data / information flows; problems with the present system; and objective of the new system.

All these have been identified in the analysis phase and documented in **Software Requirements Specification (SRS)**.

### 2.7.3 Design of Database

Design of the database involves determining its scope ranging from local to global structure. The scope is decided on the basis of interdependence among organizational units. The greater the need the interdependence, the greater the need for a global database to prevent sub-optimization by subunits.

The design of the database involves four major activities as discussed in Table 2.7.1.

Design Activity	Explanation
<b>Conceptual Modeling</b>	These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.
<b>Data Modeling</b>	Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages
<b>Storage Structure Design</b>	Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example-tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.
<b>Physical Layout Design</b>	Decisions must be made on how to distribute the storage structure across specific storage media and locations –for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

**Table 2.7.1 : Major activities in Database Designing**

### 2.7.4 Design of User-Interface

Design of user – interface involves determining the ways in which users will interact with a system. The points that need to be considered while designing the user interface are - source documents to capture raw data; hard-copy output reports; screen layouts for dedicated source-document input; inquiry screens for database interrogation; graphic and color displays; and requirements for special input/output device.

**Designing System Outputs**

One of the most important feature of an information system for users is the output it generates. Designing computer output should proceed in an organized, well thought out manner. The right output must be developed while ensuring that each output element is designed so that users will find the system easy to use effectively.

**Input Objectives :** Input design consists of developing specifications and procedures for data preparation, developing steps which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for processing.

**Output Objectives :** The output from an information system should accomplish one or more of the following objectives:

- Convey information about past activities, current status or projections of the future.
- Signal important events, opportunities, problems or warnings.
- Trigger an action.
- Confirmation of an action.

**Important factors in Input / Output design :** There are certain important factors listed in Table 2.7.2, which should be considered by the system analyst while designing user input/output forms.

Characteristic	Definition	Input Design	Output Design
<b>Content</b>	Refers to the actual pieces of data to be gathered to produce the required output to be provided to users.	The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. New documents for collecting such information may be designed.	The contents of a weekly output report to a sales manager might consist of sales person's name, sales calls made by each sales person during the week, and the amount of each product sold by each salesperson to each major client category.
<b>Timeliness</b>	Timeliness refers to when users need outputs, which may be required on a regular, periodic basis - perhaps daily, weekly, monthly, at the of quarter or annually.	Data needs to be inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system.	A sales manager, may be requiring a weekly sales report. Other users, such as airline agents, require both real- time information and rapid response times in order to render better client service.

## 2.46 Information Systems Control and Audit

<p><b>Format</b></p>	<p>Input format refers to the manner in which data are physically arranged.</p> <p>Output format refers to the arrangement referring to data output on a printed report or in a display screen.</p>	<p>After the data contents and media requirements are determined, input formats are designed on the basis of few constraints like - the type and length of each data field as well as any other special characteristics (number decimal places etc.).</p>	<p>Format of information reports for the users should be so devised that it assists in decision-making, identifying and solving problems, planning and initiating corrective action and searching.</p>
<p><b>Media</b></p>	<p>Input-output medium refers to the physical device used for input, storage or output.</p>	<p>This includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives may include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.</p>	<p>A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape/disk and voice output.</p>
<p><b>Form</b></p>	<p>Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non-quantitative, text, graphics, video and audio.</p>	<p>Forms are pre-printed papers that require people to fill in responses in a standardized way. Forms elicit and capture information required by organizational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.</p>	<p>The form of the output should be decided keeping in view the requirements for the concerned user. For example - Information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for stores.</p>

<b>Input Volume / Output Volume</b>	<p>Input volume refers to the amount of data that has to be entered in the computer system at any one time.</p> <p>The amount of data output required at any one time is known as output volume.</p>	<p>In some decision-support systems and many real-time processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.</p>	<p>It is better to use high-speed printer or a rapid-retrieval display unit, which are fast and frequently used output devices in case the volume is heavy.</p>
-------------------------------------	--	---	---

**Table 2.7.2 : Factors affecting Input / Output Form Design**

### 2.7.5 Physical Design

For the physical design, the logical design is transformed into units, which in turn can be decomposed further into implementation units such as programs and modules. During physical design, the primary concern of the auditor is effectiveness and efficiency issues. The auditor should seek evidence that designers follow some type of structured approach like – CASE tools to access their relative performance via simulations when they undertake physical design. Some of the issues addressed here are – type of hardware for client application and server application; Operating systems to be used; Type of networking; Processing – batch – online, real – time; Frequency of input, output; and Month-end cycles / periodical processing.

#### Design Principles

- There is a tendency to develop merely one design and consider it the final product. However the recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria.
- The design should be based on the analysis.
- The software functions designed should be directly relevant to business activities.
- The design should follow standards laid down. For instance, the user interface should have consistent color scheme, menu structure, location of error message and the like.
- The design should be modular.

#### Modularity

A module is a manageable unit containing data and instructions to perform a well-defined task. Interaction among modules is based on well-defined interfaces. Modularity is measured by two parameters : **Cohesion** and **Coupling**.

Cohesion refers to the manner in which elements within a module are linked.



## 2.48 Information Systems Control and Audit

Coupling is a measure of the interconnection between modules. It refers to the number and complexity of connections between 'calling' and 'called' modules.

In a good modular design, cohesion will be high and coupling low.

### 2.7.6 Design of the Hardware / System Software Platform

In some cases, the new system requires hardware and system software not currently available in an organization. For example – a DSS might require high-quality graphics output not supported by the existing hardware and software. The new hardware/system software platform required to support the application system will then have to be designed. If different hardware and software are not able to communicate with each, subsequent changes will have to be made and resources expanded in trying to make the hardware and software compatible to each other. Auditors should be concerned about the extent to which modularity and generality are preserved in the design of the hardware/system software platform.

## 2.8 SYSTEM ACQUISITION

After a system is designed either partially or fully, the next phase of the systems development starts which relates to the acquisition of hardware, software and services.

### 2.8.1 Acquisition Standards

Management should establish acquisition standards that address the same security and reliability issues as development standards. Acquisition standards should focus on -

- Ensuring security, reliability, and functionality already built into a product.
- Ensuring managers complete appropriate vendor, contract, and licensing reviews and acquiring products compatible with existing systems.
- Including invitations-to-tender and request-for-proposals. Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software.
- Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

### 2.8.2 Acquiring Systems Components from Vendors

At the end of the design phase, the organization gets a reasonable idea of the types of hardware, software and services it needs for the system being developed. Acquiring the appropriate hardware and software is critical for the success of the whole project. The organization can discover new hardware and software developments in various ways. Management also decides whether the hardware is to be purchased, leased from a third party or to be rented.

**(I) Hardware Acquisition :** In case of procuring such machinery as machine tools, transportation equipment, air conditioning equipment, etc., the management can normally rely on the time tested selection techniques and the objective selection criteria can be delegated to

the technical specialist. The management depends upon the vendor for support services, systems design, education and training etc., and expansion of computer installation for almost an indefinite period; therefore, this is not just buying the machine and paying the vendor for it but it amounts to an enduring alliance with the supplier.

**(II) Software Acquisition** : Once user output and input designs are finalized, the nature of the application software requirements must be assessed by the systems analyst. This determination helps the systems development team to decide what type of application software products are needed and consequently, the degree of processing that the system needs to handle. This helps the system developers in deciding about the nature of the systems software and computer hardware that will be most suitable for generating the desired outputs, and also the functions and capabilities that the application software must possess. At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor.

### **(III) Contracts, Software Licenses and Copyright Violations**

Contracts between an organization and a software vendor should clearly describe the rights and responsibilities of the parties to the contract. The contracts should be in writing with sufficient detail to provide assurances for performance, source code accessibility, software and data security, and other important issues.

Software license is a license that grants permission to do things with computer software. The usual goal is to authorize activities which are prohibited by default by copyright law, patent law, trademark law and any other intellectual property right. The reason for the license, essentially, is that virtually all intellectual property laws were enacted to encourage disclosure of the intellectual property.

Copyright laws protect proprietary as well as open-source software. The use of unlicensed software or violations of a licensing agreement expose organizations to possible litigation.

### **(IV) Validation of Vendors' proposals**

The contracts and software licensing process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming, but in any case it has to be gone through. This problem is made difficult by the fact that vendors would be offering a variety of configurations. The following factors have to be considered towards rigorous evaluation.

- The Performance capability of each proposed System in Relation to its Costs;
- The Costs and Benefits of each proposed;
- The Maintainability of each proposed;
- The Compatibility of each proposed system with Existing Systems; and
- Vendor Support.

## 2.50 Information Systems Control and Audit

### (V) Methods of Validating the proposal

Large organizations would naturally tend to adopt a sophisticated and objective approach to validate the vendor's proposal. Some of the validation methods are as follows :

(i) **Checklists** : It is the most simple and rather a subjective method for validation and evaluation. The various criteria are put in check list in the form of suitable questions against which the responses of the various vendors are validated.

For example : Support Service Checklists may have parameters like – Performance; System development; Maintenance; Conversion; Training; Back-up; Proximity; Hardware; Software.

(ii) **Point-Scoring Analysis** : Point-scoring analysis provides an objective means of selecting a final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Thus, even for a small business, the evaluators must consider such issues as the company's data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.

For example – Table 2.8.1 illustrates a Point Scoring Analysis list.

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software meet all mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability, etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	5
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	10	8	8	7
Totals	123	94	106	85

**Table 2.8.1 : Point Scoring Analysis List**

(iii) **Public Evaluation Reports** : Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by several buyers in the past. For those criteria, however, where published reports are not available, resort would have to be

made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts.

(iv) **Bench marking problem for vendor's proposals** : Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load and include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs. That is, benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer.

(v) **Test problems** : Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code (program in an assembly or a high level language) into the object code (machine language), response time for two or more jobs in multi-programming environment, overhead requirements of the operating system in executing a user program, length of time required to execute an instruction, etc. The results, achieved by the machine can be compared and price performance judgement can be made. It must be borne in mind, however that various capabilities to be tested would have to be assigned relative weight-age.

## 2.9 DEVELOPMENT : PROGRAMMING TECHNIQUES AND LANGUAGES

**Objective** : To convert the specification into a functioning system.

**Activities** : Application programs are written, tested and documented, conduct system testing.

**Document / Deliverable** : A fully functional and documented system.

A good coded program should have the following characteristics:

- **Reliability** : It refers to the consistence which a program provides over a period of time. However poor setting of parameters and hard coding some data, subsequently could result in the failure of a program after some time.
- **Robustness** : It refers to the process of taking into account all possible inputs and outputs of a program in case of least likely situations.
- **Accuracy** : It refers not only to what program is supposed to do, but should also take care of what it should not do. The second part becomes more challenging for quality control personnel and auditors.
- **Efficiency** : It refers to the performance which should not be unduly affected with the increase in input values.
- **Usability** : It refers to a user-friendly interface and easy-to-understand document required for any program.
- **Readability** : It refers to the ease of maintenance of program even in the absence of the program developer.

## **2.52 Information Systems Control and Audit**

### **2.9.1 Program Coding Standards**

The logic of the program outlined in the flowcharts is converted into program statements or instructions at this stage. For each language, there are specific rules concerning format and syntax. Syntax means vocabulary, punctuation and grammatical rules available in the language manuals that the programmer has to follow strictly and pedantically. Different programmers may write a program using different sets of instructions but each giving the same results. Therefore, the coding standards are defined which serves as a method of communication between teams, amongst the team members and users, thus working as a good control. Coding standards minimize the system development setbacks due to programmer turnover. Coding standards provide, simplicity, efficient utilization of storage and least processing time.

### **2.9.2 Programming Language**

Application programs are coded on the form of statements or instructions and the same is converted by the compiler to binary machine for the computer to understand and execute. The programming languages commonly used are as follows :

- High – level general purpose programming language such as COBOL and C language.
- Object oriented languages such as C++, JAVA etc.
- Scripting language like JAVAScript, VBScript.
- Decision Support or Expert System languages like PROLOG.

### **Choice of Programming Language**

The following are among the most important criteria on the basis of which the language to be used should be decided on the basis of application area; algorithmic complexity; environment in which software has to be executed; performance consideration; data structure complexity; knowledge of software development staff; and capability of in-house staff for maintenance.

### **2.9.3 Program Debugging**

Debugging is the most primitive form of testing activity which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of 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.

### 2.9.4 Test the program

A careful and thorough testing of each program is imperative to the successful installation of any system. The programmer should plan the testing to be performed, including testing all possible exceptions. The test plan should require the execution of all standard processing logic. The program test plan should be discussed with the project manager and/or system users. A log of test results and all conditions successfully tested should be kept. The log will prove invaluable in answering the inevitable question. 'Did you ever test for this condition?'

### 2.9.5 Program Documentation

The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. Managers and users should carefully review documentation in order to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. User documentation should also be reviewed for understandability i.e. the documentation should be prepared in such a way that the user can clearly understand the instructions.

### 2.9.6 Program Maintenance

The requirements of business data processing applications are subject to continual change. This calls for modification of the various programs. There are, usually separate categories of programmers called maintenance programmers who are entrusted with this task.

## 2.10 SYSTEM TESTING

Testing is a process used to identify the correctness, completeness and quality of developed computer software. Testing should systematically uncover different classes of errors in a minimum amount of time and with a minimum amount of effort. The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

Different levels of Testing are as follows :

### 2.10.1 Unit Testing

In computer programming, unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class.

Unit tests are typically written and run by software developers to ensure that code meets its design and behaves as intended. The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. A unit test provides a strict, written contract that the piece of code must satisfy.

There are five categories of tests that a programmer typically performs on a program unit :

- **Functional Tests** : Functional Tests check 'whether programs do what they are supposed to do or not'. The test plan specifies operating conditions, input values, and

## 2.54 Information Systems Control and Audit

expected results, and as per this plan programmer checks by inputting the values to see whether the actual result and expected result match.

- **Performance Tests** : Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests** : Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- **Structural Tests** : Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests** : In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

### Types of Unit Testing

#### (I) Static Analysis Testing

Some important **Static Analysis Tests** are as follows :

- **Desk Check** : This is done by the programmer himself. He checks for logical syntax errors, and deviation from coding standards.
- **Structured walk-through** : The application developer leads other programmers through the text of the program and explanation.
- **Code inspection** : The program is reviewed by a formal committee. Review is done with formal checklists. The procedure is more formal than a walk-through.

#### (II) Dynamic Analysis Testing

- **Black Box Testing** : **Black Box Testing** takes an external perspective of the test object to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure.



This method of test design is applicable to all levels of software testing : unit, integration, functional testing, system and acceptance. The higher the level, hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure

that all existent paths are tested. If a module performs a function which is not supposed to, the black box test does not identify it.

- **White Box Testing :** **White box testing** uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.
- **Gray Box Testing :** **Gray box testing** is a software testing technique that uses a combination of black box testing and white box testing. In gray box testing, the tester applies a limited number of test cases to the internal workings of the software under test. In the remaining part of the gray box testing, one takes a black box approach in applying inputs to the software under test and observing the outputs.

### 2.10.2 Integration Testing

**Integration testing** is an activity of software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before system testing with an objective to evaluate the connection of two or more components that pass information from one area to another. Integration testing takes as its input - modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing. This is carried out in the following manner:

- **Bottom-up Integration :** **Bottom-up integration** is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system. Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available. The disadvantage, however is that testing of major decision / control points is deferred to a later period.
- **Top-down Integration :** **Top-down integration** starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module. An incomplete portion of a program code that is put under a function in order to allow the function and the program to be compiled and tested, is referred to as a stub. A stub does not go in to the details of implementing details of the function or the program being executed.

Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached. Since decision- making processes are likely to occur in the higher



## 2.56 Information Systems Control and Audit

levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested, not with real outputs from subordinate modules, but from stubs.

- **Regression Testing** : Each time a new module is added as part of integration testing, the software changes. New data flow paths are established, new I/O may occur and new control logic is invoked. These changes may cause problems with functions that previously worked flawlessly. In the context of the integration testing, the regression tests ensure that changes or corrections have not introduced new errors. The data used for the regression tests should be the same as the data used in the original test.

### 2.10.3 System Testing

**System testing** is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well defined subsets of the software's functionality have been implemented. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non- production test environment. The types of testing that might be carried out are as follows :

- **Recovery Testing** : This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.
- **Security Testing** : This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, authentication, authorization, availability and non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.
- **Stress or Volume Testing** : Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
- **Performance Testing** : In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

### 2.10.4 Final Acceptance Testing

**Final Acceptance Testing** is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users. Thus the final acceptance testing has two major parts:

- **Quality Assurance Testing** : It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance methodology.
- **User Acceptance Testing** : It ensures that the functional aspects expected by the users have been well addressed in the new system. There are two types of the user acceptance testing :
  - ◆ **Alpha Testing** : This is the first stage, often performed by the users within the organization.
  - ◆ **Beta Testing** : This is the second stage, generally performed by the external users. This is the last stage of testing, and normally involves sending the product outside the development environment for real world exposure.

## 2.11 SYSTEMS IMPLEMENTATION

**Objective** : To implement the new system i.e. put it into production.

**Activities** : The activities involved in System Implementation are as follows :

- Conversion of data to the new system files.
- Training of end users.
- Completion of user documentation.
- System changeover.
- Evaluation of the system a regular intervals.

**Document / Deliverable** : A full functional / documented system in its operational environment.

The process of ensuring that the information system is operational and then allowing users to take over its operation for use and evaluation is called **Systems Implementation**. Implementation includes all those activities that take place to convert from the old system to the new. The new system may be totally new, replacing an existing manual or automatic system or it may be a major modification in an existing system.

### 2.11.1 Activities during Implementation Stage

The activities involved in system implementation stage are as follows :

(I) **Equipment Installation** : The hardware required to support the new system is selected prior to the implementation phase. The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase. An installation checklist should be developed at this time with operating advice from the vendor and system development team. In those installations where people are experienced in the installation of the same or similar equipment, adequate time should be scheduled to allow completion of the following activities :

## 2.58 Information Systems Control and Audit

- **Site Preparation** : An appropriate location must be found to provide an operating environment for the equipment that will meet the vendor's temperature, humidity and dust control specifications.
- **Installation of new hardware / software** : The equipment must be physically installed by the manufacturer, connected-to the power source and wired to communication lines, if required. If the new system interfaces with the other systems or is distributed across multiple software platforms, some final commissioning tests of the production environment may be desirable to prove end to end connectivity.
- **Equipment check out** : The equipment must be turned on for testing under normal operating conditions. Not only the routine 'diagnostic test' should be run by the vendor, but also the implementation team should devise and run extensive tests of its own to ensure that equipments are in proper working condition.

(II) **Training Personnel** : A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system. Thus, training is a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer professionals generally need some type of training. Often this is imparted through classes, which are organized by vendor, and through hands-on learning techniques.

(III) **System Implementation Conversion Strategies** : Conversion or changeover is the process of changing from the old system (manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover. The Four types of implementation strategies are as follows :

(i) **Direct Implementation / Abrupt change-over** : This is achieved through an abrupt takeover – an all or nothing approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Fig 2.11.1 depicts Direct Implementation which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

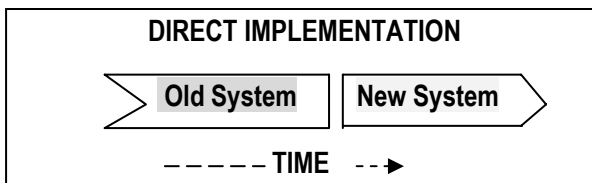


Fig. 2.11.1 : Direct Implementation

(ii) **Phased implementation** : With this strategy, implementation can be staged with conversion to the new system taking place by degrees. For example - some new files may be converted and used by employees whilst other files continue to be used on the old system ie. the new is brought in stages (phases). If each phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in Fig. 2.11.2.

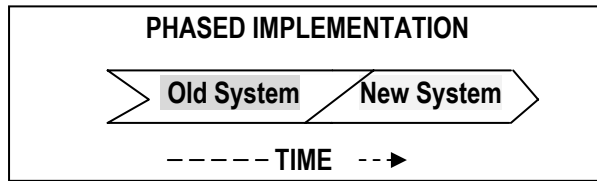


Fig. 2.11.2 : Phase Implementation

(iii) **Pilot implementation** : With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption. For example - it might be tried out in one branch of the company or in one location.

If successful then the pilot is extended until it eventually replaces the old system completely. Fig. 2.11.3 depicts Pilot Implementation.

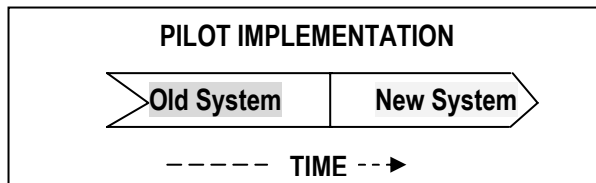


Fig. 2.11.13 : Pilot Implementation

(iv) **Parallel running implementation** : This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online. With this strategy, the old and the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and new system carries on as the only system. Fig. 2.11.4 shows parallel implementation.

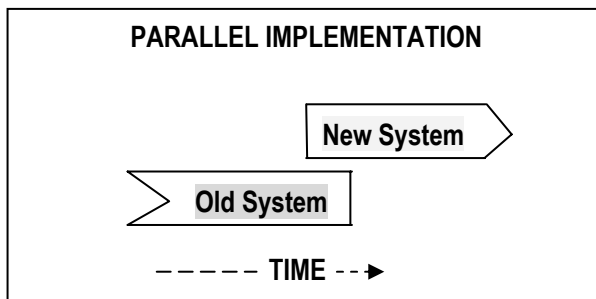


Fig. 2.11.4 : Parallel Implementation

### 2.11.2 Activities involved in conversion

Conversion includes all those activities which must be completed to successfully convert from the previous system to the new information system. Fundamentally these activities can be classified as follows :

## 2.60 Information Systems Control and Audit

(i) **Procedure conversion** : Operating procedures should be completely documented for the new system that applies to both computer-operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output, and internal control must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change.

(ii) **File conversion** : Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on-line files (common database) or off-line files.

In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.

(iii) **System conversion** : After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems.

(iv) **Scheduling personnel and equipment** : Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, however, the job becomes more routine.

Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment. The master schedule for next month should provide sufficient computer time to handle all required processing.

## 2.12 POST IMPLEMENTATION REVIEW AND SYSTEMS MAINTENANCE

**Objective** : To assess and review the complete working solution.

**Activities** : Some of the Systems maintenance activities are as follows :

- Adding new data elements;
- Modifying reports;
- Adding new reports; and
- Changing calculations.

**Document / Deliverable :** A document stating scope of further improvements, if any like-

- Could further training or coaching improve the degree of benefit being generated?
- Are there further functional improvements or changes that would deliver greater benefit?
- Are specific improvements required in procedures, documentation, support, etc?
- What learning points are there for future projects?

### 2.12.1 Post Implementation Review

A **Post Implementation Review** answers the question “Did we achieve what we set out to do in business terms?” Some of the purposes served a Post Implementation Review ascertains the degree of success from the project, in particular, the extent to which it met its objectives, delivered planned levels of benefit, and addressed the specific requirements as originally defined.

- It examines the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefit delivered.

A Post-Implementation Review should be scheduled some time after the solution has been deployed. Typical periods range from 6 weeks to 6 months, depending on the type of solution and its environment. There are two basic dimensions of Information system that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

- **Development evaluation :** Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It requires schedules and budgets to be established in advance and that records of actual performance and cost be maintained. However, it may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.
- **Operation evaluation :** The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties. Operation evaluation answers such questions : Operation evaluation is relatively straightforward if evaluation criteria are established in advance. For example, if the systems analyst lays down the criterion that a system which is capable of supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.
- **Information evaluation :** An information system should also be evaluated in terms of information it provides. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operation evaluations. The objective of an information system is to provide information to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.

## 2.62 Information Systems Control and Audit

### 2.12.2 System Maintenance

Maintaining the system is an important aspect of SDLC. As key personnel change positions in the organization, new changes will be implemented, which will require system updates.

Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements. Maintenance can be categorized in the following two ways :

- **Scheduled maintenance :** **Scheduled maintenance** is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
- **Rescue maintenance:** **Rescue maintenance** refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective maintenance :** **Corrective maintenance** deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors.

The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.

- **Adaptive maintenance :** **Adaptive maintenance** consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective maintenance :** **Perfective maintenance** mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive maintenance :** **Preventive maintenance** concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

## 2.13 OPERATION MANUALS

**Operation Manuals :** A user's guide, also commonly known as an **Operation Manual**, is a technical communication document intended to give assistance to people using a particular system. It is usually written by a technical writer, although user guides are written by programmers, product or project managers, or other technical staff, particularly in smaller

companies. Operation manuals are most commonly associated with electronic goods, computer hardware and software. The section of an operation manual after include the following :

- A cover page, a title page and copyright page;
- A preface, containing details of related documents and information on how to navigate the user guide;
- A contents page;
- A guide on how to use at least the main functions of the system;
- A troubleshooting section detailing possible errors or problems that may occur, along with how to fix them;
- A FAQ (Frequently Asked Questions);
- Where to find further help, and contact details;
- A glossary and, for larger documents, an index;

Sample format of any operations manual could be as shown in Fig. 2.13.1.

<p><b>1.0 GENERAL INFORMATION</b></p> <p><b>1.1 SYSTEM OVERVIEW</b></p> <p>1.2 Project References</p> <p>1.3 Authorized Use Permission</p> <p>1.4 Points of Contact</p> <p style="padding-left: 20px;">1.4.1 Information</p> <p style="padding-left: 20px;">1.4.2 Coordination</p> <p style="padding-left: 20px;">1.4.3 Help Desk</p> <p>1.5 Organization of the Manual</p> <p>1.6 Acronyms and Abbreviations</p> <p><b>2.0 SYSTEM OPERATIONS OVERVIEW</b></p> <p>2.1 System Operations</p> <p>2.2 Software Inventory</p> <p>2.3 Information Inventory</p> <p style="padding-left: 20px;">2.3.1 Resource Inventory</p> <p style="padding-left: 20px;">2.3.2 Report Inventory</p> <p>2.4 Operational Inventory</p> <p>2.5 Processing Overview</p> <p style="padding-left: 20px;">2.5.1 System Restrictions</p> <p style="padding-left: 20px;">2.5.2 Waivers of Operational Standards</p> <p style="padding-left: 20px;">2.5.3 Interfaces with Other Systems</p> <p>2.6 Communications Overview</p> <p>2.7 Security</p>	<p><b>3.0 RUN DESCRIPTION</b></p> <p><b>3.1 RUN INVENTORY</b></p> <p><b>3.2 RUN DESCRIPTION</b></p> <p style="padding-left: 20px;">*3.2.x [Run Identifier]</p> <p style="padding-left: 40px;">3.2.x.1 Run Interrupt</p> <p style="padding-left: 40px;">Checkpoints</p> <p style="padding-left: 40px;">3.2.x.2 Set-Up and Diagnostic Procedures</p> <p style="padding-left: 40px;">3.2.x.3 Error Messages</p> <p style="padding-left: 40px;">3.2.x.4 Restart/Recovery Procedures</p> <p style="padding-left: 40px;">* Each run should be under a separate header. Generate new sections and subsections as necessary for each run from 3.2.1 through 3.2.x.</p>
---	--

**Fig. 2.13.1 : Sample format of Operations Manual**

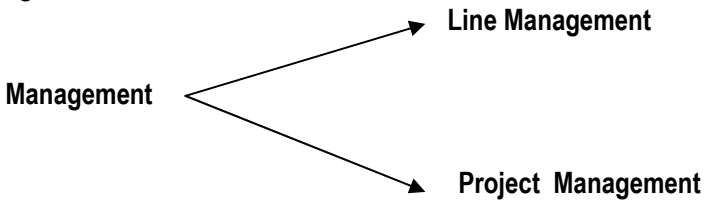


## 2.64 Information Systems Control and Audit

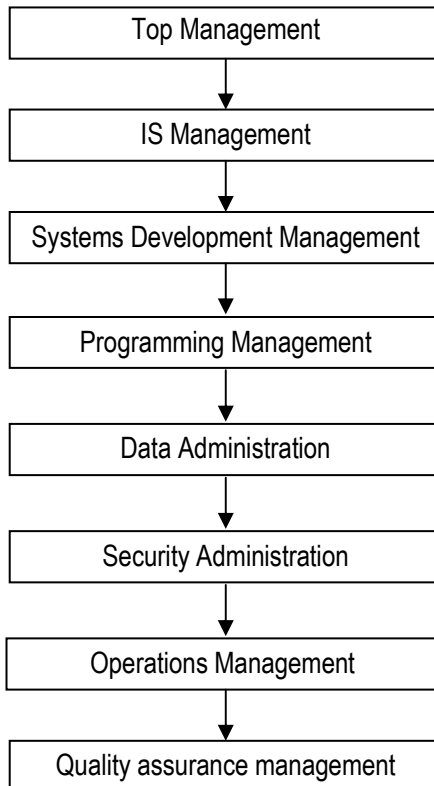
### 2.14 ORGANIZATIONAL STRUCTURE OF IT DEPARTMENT

We will now give a brief introduction about the management structure of IT department.

#### 2.14.1 Management Structure



**Line Management Structure** : The information system management subsystems in an organization attempt to ensure that the development, implementation, operation and maintenance of information systems proceed in a planned and controlled manner. They function to provide a stable environment in which information systems are built and operated on a day-to-day basis. Several levels of management subsystems have been identified corresponding to the organization hierarchy shown in Fig. 2.14.1 and major functions performed within a data processing installation.



**Fig. 2.14.1 : Several levels of management subsystems**

**Top Management :** Top management of the organization must ensure that the data processing installation is well managed. It is responsible primarily for long run policies decisions on how computers will be used in the organization.

**IS Management :** IS management has overall responsibility for planning and control of all computer activities and also provides inputs to top management's long run policy decision making and translates long run policies into short run goals and objectives.

**Systems Development Management :** Systems Development Management is responsible for the design, implementation and maintenance of application systems.

**Programming Management :** Programming management is responsible for programming new systems, maintaining old systems and providing general systems support software.

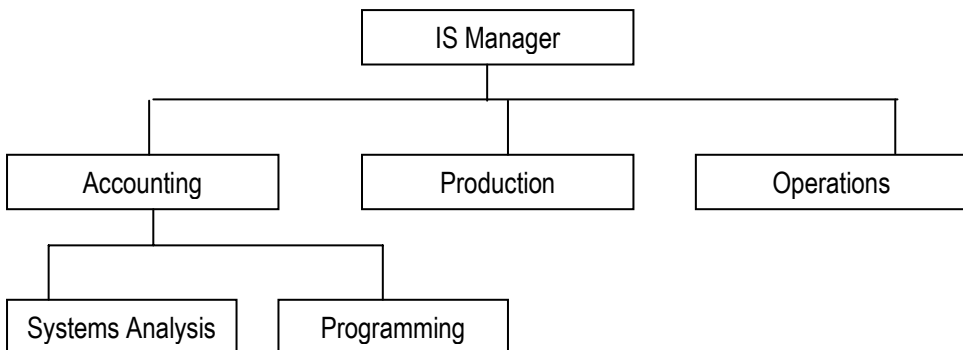
**Data Administration :** Data administration is responsible for the control and use of an organization's data including the database and library of application system files.

**Security Administration :** Security administration is responsible for the physical security of the data processing and IS programs.

**Operations Management :** Operations Management controls the day-to-day operations of data processing systems. It is responsible for data preparation; the data flow through the installation, production running of systems, maintenance of hardware and sometimes maintenance of program and file library facilities.

**Quality Assurance Management :** Quality Assurance Management undertakes an in-depth quality assurance review of data processing in each application system. This review involves a detailed check of the authenticity, accuracy and completeness of input, processing and output.

**2.14.2 Project Management Structure :** In project management, project requests are submitted to and prioritized by the steering committee. The project manager, who may be a non-IS staff member, should be given complete operational control of the project and be allocated the appropriate resources for the successful completion of the project. IS auditors may be included in the project team as control advocates and experts. They also provide an independent, objective review to ensure that the level of commitment of the responsible parties is appropriate.



**Fig. 2.14.2 : Roles performed by IS Manager**

## 2.66 Information Systems Control and Audit

### Duties and Responsibilities :

Fig. 2.14.2 shows the tasks performed by an IS Manager. The structure of an IT Department is divided into two main areas of activity:

1. Information processing.
2. System development and enhancement.

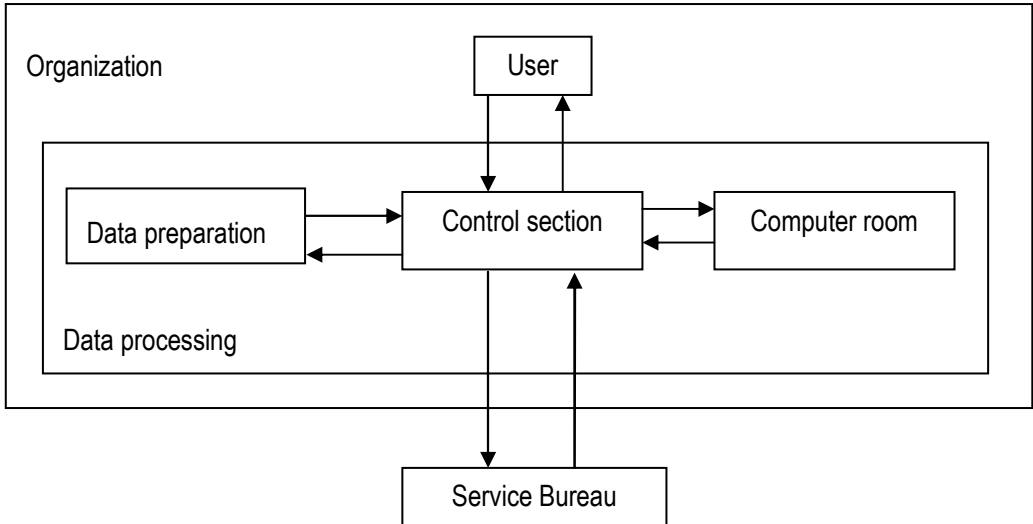
Information Processing or IP is primarily concerned with the operational aspect of the information-processing environment and often includes computer operations, systems programming, telecommunications and librarian functions.

System development is concerned with the development, acquisition and maintenance of computer application systems and performs systems analysis and programming functions.

- **Data entry** : The data entry supervisor is responsible for ensuring whether the data is authorized, accurate and complete when entered into the system. Components in the input subsystem are responsible for bringing information into a system. The information takes two forms : first, it may be raw data to be processed and perhaps applied against the database; second, it may be instructions to direct the system to execute particular processes, updater or interrogate particular data, or prepare particular types of output. Both types of information input must be validated. Any errors detected must be controlled so that the input resubmission is authentic, accurate, complete, unique and timely.
- **File Library** : The file librarian is responsible for recording, issuing, receiving and safeguarding all programs and data files that are maintained on computer tapes or disks. Managing the organization's library of machine-readable files involves three functions. First, files must be used only for the purposes intended. Control must be exercised over program files, data files and procedure files. Second, the storage media used for files must be maintained in correct working order. Third, a file backup strategy and file retention strategy must be implemented. Within the IT department, responsibility for managing files is vested in a file library section.
- **Control Group** : The control group manages the flow of data and is responsible for the collection, conversion and control of input, and balancing the distribution of output to the user community. The input/output control group should be in a separate area where only authorized personnel are permitted. The supervisor of the control group usually reports to the IPF operations managers.
- **Operations** : 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. Though there are some variations across the organizations, the operations group within the IT department undertakes major functions like - Computer operations; Communication network control; Data preparation; Production work flow control; File library; Documentation library; and Performance monitoring.

- **Security Administration** : The security administrator in a data processing organization is responsible for matters of physical security. In other words, the security administrator attempts to ensure that the physical facilities in which the systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of operation.
- **Physical Security** : A complete reliable protection scheme must take into account the possibility of physical attacks on the database, ranging from disclosure of a password to theft of the physical storage devices. We can protect well by encrypting data. A high security system needs better identification than a password, such as personal recognition of the user by a guard.
- **Data Security** : Database management systems often provide controls over data definition and data manipulation facilities. In environments, which combine database management with online transaction processing, access to the database objects such as tables or views can be controlled through internal database mechanisms, which limit what the transaction or program, can do. Various auditing or journaling are also available. Utility access and submission, as well as monitoring and performance tools, should be restricted to appropriate personnel.
- **Conducting a Security program** : A security program is a series of ongoing, regular, periodic evaluations conducted to ensure that the physical facilities of an Information System are safeguarded adequately. The first security evaluation conducted may be a major exercise; the security administrator has to consider an extensive list of possible threats to the organization, prepare an inventory of assets, evaluate the adequacy of controls, implement new controls, etc. Subsequent security evaluations may focus only on changes that have occurred, perhaps in light of the purchase of new hardware or a new threat etc. Nevertheless, even in the absence of visible changes, security evaluations need to be repeated periodically to determine whether covert changes have occurred that necessitate modifications to controls. Fig. 2.14.3 shows the activities involved in an organization.
- **Production Work Flow Control** : Production workflow control in an Information System, is the responsibility of a control section. The control section manages the flow of data between users and the information system, and between data preparation and the computer room. It is also more difficult for operators and data preparation personnel to collude and to perpetrate a fraud – for example, by alerting input data.

## 2.68 Information Systems Control and Audit



**Fig. 2.14.3 : Activities involved in an Organization**

- **Quality Assurance** : Quality Assurance group is responsible for testing and verifying whether the program changes and documentation adhere to standards and naming conventions before the programs are moved into production. The control section facilitates the orderly flow of data and checks to see that the input is in order by scanning it for reasonableness and completeness and by checking control totals. If the input passes the quality assurance check, it is entered into a log and dispatched either to the computer room, if it is already in machine-readable form or to data preparation, if it must be keyed to cards, tape or disk.
- **Systems Analysis** : System analysts are responsible for interpreting the needs of the user, determining the programs and the programmers necessary to create the particular application. System analysts design systems based on the needs of the user. For the auditor acting as a participant in the system development process, the information processing system design phase is one of major involvement. From a system effectiveness viewpoint, the auditor is concerned with whether the design meets strategic requirements. From efficiency viewpoint the auditor is concerned with the resources that will be needed to run the system. From safeguarding access and data integrity viewpoint, the auditor is concerned with the controls designed into the system.
- **Applications Programming** : Applications programmers are responsible for developing new systems and for monitoring systems in production. They should work in a test only environment and should not move test versions into the production environment. Application programmers should not have access to system program libraries.
- **Systems programming** : System programmers are responsible for maintaining the systems software including the operating systems.

- **Local Area Network (LAN) Administration** : LAN administrator is responsible for technical and administrative control over the local area network. This includes ensuring transmission links are functioning correctly, backups of the system are occurring and software/hardware purchases are authorized and properly installed. In smaller installations, this person may be responsible for security administration over the LAN. The LAN administrator should have no application responsibilities, but may have end-user responsibilities. The LAN administrator may report to the director of the IPF and in a decentralized operation, he can report to the end-user manager.
- **Help Desk Administration** : The Help Desk Administrator is responsible for monitoring, improving and controlling system performance in mainframe and client/server hardware and software. The Help Desk Administration may be useful when data entry is not based upon a dedicated source document. If users are uncertain about the nature or format of the data to be entered into a particular field, they may ask the system to provide information to assist them.

**References :**

1. Valacich George, Haffer, Essentials of Systems Analysis & Design, Prentice Hall India, 11<sup>th</sup> Edition 2004.
2. Charles Parker & Thomas Case, Management Information System Strategy & Action, 11<sup>th</sup> Edition, Mcgraw Hill, 1993.
3. [http://www.cms.hhs.gov/SystemLifecycleFramework/Downloads/Selecting\\_Development\\_Approach.pdf](http://www.cms.hhs.gov/SystemLifecycleFramework/Downloads/Selecting_Development_Approach.pdf)
4. [http://en.wikipedia.org/wiki/Systems\\_Development\\_Life\\_Cycle](http://en.wikipedia.org/wiki/Systems_Development_Life_Cycle)
5. [http://www.klbschool.org.uk/ict/gcse/theory/5\\_3/5\\_3\\_3\\_implementation.htm](http://www.klbschool.org.uk/ict/gcse/theory/5_3/5_3_3_implementation.htm)
6. <http://www.epmbook.com/pir.htm>

**Self - Examination Questions**

1. What is Systems Development Process?
2. What activities are part of the Systems Development Life Cycle (SDLC)?
3. Discuss various approaches to systems development.
4. What types of systems are best for development by the traditional approach? What types of systems by prototyping approaches? What types by end user development?
5. How is systems development handled in smaller organizations?
6. What is the purpose of a preliminary investigation? What outcome is expected from it? Who carries out this investigation?
7. What do you mean by feasibility study? How is it conducted?
8. What systems costs are estimated during feasibility study for various alternative solutions?

## 2.70 Information Systems Control and Audit

9. What is systems requirement analysis? How are requirements determined?
10. Discuss various fact finding techniques.
11. What role does observation play in system investigation?
12. Discuss, in detail, how the investigation of present system is conducted by the system analyst.
13. What are the major categories of systems development tools?
14. What is a data flow diagram (DFD)? Give an example of a DFD.
15. What do you understand by the term "CASE tools"? Briefly describe various CASE tools.
16. What is a data dictionary? What are its uses?
17. What objectives guide the systems analyst in designing an information system?
18. Distinguish between logical design and physical design.
19. What guidelines should be followed while preparing the layout form of (i) printed output, (ii) visual display unit.
20. Discuss various issues that should be considered while designing systems input?
21. Discuss, in detail, the guidelines that should be observed in designing an input form?
22. Why coding system is required in an information system? What are the desired characteristics of a good coding scheme?
23. What is a system manual? What information is included in it?
24. What factors should be considered in equipment selection?
25. What are the different sources of acquiring software?
26. Briefly describe the criteria for vendor's selection for a computer system.
27. Discuss some of the methods for validating vendors' proposal for a computer system.
28. What is the meaning of the term "Program Debugging"?
29. 'Program debugging is very crucial for the success of a program'. Do you agree with this statement? Give reasons.
30. Draw a flowchart to read a number N and print all its divisors.
31. Briefly describe various steps involved in system testing.
32. Describe the types of activities that make up the system implementation phase of development.
33. Describe various steps that should be taken for the successful installation of the equipment.
34. Draw a flowchart for computing the sum of the digits of any given number.
35. In what different ways could system conversion take place? Explain.

36. Describe briefly, various activities that should be completed for successful conversion of an existing system to the new information system.
37. What is the purpose of system evaluation? How is it performed?
38. Draw a flowchart to computer the sum of squares of integers from 1 to 50.
39. What do you understand by the term "Systems Maintenance"?
40. Draw a flowchart to arrange the given data in an ascending order.



## CONTROL OBJECTIVES

---

### LEARNING OBJECTIVES :

- To understand the importance of internal controls and control objectives,
- How to set and monitor Internal Control systems,
- Categories of Control Techniques: System development, System implementation, Change management, Data integrity, Privacy and Security, and
- An overview of the entire IS Audit process.

### 3.1 INFORMATION SYSTEMS CONTROLS

The increasing use of information technology in a large number of organizations has made it imperative that appropriate information systems are implemented in an organization. Information technology covers all key aspects of business processes of an enterprise and has an impact on its strategic and competitive advantage for its success. The enterprise strategy outlines the approach it wishes to formulate with relevant policies and procedures on harnessing the resources to achieve business objectives.

Control is defined as: Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented or detected and corrected.

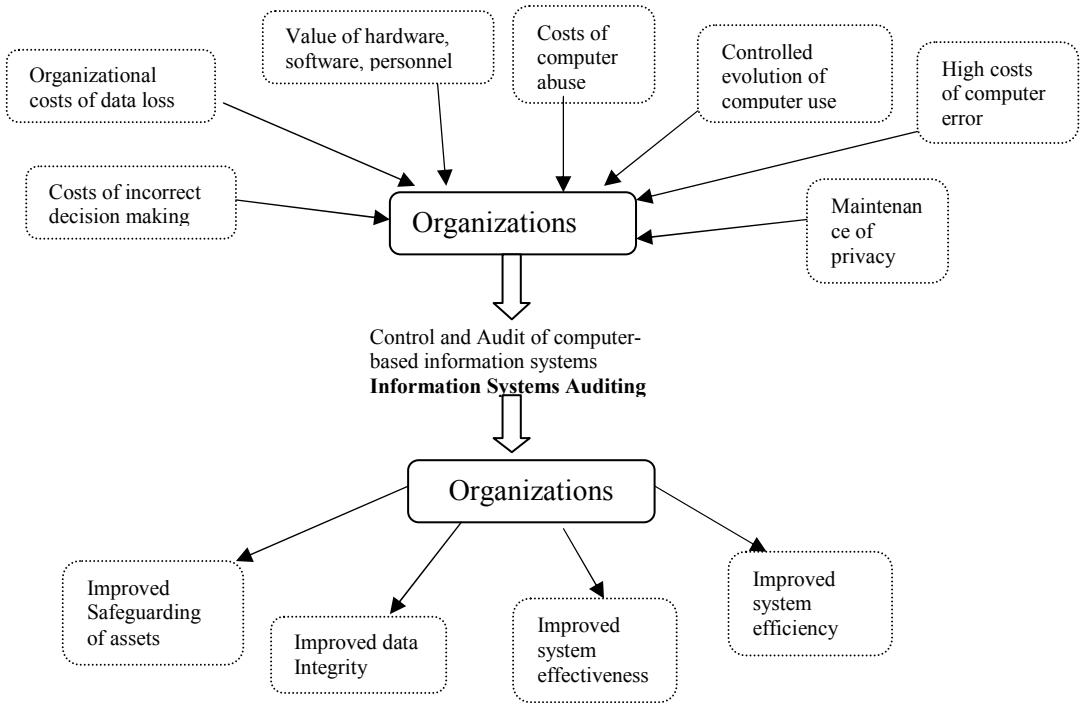
Thus an information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

### 3.2 NEED FOR CONTROL AND AUDIT OF INFORMATION SYSTEMS

Technology has impacted what can be done in business in terms information and as a business enabler. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information by empowering the business decision maker. With the advent of affordable hardware, technology has become a critical component of business. Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization. Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

### 3.2 Information Systems Control and Audit

Factors influencing an organization toward control and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 3.1.



**Fig. 3.1 : Impact of control and audit influencing an organization**

- (i) *Organisational Costs of Data Loss* : Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- (ii) *Incorrect Decision Making* : Management and operational controls taken by managers involve detection, investigations and correction of out-of-control processes. These high level decisions require accurate data to make quality decision rules.
- (iii) *Costs of Computer Abuse* : Unauthorised access to computer systems, computer viruses, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.)
- (iv) *Value of Computer Hardware, Software and Personnel* : These are critical resources of an organisation which has a credible impact on its infrastructure and business competitiveness.
- (v) *High Costs of Computer Error* : In a computerised enterprise environment where many critical business processes are performed a data error during entry or process would cause great damage.
- (vi) *Maintenance of Privacy* : Today data collected in a business process contains details about an individual on medical, educational, employment, residence etc. These data

were also collected before computers but now there is a fear that privacy has eroded beyond acceptable levels.

- (vii) *Controlled evolution of computer Use* : Technology use and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.
- (viii) *Information Systems Auditing* : is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that include not only attest objectives but also effectiveness and efficiency objectives.
- (ix) *Asset Safeguarding Objectives* : The information system assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorised access.
- (x) *Data Integrity Objectives* : is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation depends on the value of information, the extent of access to the information and the value of data to the business from the perspective of the decision maker, competition and the market environment.
- (xi) *System Effectiveness Objectives* : Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet substantial user requirements.
- (xii) *System Efficiency Objectives* : To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

### **3.3 EFFECT OF COMPUTERS ON INTERNAL CONTROLS**

The internal controls within an enterprise in a computerised environment the major areas of impact with the goal of asset safeguarding, data integrity, system efficiency and effectiveness are discussed below.

- (i) *Personnel* : Whether or not staffs are trustworthy, if they know what they are doing and, if they have the appropriate skills and training to carry out their jobs to a competent standard.
- (ii) *Segregation of duties* : a key control in an information system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish. The various stages in the transaction cycle are spread between two or more individuals. However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department.

Within an IT environment, the staff in the computer department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output. IT staff may also be in a position to alter transaction data or even the financial applications which process the transactions. This

### 3.4 Information Systems Control and Audit

gives them the knowledge and means to alter data, all they would then require is a motive.

- (iii) *Authorisation procedures* : to ensure that transactions are approved. In some on-line transaction systems written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals)
- (iv) *Record keeping* : the controls over the protection and storage of documents, transaction details, and audit trails etc.
- (v) *Access to assets and records* : In the past manual systems could be protected from unauthorised access through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs are vulnerable to unauthorised amendment at the computer or from remote locations. The use of wide area networks, including the Internet, has increased the risk of unauthorised access. The nature and types of control available have changed to address these new risks.
- (vi) *Management supervision and review* : Management's supervision and review helps to deter and detect both errors and fraud.
- (vii) *Concentration of programs and data* : Transaction and master file data (e.g. pay rates, approved suppliers lists etc.) may be stored in a computer readable form on one computer installation or on a number of distributed installations. Computer programs such as file editors are likely to be stored in the same location as the data. Therefore, in the absence of appropriate controls over these programs and utilities, there is an increased risk of unauthorised access to, and alteration of financial data.

The computer department may store all financial records centrally. For example, a large multinational company with offices in many locations may store all its computer data in just one centralised computer centre. In the past, the financial information would have been spread throughout a client's organisation in many filing cabinets.

If a poorly controlled computer system was compared to a poorly controlled manual system, it would be akin to placing an organisation's financial records on a table in the street and placing a pen and a bottle of correction fluid nearby. Without adequate controls anyone could look at the records and make amendments, some of which could remain undetected.

Internal controls used within an organisation comprise of the following five interrelated components:

*Control environment* : Elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.

*Risk Assessment* : Elements that identify and analyze the risks faced by an organisation and the ways the risk can be managed. Both external and internal auditors are concerned with errors or irregularities cause material losses to an organisation.

*Control activities* : Elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of recorded amounts occur. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.

*Information and communication* : Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.

*Monitoring* : Elements that ensure internal controls operate reliably over time.

### **3.4 EFFECT OF COMPUTERS ON AUDIT**

To cope with the new technology usage in an enterprise the Auditor is to be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria. The two basic functions carried out to examine these changes are summarised under as-

- (i) Changes to Evidence Collection; and
- (ii) Changes to Evidence Evaluation.

(i) *Changes to Evidence Collection* : Changes in the audit trail say the existence of an audit trail is a key financial audit requirement, since without an audit trail, the financial auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts. The performance of evidence collection and understanding the reliability of controls involves issues like-

- *Data retention and storage* : A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities the auditor may not be able to review a whole reporting period's transactions on the computer system. For example, the client's computer system may save on data storage space by summarising transactions into monthly, weekly or period end balances.

If the client uses a computerised financial system all, or part of the audit trail may only exist in a machine readable form. Where this is the case, the auditor may have to obtain and use specialised audit tools and techniques which allow the data to be converted and interrogated.

Computerised financial data is usually stored in the form of 1s and 0s, i.e. binary, on magnetic tapes or disks. It is not immediately obvious to the auditor what the 1s and 0s mean. The data must be translated into 'normal' text by an additional process before it can be read and understood by the auditor. Since there are various formats for representing electronic data the auditor must find out what format the client has used, e.g. simple binary, hexadecimal, ASCII

### 3.6 Information Systems Control and Audit

or EBCDIC, etc. For example, the character A has a decimal value of 65 in ASCII, which can be stored as 1000001 in binary, or 41 in hexadecimal. The representation of client data is covered in the INTOSAI IT audit training module "Data Downloading".

When a client gives the auditor a magnetic tape containing transaction details, the data is not readily accessible. Unlike receiving a printed transaction listing, the auditor cannot just pick up a magnetic tape and read off the transactions. The data on the disk or tape may be in a different format and hence may require conversion and translation. Once the data has been uploaded onto the auditor's machine audit software may be required to interrogate the information.

- *Absence of input documents* : Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.
- *Lack of a visible audit trail* : The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- *Lack of visible output* : The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- *Audit evidence*. Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.

Where transactions are system generated, the process of formal transaction authorisation may not have been explicitly provided in the same way as in a manual environment, i.e. each transaction is not supported by the signature of a manager, supervisor or budget holder. This may alter the risk that transactions may be irregular or ultra vires. Where human intervention is required to approve transactions the use of judgement is normally required. Judgement is a feature which computers are generally not programmed to demonstrate.

- *Legal issues* : The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

The admissibility of the evidence provided by a client's computer system may need special consideration. The laws regarding the admissibility of computer evidence varies from one country to another. Within a country laws may even vary between one state and another. If the auditor intends to gather evidence for use in a court, s(he) should firstly find out what the local or national laws stipulate on the subject.

In addition, the admissibility of evidence may vary from one court to another. What is applicable in a civil court may not be applicable in a criminal court.

(ii) *Changes to Evidence Evaluation* : Evaluation of audit trail and evidence is to trace consequences of control strength and weakness through the system. The evidence evaluation function of information systems leads to identify periodic and deterministic errors.

- *System generated transactions* : Financial systems may have the ability to initiate, approve and record financial transactions. This is likely to become increasingly common as more organisations begin to install expert systems and electronic data interchange (EDI) trading systems. The main reason clients are starting to use these types of system is because they can increase processing efficiency ( for example, if a computer system can generate transactions automatically there will be no need to employ someone to do it manually, and hence lower staff costs)

Automated transaction processing systems can cause the auditor problems. For example when gaining assurance that a transaction was properly authorised or in accordance with delegated authorities. The auditor may need to look at the application's programming to determine if the programmed levels of authority are appropriate.

Automated transaction generation systems are frequently used in 'just in time' (JIT) inventory and stock control systems : When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier (perhaps using EDI technology)

- *Systematic Error* : Computers are designed to carry out processing on a consistent basis. Given the same inputs and programming, they invariably produce the same output. This consistency can be viewed in both a positive and a negative manner.

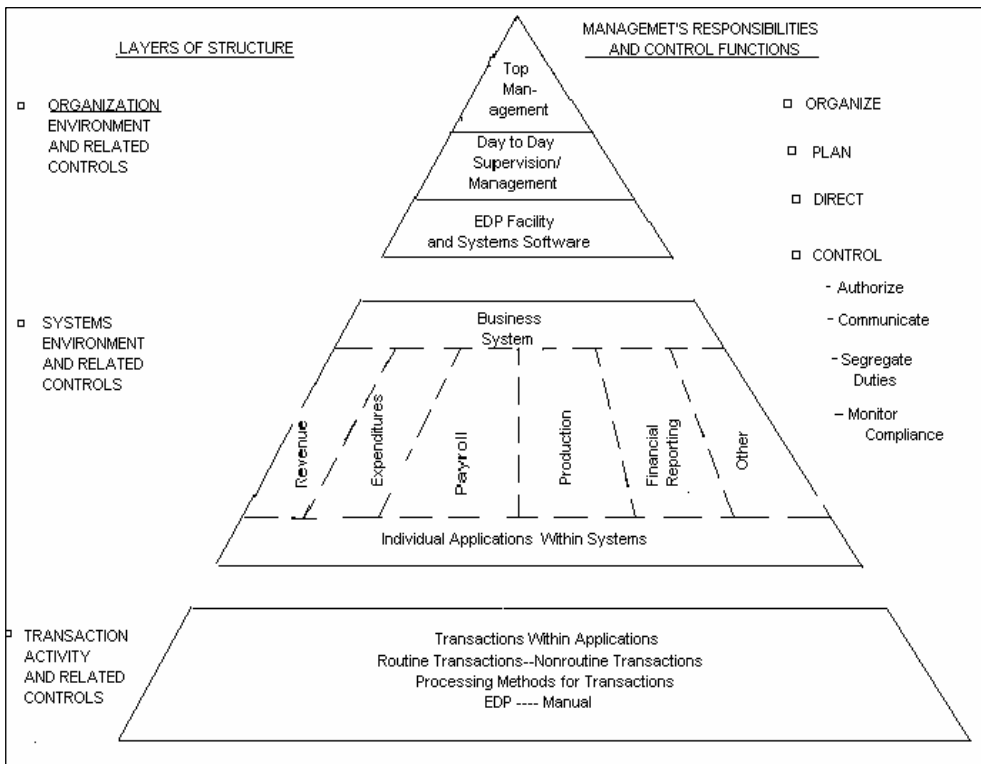
If the computer is doing the right thing, then with all other things being equal, it will continue to do the right thing every time. Similarly, if the computer is doing the wrong thing and processing a type of transaction incorrectly, it will continue to handle the same type of transactions incorrectly every time. Therefore, whenever an auditor finds an error in a computer processed transaction, s(he) should be thorough in determining the underlying reason for the error. If the error is due to a systematic problem, the computer may have processed hundreds or thousands of similar transactions incorrectly

### 3.5 RESPONSIBILITY FOR CONTROLS

Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems. Management should consistently apply the internal control standards to meet each of the internal control objectives

### 3.8 Information Systems Control and Audit

and to assess internal control effectiveness. The number of management levels depends on the company size and organisation structure, but generally there are three such levels senior, middle and supervisory. Senior management is responsible for strategic planning and objectives thus setting the course in the lines of business that the company will pursue, Middle management develops the tactical plans, activities and functions that accomplish the strategic objectives, supervisory management oversees and controls the daily activities and functions of the tactical plan.



**Fig. 3.2 : Structure of the Control environment**

(i) *Long-range planning* : includes documenting goals and objectives, explaining how strengths will be used and how weakness will be compensated for or corrected. The elements of long-range planning incorporate:

The goals and objective of the plan-for use in measuring progress,

- Revenue and expense estimates,
- Time allowance and target dates, and
- Strengths and weakness.



- (ii) *Long-range planning and IT department* : The information system managers must take systematic and proactive measures to
- Develop and implement appropriate, cost-effective internal control for results-oriented management;
  - Assess the adequacy of internal control in programs and operations;
  - Separately assess and document internal control over information systems consistent with the information security policy of the organisation
  - Identify needed improvements;
  - Take corresponding corrective action; and
  - Report annually on internal control through management assurance statements
- (iii) *Shot-range planning or tactical planning*- the functions and activities performed every day are established to meet the long-range goals. For example, data processing job plan defines daily activities of developing software and obtaining hardware in sufficient time to support business activities.
- (iv) *Personnel Management controls* : This involves activities and functions to accomplish the administration of individuals, salary and benefits costs. The control techniques are-
- Job descriptions- It's a management control to communicate management requirement and provide a standard for performance measurement.
  - Salary and benefits budget : To identify the cost factors and evolve a strategic plan for new product and services.
  - Recruiting standards and criteria-This control is critical for IS positions which requires technical training and experience to develop and maintain operational efficiency.
  - Job performance evaluations : To counsel and motivate employees to maintain quality of systems design and conformance with deadlines and budget time.
  - Screening and security standards : In an IS environment an intentionally erroneous or fraudulent program can damage a company, even causing bankruptcy. Screening and credit reports are preventive control measures with applicable labour laws and regulations.

### 3.6 THE IS AUDIT PROCESS

The Audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following :

- Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

### **3.10 Information Systems Control and Audit**

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency. The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilisation of resources)

#### **3.6.1 Responsibility of IS Auditor**

The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. The set of skills that is generally expected of an IS auditor include :

- Sound knowledge of business operations, practices and compliance requirements,
- Should possess the requisite professional technical qualification and certifications,
- An good understanding of information Risks and Controls,
- Knowledge of IT strategies, policy and procedure controls,
- Ability to understand technical and manual controls relating to business continuity, and
- Good knowledge of Professional Standards and Best practices of IT controls and security.

Therefore the audit process begins by defining the scope and objectives to adapt the standards and benchmarks for developing information model for collecting and evaluating evidence to execute the audit.

#### **3.6.2 Functions of IS Auditor**

IT Auditor often is the translator of business risk, as it relates to the use of IT, to management, someone who can check the technicalities well enough to understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management.

IT auditors review risks relating to IT systems and processes, some of them are:

- (i) Inadequate information security (e.g. missing or out of date antivirus controls, open computer ports, open systems without password or weak passwords etc.)
- (ii) Inefficient use of corporate resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
- (iii) Ineffective IT strategies, policies and practices (including a lack of policies for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.)
- (iv) IT-related frauds (including phishing, hacking etc)

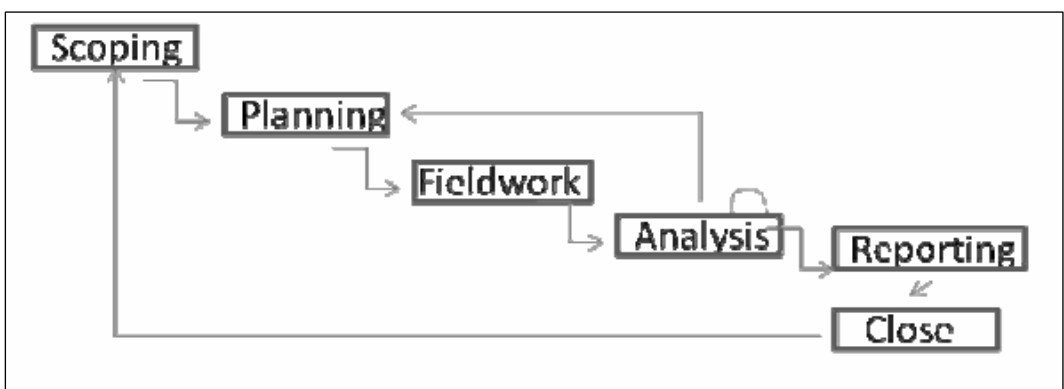
### 3.6.3 Categories of IS audits

IT audits has been categorized in to five types:

- (i) *Systems and Applications* : An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity
- (ii) *Information Processing Facilities* : An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- (iii) *Systems Development* : An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- (iv) *Management of IT and Enterprise Architecture* : An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- (v) *Telecommunications, Intranets, and Extranets* : An audit to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

### 3.6.4 Steps in Information Technology Audit

Different audit organizations go about IT auditing in different ways and individual auditors have their own favourite ways of working. It can be categorized into six stages-



**Fig. 3.3 : Steps in IS Audit process**

- (i) *Scoping and pre-audit survey* : the auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

### 3.12 Information Systems Control and Audit

- (ii) *Planning and preparation* : during which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.
- (iii) *Fieldwork* : gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.
- (iv) *Analysis* : this step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Treats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.
- (v) *Reporting* : reporting to the management is done after analysis of data gathered and analysis.
- (vi) *Closure* : closure involves preparing notes for future audits and following –up management to complete the actions they promised after previous audits.

Steps 3 and 4 may on occasions involve the use of automated data analysis tools such as ACL or IDEA, if not Excel, Access and hand-crafted SQL queries. Automated system security analysis, configuration or vulnerability management and security benchmarking tools are also a boon for reviewing security parameters, and of course basic security management functions that are built-in to modern systems can help with log analysis, reviewing user access rights etc.

#### 3.6.5 Audit Standards

IS auditors need guidance and a different yardstick to measure the 3Es' (Economy, Efficiency and Effectiveness) of a system. The objective is to determine on how to achieve implementation of the IS auditing standards, use professional judgement in its application and be prepared to justify any departure.

He needs guidance on how :

- IS should be assessed to plan their audits effectively?
- To focus their effort on high-risk areas and;
- To assess the severity of any errors or weaknesses found.

The Institute of Chartered Accountants of India has issued AASs covering various aspects. Although these standards are primarily concerned with the audit of financial information, they can be adapted for the purposes of IS Audit depending on its scope and objectives. The following AASs issued by the Institute of Chartered Accountants of India can be adapted for the IS Audits :

1. Basic Principles Governing an Audit
2. Objective and scope of the Audit of Financial Statements
3. Documentation
4. The Auditor's responsibility to consider detect / error in an Audit of financial Statements

5. Audit Evidence
6. Risk Assessment and Internal Controls
7. Relying Upon the Work of an Internal Auditor
8. Audit Planning
9. Using the Work of an Expert
10. Using the Work of Another Auditor
11. Representations by Management
12. Responsibility of Joint Auditors
13. Audit Materiality
14. Analytical Procedures
15. Audit Sampling
16. Going Concern
17. Quality control for Audit Work
18. Audit of Accounting Estimates
19. Subsequent Events
20. Knowledge of Business
21. Consideration of Laws and Regulations in and audit of Financial Statements
22. Initial Engagements Opening Balances
23. Related Parties
24. Audit considerations relating to Using Service organisations
25. Comparatives
26. Terms of Audit Engagement
27. Communication of Audit Matters With Those Charged with Governance
28. The Auditor's Report on Financial Statements
29. Auditing in a Computer Information Systems Environment
30. External Confirmations
31. Engagements to compile Financial Information
32. Engagements to Perform Agreed upon Procedures regarding Financial Information.

## 3.14 Information Systems Control and Audit

Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.

Several well known organizations have given practical and useful information on IS Audit and few are well known organizations have given practical and useful information on IS Audit are :

**3.6.6 ISACA (Information Systems Audit and Control Association)** is a global leader in information governance, control, security and audit. ISACA developed the following to assist IS auditor while carrying out an IS audit.

*IS auditing standards* : ISACA issued 16 auditing standards which defines the mandatory requirements for IS auditing and reporting.

*IS auditing guidelines* : ISACA issued 39 auditing guidelines which provide a guideline in applying IS auditing standards.

*IS auditing procedures* : ISACA issued 11 IS auditing procedures which provide examples of procedure an IS auditor need to follow while conducting IS audit for complying with IS auditing standards.

*COBIT (Control objectives for information and related technology)* : is a framework containing good business practices relating to information technology

**3.6.7 ISO 27001 (Information Security Management-Specification with Guidance for Use)** a global standard issued by ISO (The International Organization for Standardization) and IEC (The International Electro technical Commission) in October 2005. It helps to establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems. ISO/ IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. IT helps organizations in identification and clarification of existing information security management, formulating security requirements and objectives, managing security risks in cost effectively manner, to ensure compliance with laws and regulations, to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons and implementation of business-enabling information security.

**3.6.8 IIA (The Institute of Internal Auditors)** is an international professional association. This association provides dynamic leadership for the global profession of internal auditing. IIA issued Global Technology Audit Guide (GTAG) GTAG provides management of organisation about information technology management, control, and security and IS auditors with guidance on different information technology associated risks and recommended practices. Following is the list of GTAG developed by IIA.

GTAG 1 : Information Technology Controls

GTAG 2 : Change and Patch Management Controls : Critical for Organizational Success

GTAG 3 : Continuous Auditing : Implications for Assurance, Monitoring, and Risk Assessment

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

GTAG 9 : Identity and Access Management.

**3.6.9 ITIL (IT Infrastructure Library)** is the best practice in IT Service Management, developed by OGC and supported by publications, qualifications and an international user group. It gives a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures that can be tailored to any IT organization. ITIL provides a systematic and professional approach to the management for IT services. ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organisations' growing dependency on IT and embodies the best practices for IT Service Management.

Information System Audit and Control Association (ISACA) has long recognized the importance of information security and control and offers a wide range of products and services on the topic. Most significantly, in 2002 ISACA introduced the Certified Information Security Manager (CISM) certification, recognizing the special role played by those who manage an enterprise's information security program.

### **3.6.10 Control objectives for Information related Technology (COBIT)**

The Information Systems Audit and control Foundation (ISACF) developed the Control Objectives for Information and related Technology (COBIT) COBIT is a framework of generally applicable information systems security and control practices for IT control. The framework allows management to benchmark the security and control practices of IT environments, users of IT services to be assured that adequate security and control exist, and auditors to substantiate their opinions on internal control and to advise on IT security and control matters.

The framework addresses the issue of control from three vantage points, or dimensions:

- (i) *Business Objectives*. To satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives : effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements, and reliability.
- (ii) *IT resources*, while include people, application systems, technology, facilities, and data.
- (iii) *IT processes*, which are broken into four domains : planning and organization, acquisition and implementation, delivery and support, and monitoring.

### 3.16 Information Systems Control and Audit

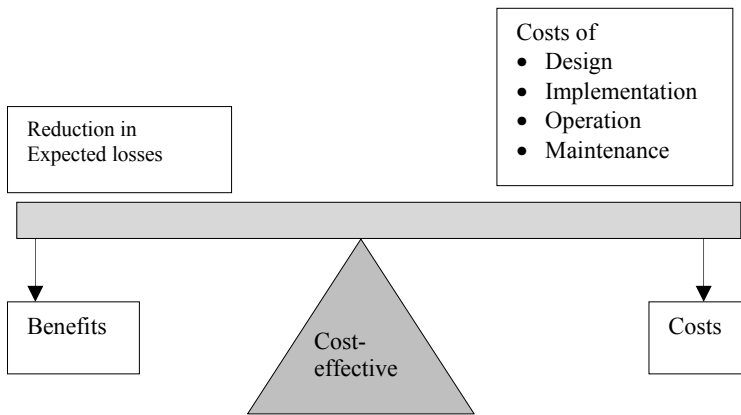
COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession. It is helping managers learn how to balance risk and control investment in an information system environment. It provides users with greater assurance that the security and IT controls provided by internal and third parties are adequate. It guides auditors as they substantiate their opinions and as they provide advice to management on internal controls.

COBIT is discussed in detail in Chapter 8 of the Study material.

#### 3.6.11 Cost effectiveness of control procedures

No internal control system can provide foolproof protection against all internal control threats. The cost of a foolproof system would be prohibitive. In addition, because many controls negatively affect operational efficiency, too many controls slow the system and make it inefficient. Therefore,

the objective in designing an internal control system is to provide reasonable assurance that control problems do not take place.



**Fig. 3.4 : Cost-Effectiveness of Controls**

To determine if a control is effective an auditor must compare the reduction in expected losses that will occur by virtue of having the control with the costs of designing, implementing, operating and maintaining the control. Implementing and operating controls in a system involves the following five costs-

- (i) *Initial setup cost* : This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.
- (ii) *Executing cost* : This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system.
- (iii) *Correction costs* : The control has operated reliably in signalling an error or irregularity, the cost associated with the correction of error or irregularity.



- (iv) *Failure cost* : The control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.
- (v) *Maintenance costs* : The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.

The benefit of an internal control procedure must exceed its cost. Costs are easier to measure than benefits, however. The primary cost element is personnel, including the time to perform control procedures, the costs of hiring additional employees to achieve effective segregation of duties, and the costs of programming controls into an information system. Internal control benefits stem from reduced losses. One way to calculate benefits involves expected loss, the mathematical product of risk and exposure.

The benefit of a control procedure is the difference between the expected loss with the control procedure(s) and the expected loss without it.

*Determine Cost-Benefit Effectiveness* : After estimating benefits and costs, management determines if the control is cost beneficial. For example, at one of the multinational company, data errors occasionally required the entire payroll to be reprocessed, at a cost of Rs. 10,000. Management determined that a data validation step would reduce error risk from 15 per cent to 1 per cent, at a cost of Rs.600 per pay period. The cost-benefit analysis that management used to determine if the validation step should be employed is shown in Table 1.

	Without Validation Procedure	With Validation Procedure	Net Expected Difference
Cost to reprocess entire payroll	Rs. 10,000	Rs. 10,000	
Risk of payroll data errors	15%	1%	
Expected reprocessing cost (Rs. 10,000 × risk)	Rs. 1,500	Rs. 100	Rs. 1,400
Cost of validation procedure	Rs. 0	Rs. 600	Rs. (600)
Net expected benefit of validation procedure			Rs. 800

**Table 3.1 : Cost Effectiveness of Controls**

If the proposed payroll validation procedure is not utilised, then the expected loss to the company is Rs.1,500. Because the expected loss with the validation step is Rs.100, the control provides an expected benefit of Rs.1,400. After deducting the control costs of Rs.600, the validation step provides a net benefit of Rs.800 and clearly should be implemented.

In evaluating the costs and benefits of control procedures, management must consider factors other than those in the expected benefit calculation. For example, if an exposure threatens an organisation's existence, it may be worthwhile to spend more than indicated by the cost-benefit analysis to minimize the possibility that the organization will perish. This extra cost can be viewed as a catastrophic loss insurance premium.

## **3.18 Information Systems Control and Audit**

### **3.7 INFORMATION SYSTEMS CONTROL TECHNIQUES**

The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective information control framework, which comprises policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

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”.

#### **3.7.1 Objective of Controls**

The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Exposures are potential losses due to threats materializing. All exposures have causes. Some categories of exposures are:

- Errors or omissions in data, procedure, processing, judgment and comparison.
- Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison.
- Inefficient activity in procedures, processing and comparison.
- Some of the critical control considerations in a computerized environment are:
- Lack of management understanding of IS risks and lack of necessary IS and related controls.
- Absence or inadequate IS control framework.
- Absence of or weak general controls and IS controls.
- Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff.
- Complexity of implementation of controls in distributed computing environments and extended enterprises.
- Lack of control features or their implementation in highly technology driven environments.
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

Control objective is defined as “A statement of the desired result or purpose to be achieved by implementing control procedures in particular IT process or activity”. Control objectives define what is sought to be accomplished by implementing the control and the purpose thereof. The control objectives serve two main purposes:

- (i) Outline the policies of the organization as laid down by the management.
- (ii) A benchmark for evaluating whether control objectives are met.

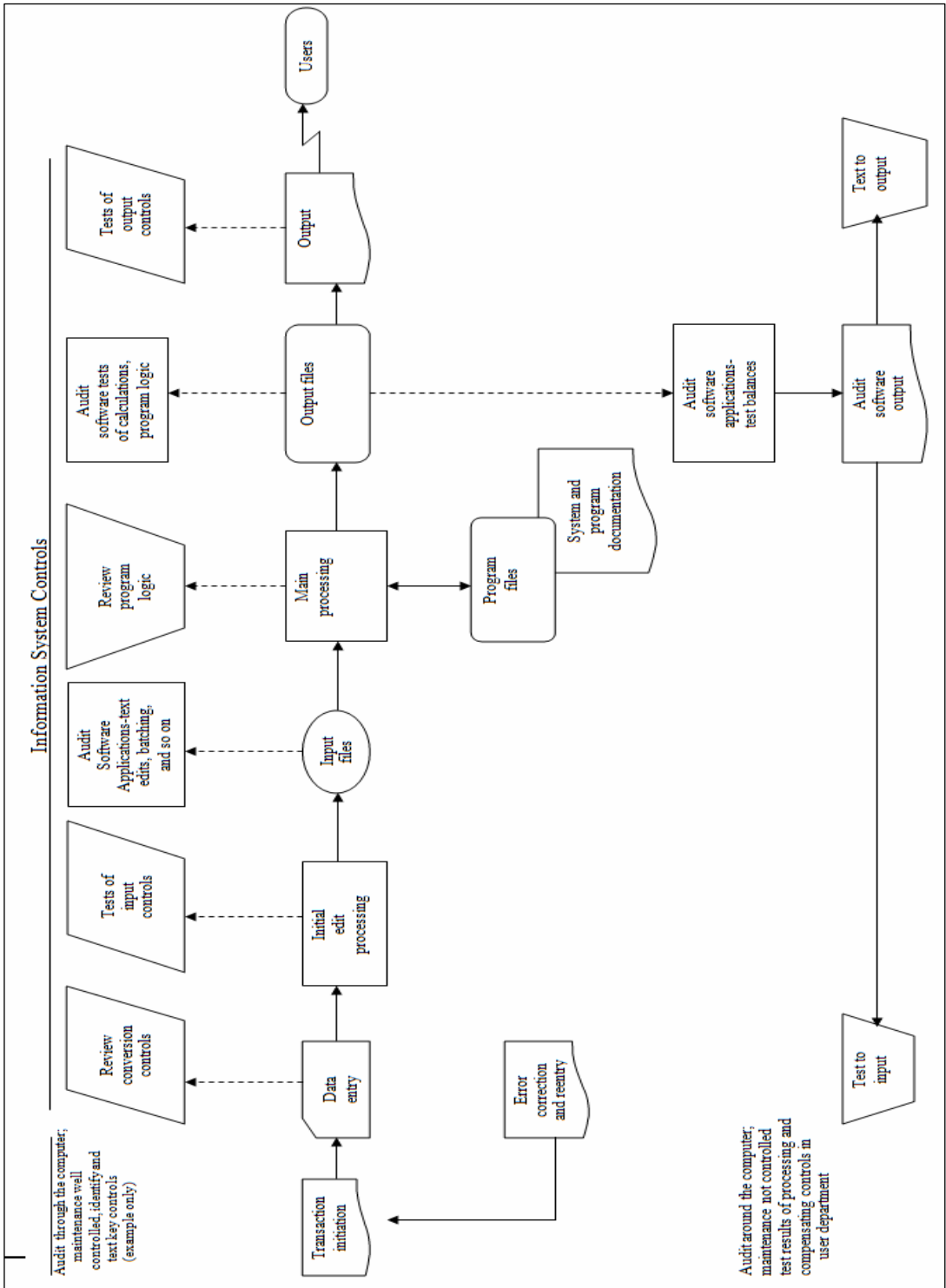
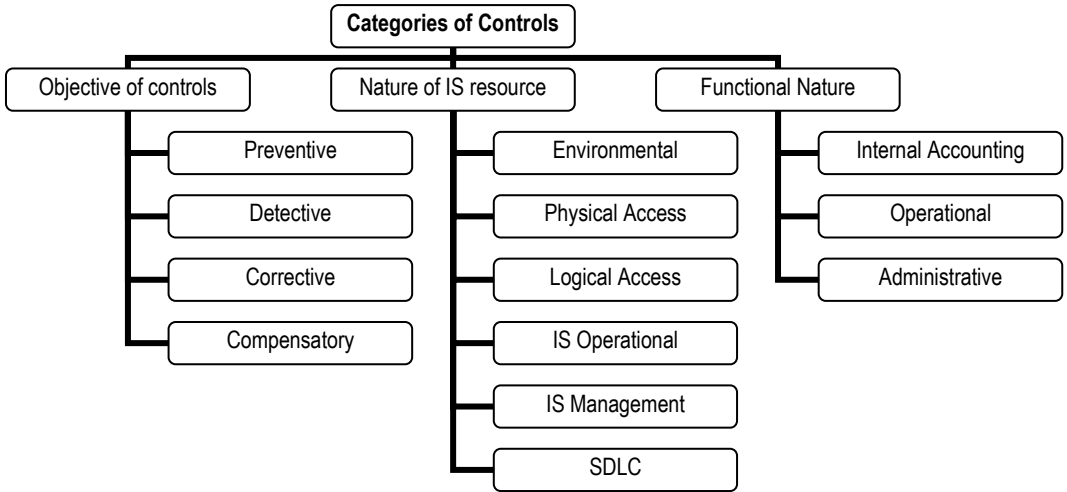


Fig. 3.5 : Information Systems Controls

### 3.20 Information Systems Control and Audit

#### 3.7.2 Categories of Controls

Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on computer controls. These categories are:



**Fig. 3.6 : Categories of Controls**

Based on the objective with which controls are designed or implemented, controls can be classified as:

(i) *Preventive Controls* : Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. The broad characteristics of preventive controls are:

- (i) A clear-cut understanding about the vulnerabilities of the asset
- (ii) Understanding probable threats
- (iii) Provision of necessary controls for probable threats from materializing

As has been discussed earlier in this section, any control can be implemented in both a manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Now let us discuss the examples of preventive controls and how the same control is implemented in different environments.

Examples of preventive controls

- Employ qualified personnel
- Segregation of duties
- Access control
- Vaccination against diseases
- Documentation

- Prescribing appropriate books for a course
- Training and retraining of staff
- Authorization of transaction
- Validation, edit checks in the application
- Firewalls
- Anti-virus software (sometimes this acts like a corrective control also), etc
- Passwords

The above list in no way is exhaustive, but is a mix of manual and computerized, preventive controls. The following table shows how the same purpose is achieved by using manual and computerized controls.

Purpose	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard	Use access control software, smart card, biometrics, etc.
Restricted unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications	Use access control, viz. User ID, password, smart card, etc.

**Table 3.2 : Preventive Controls**

(ii) *Detective Control* : These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.
- An established mechanism to refer the reported unlawful activities to the appropriate person or group
- Interaction with the preventive control to prevent such acts from occurring
- Surprise checks by supervisor

Examples of detective controls include

- Hash totals
- Check points in production jobs
- Echo control in telecommunications

### 3.22 Information Systems Control and Audit

- Error message over tape labels
- Duplicate checking of calculations
- Periodic performance reporting with variances
- Past-due accounts report
- The internal audit functions
- Intrusion detection system
- Cash counts and bank reconciliation
- Monitoring expenditures against budgeted amount

(iii) *Corrective Controls* : Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control. The main characteristics of the corrective controls are:

- Minimize the impact of the threat
- Identify the cause of the problem
- Remedy problems discovered by detective controls
- Get feedback from preventive and detective controls
- Correct error arising from a problem
- Modify the processing systems to minimize future occurrences of the problem

Examples of Corrective Controls

- Contingency planning
- Backup procedure
- Rerun procedures
- Treatment procedures for a disease
- Change input value to an application system
- Investigate budget variance and report violations.

(iv) *Compensatory Controls* : Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind—*the cost of the lock should not be more than the cost of the assets it protects*. Sometimes while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, there should be adequate compensatory measures which may although not be as

efficient as the appropriate control, can indubitably reduce the probability of threats to the assets. Such measures are called compensatory controls. Some examples of compensatory control given below will make the concept more clear.

Another classification of controls is based on the nature of such controls with regard to the nature of IS resources to which they are applied:

- (i) *Environmental controls* : Controls relating for housing IT resources such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.
- (ii) *Physical Access Controls* : Controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, video monitoring etc.
- (iii) *Logical Access Controls* : Controls relating to logical access to information resources such as operating systems controls, Application software boundary controls, networking controls, access to database objects, encryption controls etc.
- (iv) *IS Operational Controls* : Controls relating to IS operation, administration and its management such as day begin and day end controls, IS infrastructure management, Helpdesk operations etc.
- (v) *IS Management Controls* : Controls relating to IS management, administration, policies, procedures, standards' and practices, monitoring of IS operations, Steering committee etc.
- (vi) *SDLC Controls* : Controls relating to planning, design, development, testing, implementation and post implementation, change management of changes to application and other software.

Further another category of controls is based on their 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. The information system auditor will be most familiar with :

- (i) *Internal Accounting controls* : Controls which are intended to safeguard the client's assets and ensure the reliability of the financial records;
- (ii) *Operational controls* : These deals with the day to day operations, functions and activities to ensure that the operational activities are contributing to business objectives.
- (iii) *Administrative controls* : These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

### 3.24 Information Systems Control and Audit

#### 3.7.3 Control Techniques

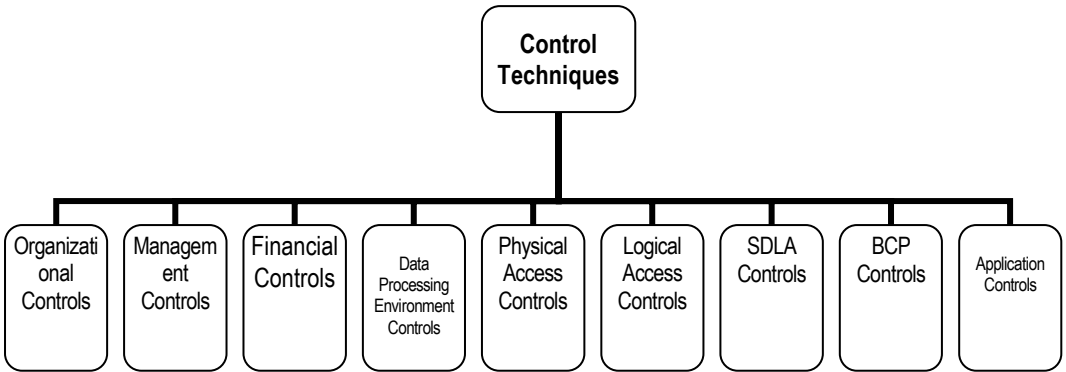


Fig. 3.7 : Control Techniques

#### 3.7.4 Organizational Controls

Enterprise controls are concerned with the decision-making processes that lead to management authorization of transactions. Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources. Combining data processing into the business units would be too much responsibility for one manager. Organizational control techniques include documentation of :

- Reporting responsibility and authority of each function,
- Definition of responsibilities and objectives of each functions,
- Policies and procedures,
- Job descriptions, and
- Segregation of duties.

(i) *Responsibilities and objectives* : Each IS function must be clearly defined and documented, including systems software, application programming and systems development, database administration, and operations. The senior manager, of all these groups, and managers of the individual groups make up the IS management team responsible for the effective and efficient utilization of IS resources. Their responsibilities include:

- Providing information to senior management on the IS resources, to enable senior management to meet strategic objectives.
- Planning for expansion of IS resources
- Controlling the use of IS resources
- Implementing activities and functions that support accomplishment of company's strategic plan.



(ii) *Policies, standards, procedures and practices* : These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Policies establish the rules or boundaries of authority delegated to individuals in the enterprise.

Procedures establish the instructions that individuals must follow to complete their daily assigned tasks. Mandating that all requests for changes to existing programs must be approved by user and IS management before programmers and analyst can work on them is an example of a policy. Documented instructions for filling out a standard change request form, how to justify the costs of the change, how to specify the changes needed, how to obtain approvals, and who to obtain the approvals from are examples of procedures. Documented policies should exist in IS for:

- Use of IS resources,
- Physical security,
- Data security
- On-line security,
- Microcomputer use,
- Reviewing, evaluating, and purchasing hardware and software,
- System development methodology, and
- Application program changes.

Documented procedures should exist for all data processing activities.

(iii) *Job descriptions* : These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee. All jobs must have a current, documented job description readily available to the employee. Job descriptions establish responsibility and the accountability of the employee's actions.

(iv) *Segregation of duties* : This is a common control technique aimed at separating conflicting job duties, primarily to discourage fraud, because separating duties makes collusion necessary to commit a fraud. Such separation can also force an accuracy check of one-person work by another, so that employees to some extent police each other. Examples of segregation of duties are:

- Systems software programming group from the application programming group
- Database administration group from other data processing activities
- Computer hardware operations from the other groups
- Application programming group into various subgroups for individual application systems
- Systems analyst function from the programming function
- Physical, data, and online security group(s) from the other IS functions.
- *IS Audit*

### **3.26 Information Systems Control and Audit**

It is the responsibility of the senior management to implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. From a functional perspective, segregation of duties should be maintained between the following functions:

- Information systems use
- Data entry
- Computer operation
- Network management
- System administration
- Systems development and maintenance
- Change management
- Security administration
- Security audit

#### **3.7.5 Management Controls**

The controls adopted by the management of an enterprise are to ensure that the information systems function correctly and that they meet the strategic business objectives. The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled. The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organisation. The high level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organisation down (i.e) the responsibility still lies with the senior management.

The controls to consider when reviewing the organisation and management controls in an IS system shall include:

- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organisational structure.
- **An official IT structure:** There should be a prescribed organisation structure with all staff deliberated on their roles and responsibilities by written down and agreed job descriptions.
- **An IT steering committee:** The steering committee shall comprise of user representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

### 3.7.6 Financial Control Techniques

These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

(i) *Authorization* : This entails obtaining the authority to perform some act typically access to such assets as accounting or application entries.

(ii) *Budgets* : These estimates of the amount of time or money expected to be spent during a particular period of time, project, or event. The budget alone is not an effective control-budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

(iii) *Cancellation of documents* : This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.

(iv) *Documentation* : This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.

(v) *Dual control* : This entails having two people simultaneously access an asset. For example, the depositories of banks' 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people : once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.

(vi) *Input/ output verification* : This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.

(vii) *Safekeeping* : This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

(viii) *Segregation of duties* : This entails assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check of the other persons work. For example, the responsibilities for making financial entries to the application and to the general ledger should be separated.

(ix) *Sequentially numbered documents* : These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

## **3.28 Information Systems Control and Audit**

(x) *Supervisory review* : This refer to review of specific work by a supervisor : but what is not obvious is that this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

### **3.7.7 Data Processing Environment Controls**

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

### **3.7.8 Physical Access Controls**

These controls are personnel; hardware and software related and include procedures exercised on access by employees/outside to IT resources. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy.

These Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to individuals who have been authorized to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited. The other measures relate to Visitor Escort, Personnel Health and Safety, Protection against Environmental Factors and Uninterruptible Power Supply.

### **3.7.9 Logical Access Controls**

These controls are software related and include procedures exercised in the IS software through access controls through system software and application software. Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and access control, user identification and authorization profiles, incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

### **3.7.10 SDLC (System Development Life Cycle) controls**

These are functions and activities generally performed manually that control the development of application systems, either through in-house design and programming or package purchase. The first control requirement is system development standards that specify the

activities that should occur in each system development life cycle (SDLC) phase. For example, these standards specify the type and quantity of testing that should be conducted. The second element of controls is documented procedures communicate how the activities in each phase should be accomplished. These procedures establish control functions in each phase.

### **3.7.11 Business Continuity (BCP) Controls**

These controls relate to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption. The controls include criticality classification, alternative procedures, back-up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity activation, fallback and resumption plans, risk management activities, assessment of single points of failure and problem management.

### **3.7.12 Application Control Techniques**

These include the programmatic routines within the application program code. The financial controls, discussed earlier, are performed by the user to help ensure the accuracy of application formed by the use to help ensure the accuracy of application processing. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, data ownership, data administration policies, data models and data representation standards, integration and consistency across platforms, legal and regulatory requirements. Any function or activity that works to ensure the processing accuracy of the application can be considered an application control.

**3.7.13 Audit Trails :** Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines which events will be recorded in the log. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

Applications system Controls involve ensuring that individual application systems safeguard assets (reducing expected losses), maintain data integrity (ensuring complete, accurate and

### 3.30 Information Systems Control and Audit

authorized data) and achieve objectives effectively and efficiently from the perspective of users of the system from within and outside the organization.

#### 3.7.14 Audit Trail Objectives

Audit trails can be used to support security objectives in three ways :

- Detecting unauthorized access to the system,
- Facilitating the reconstruction of events, and
- Promoting personal accountability.

Each of these is described below:

(i) *Detecting Unauthorized Access* : Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed, real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

(ii) *Reconstructing Events* : Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

(iii) *Personal Accountability* : Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior . Individual are likely to violate an organization's security policy if they know that their actions are recorded in an audit log.

*Implementing an Audit Trail* : The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls. Audit logs, however, can generate data in overwhelming detail. Important information can easily get lost among the superfluous detail of daily operation. Thus, poorly designed logs can actually be dysfunctional.

### 3.8 USER CONTROLS

Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface

between the user and the business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his job description and assigned responsibilities. He is able to relate to the advantages of technology when he is able to interact with the computer system from the perspective of meeting his job objectives. From the point of view of users, it is the applications that drive the business logic. The following table lists the user controls that are to be exercised for system effectiveness and efficiency.

Controls	Scope	Audit Trail	
		Accounting	Operations
Boundary Controls	<p>Establishes interface between the user of the system and the system itself.</p> <p>The system must ensure that it has an authentic user.</p> <p>Users must ensure that they are given authentic resources.</p> <p>Users allowed using resources in restricted ways.</p>	<p>Authentication of the users of the system(identity)</p> <p>Resources and Action privileges requested/provided/denied.</p> <p>Number of sign-on attempts</p> <p>In case of digital signatures for authentication audit trail includes- Registration of public keys, Registration of signatures and Notification of key compromises.</p>	<p>Resource usage from log-on to log-out time.</p> <p>Say, intrusion-detection control to monitor the amount of process time consumed by a user to detect deviations from the past trails for a similar process by the user.</p>
Input Controls	<p>Responsible for the data and instructions in to the information system.</p> <p>Input Controls are validation and error detection of data input into the system.</p>	<p>Originator of the data/instruction, time and date the data/instruction entered, physical device used by the user, type of data/instruction and output processed.</p>	<p>Number of read errors, Number of keying errors, Frequency of instruction usage and time-taken to process an instruction.</p>
Processing Controls	<p>Responsible for computing, sorting, classifying and summarizing data.</p> <p>It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.</p>	<p>To trace and replicate the processing performed on a data item.</p> <p>Triggered transactions to monitor input data entry, intermediate results and output data values.</p>	<p>A comprehensive log on resource consumption data with respect to hardware(processor time, peripherals, memory, communication etc)</p> <p>Software (programs, instructions),Data(file access, frequency of access)</p>

### 3.32 Information Systems Control and Audit

Output Controls	To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.	It shows what output was presented to users, who received the output, when the output was received and what action were taken with the output.	Maintains the record of resources consumed – graphs, images, report pages, printing time and display rate.
Database Controls	Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains declarative data-payroll file storing information about the pay rates for each employee. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.	A unique time stamp to all transactions, before and after images of the data item on which a transaction is applied and any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.	To maintain a chronology of events that consumes resources of the data base. The response time on the queries made on the data base.

**Table 3.3 : User controls and Audit Trail**

#### 3.8.1 User controls : Error Identification, Correction and Recovery Controls

(i) *Boundary Controls* : The major controls of the boundary system are the access control mechanisms. Access controls are implemented with an access control mechanism and links the authentic users to the authorized resources they are permitted to access. The access control mechanism the three steps of identification, authentication and authorization with respect to the access control policy implemented as shown in the Fig.3.8. The user can provide three classes of input information for the authentication process and gain access control to his required resources. The three classes of information with respect to the corresponding input to the boundary control are summarized in the table below.



Class of information	Types of input
Personal Information	Name, Birth date, account number, password, PIN
Personal characteristics	Fingerprint, voice, hand size, signature, retinal pattern.
Personal objects	Identification cards, badge, key, finger ring.

Table 3.4 : Authentic Information

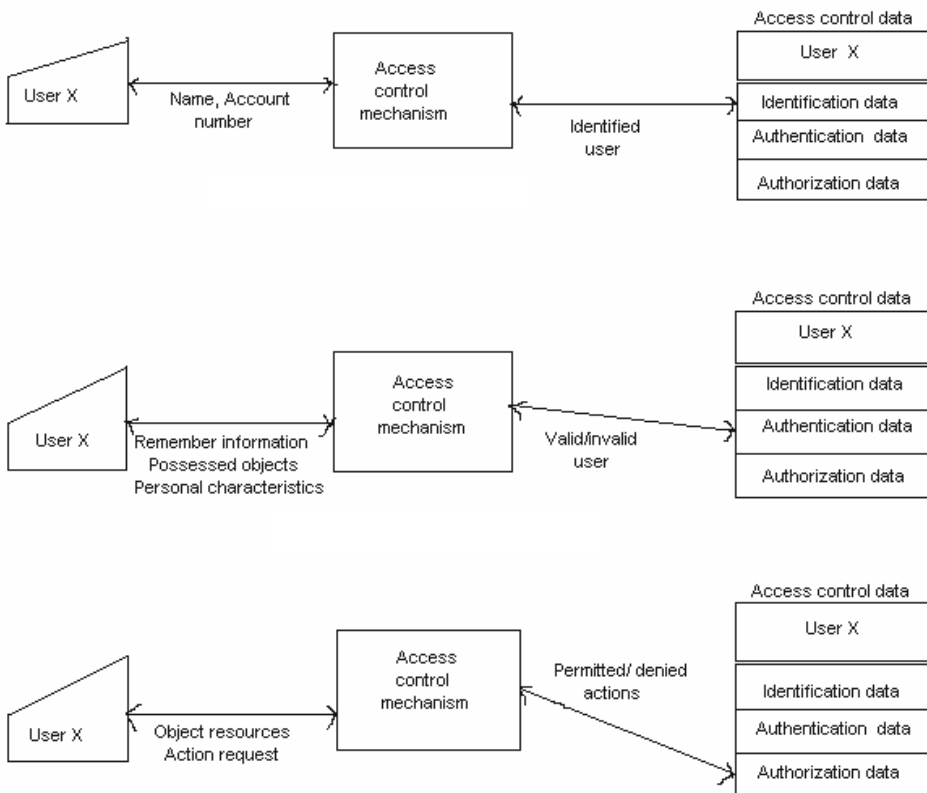
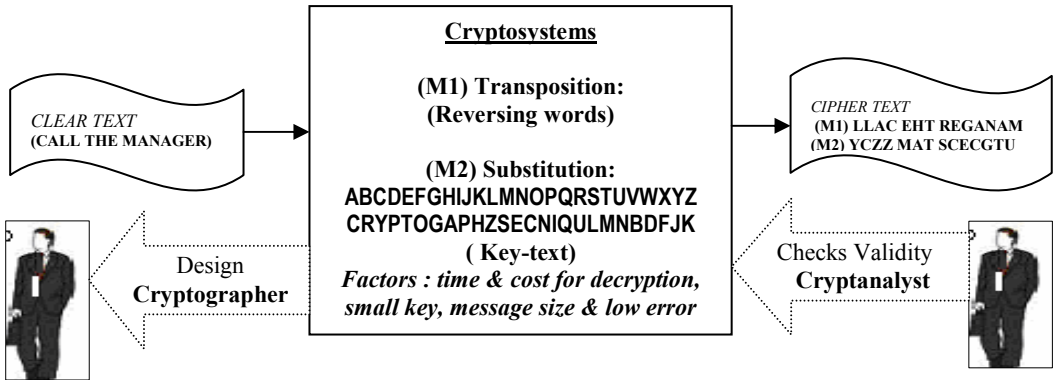


Fig. 3.8 : Identification/Authentication /Authorization Process

Boundary control techniques are:

- Cryptography** : deals with programs for transforming data into codes that are meaningless to anyone who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution)

### 3.34 Information Systems Control and Audit



**Fig. 3.9 : Cryptography**

- **Passwords** : User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
- **Personal Identification Numbers (PIN)** : The personal identification number is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **Identification Cards** : Identification cards are used to store information required in an authentication process. These cards used to identify a user are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.



**Fig. 3.10 : What you have (Token), what you know (password/PIN) and who you are (Biometric)**

(ii) **Input Controls** : are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since substantial time is spent on input of data, involve human intervention and are therefore error and fraud prone. Data codes are used to uniquely identify an entity or identify an entity as a member of a group or set. Poorly designed data codes cause recording and keying errors. Auditors should

evaluate the quality of coding systems to analyze their impact on the integrity and accurateness of data keyed into the system.

Types of data coding errors:

- Addition : Addition of an extra character in a code e.g. 54329 coded as 543219
- Truncation : Omission of characters in the code e.g. 54329 coded as 5439
- Transcription : Recording wrong characters 54329 coded as 55329
- Transposition : Reversing adjacent characters 54329 coded as 453219
- Double transposition : Reversing characters separated by one or more characters i.e., 54329 is entered as 52349.
- Factors affecting coding errors as follows:
  - *Length of the code* : Long codes are naturally prone to more errors. Long codes should be broken using hyphens, slashes or spaces to reduce coding errors.
  - *Alphabetic numeric mix* : The code should provide for grouping of alphabets and numerical separately if both are used. Intermingling both would result in more errors.
  - *Choice of characters* : Certain alphabets are confused with numerical such as B, I, O, S, V and Z would be confused with 8,1,0,5,U, 2 when written on source document and entered into the system. Such as characters should be avoided
  - *Mixing uppercase/lowercase fonts* : Upper case and lower case should NOT be mixed when using codes since they delay the process of keying in due to usage of the shift key.
  - Further such codes are prone to errors.
  - *Sequence of characters* : Character sequence should be maintained as much as possible. Such as using ABC instead of ACB.

Errors made in transcribing and keying data can have serious consequences on the enterprise. Control used to guard against these types of errors is a check digit. Check digits are redundant digits that helps verify the accuracy of other characters in the code that is checked. The program recalculates the check digits and compares with the check digit in the code when the code is entered to verify if the code is correct. Check digits may be prefixes or suffixes to the actual data. When the code is entered, a program recalculates the check digit to determine the accuracy.

- *Existence/Recovery Controls* : Controls relating to data input are critical. It might be necessary to reprocess input data in the event master files are lost, corrupted, or destroyed. Controls relating to instructions are often in the form of changes to data which are recorded in the audit trail. Thus source documents or transaction listings are to be stored securely for longer periods for reasons – compliance with statutory requirements.

(iii) *Processing Controls* : Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the

### 3.36 Information Systems Control and Audit

accuracy of data being processed. Normally the processing controls are enforced through the database management system that stores the data. However, adequate controls should be enforced through the front end application system also to have consistency in the control process.

Data processing controls are:

- *Run-to-run totals* : These help in verifying data that is subject to process through different stages. If the current balance of an invoice ledger is Rs.150,000 and the additional invoices for the period is of total Rs.20,000 then the total sales value should be Rs.170,000. A specific record (probably the last record) can be used to maintain the control total.
- *Reasonableness verification* : Two or more fields can be compared and cross verified to ensure their correctness. For example the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.
- *Edit checks* : Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.
- *Field initialization* : Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e., setting all values to zero before inserting the field or record.
- *Exception reports* : Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and why the particular transaction was not processed or what is the error in processing the transaction. For example, while processing a journal entry if only debit entry was updated and the credit entry was not updated due to absence of one of the important fields, then the exception report would detail the transaction code, and why it was not updated in the database.
- *Existence/Recovery Controls* : The check-point/restart logs, facility is a short-term backup and recovery control that enables a system to be recovered if failure is temporary and localized.

(iv) *Output Controls* : ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a floppy disk or CD-ROM or it can be a Word document on the computer's hard disk. Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent. Output controls have to be enforced both in a batch-processing environment as well as in an online environment.

- *Storage and logging of sensitive, critical forms* : Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments etc.

- *Logging of output program executions* : When programs used for output of data are executed, it should be logged and monitored. In the absence of control over such output program executions, confidentiality of data could be compromised.
  - *Spooling/Queuing* : “Spool” is an acronym for “Simultaneous Peripherals Operations Online”. This is a process used to ensure that the user is able to continue working, even before the print operation is completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then “spooled” to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer. This queue should not be subject to unauthorized modifications.
  - *Controls over printing* : it should be ensured that unauthorized disclosure of information printed is prevented. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
  - *Report distribution and collection controls* : Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained as to what reports were generated and to whom it was distributed. Where users have to collect reports the user should be responsible for timely collection of the report especially if it is printed in a public area. A log should be maintained as to what reports were printed and which of them were collected. Uncollected reports should be stored securely.
  - *Retention controls* : Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period
  - *Existence/Recovery Controls* : are needed to recover output in the event that it is lost or destroyed. If the output is written to a spool of files or report files and has been kept, then recovering and new generation is easy and straight-forward. The state of a transaction at a point of time with before and after images. Check/restart helps in recovery when a hardware problem causes a program that prints customer invoices to abort in midstream.
- (v) *Database Controls* : Protecting the integrity of a database when application software acts as an interface to interact between the user and the database are called the update controls and report controls.

The update controls are :

- *Sequence Check Transaction and Master Files* : Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updation, insertion or deletion of records in the master file with respect to

### 3.38 Information Systems Control and Audit

the transaction records. If errors in this stage are overlooked it leads to corruption of the critical data.

- *Ensure All Records on Files are processed* : While processing the transaction file records mapped to the respective master file the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.
- *Process multiple transactions for a single record in the correct order* : Multiple transactions can occur based on a single master record (eg. dispatch of a product to different distribution centers) Here the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.
- *Maintain a suspense account* : When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record then these transactions are maintained in a suspense account. A non-zero balance of the suspense accounts reflect the errors to be corrected.

The Report controls are:

- *Standing Data* : Application programs use many internal tables to perform various functions like say gross pay calculation, billing calculation based on a price table, bank interest calculation etc,. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Any changes or errors in these tables would have an adverse effect on the organizations basic functions. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.
- *Print-Run-to Run control Totals* : Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.
- *Print Suspense Account Entries* : Similar to the update controls the suspense account entries are to be periodically monitors with the respective error file and action taken on time.
- *Existence/Recovery Controls* : The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup strategies are implemented using prior version and log of transactions or changes to the database. Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

### 3.9 SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS

It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems and related technologies. Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion. Methodology also should make it possible for management to trace information inputs from their source to their final disposition or from their final disposition back to the original source (the audit trail)

Software development is an integrated process spanning the entire IT organization. The term “life cycle” can be taken to represent the collection of agreed upon steps to control development, modification and distribution of code. While change and configuration management denote separate entities exerting policy over standards for the production environment, the design of these standards and all efforts between these points can be characterized as the world of software development and code.

The IT Governance Institute (ITGI) has produced clear and aligned frameworks for the representation of software development best practice. The newly numbered control process Acquire and Implement 7 (AI7), *Install and accredit solutions and changes of Control Objectives for Information and related Technology (COBIT®)4.0* is the most widely adopted matrix and measure for all integrated IT and enterprise controls. It aligns with the concepts of the Capability Maturity Model (CMM), IT Infrastructure Library (ITIL), ISO/IEC 17799 and COSO, COBIT 4.0 advances with increased attention in the areas of SDLC, quality and project risk management.

*Install and accredit solutions and changes* is the high-level functional area that captures the greatest number of features representing the activities related to SDLC or release management. AI7 as stated in the standards document:

*New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed expectations and outcomes.*

AI7 includes inputs and outputs to configuration, project, change, maintenance and acquisition programs. With handoffs based in triggers, performance goals, measurements and business-based criteria, documented consensus, and tested results, evidence of their implementation is best suited to automated systems. For a detail discussions on the standards (COBIT, ITIL and CMMI) refer to chapter 8.

### **3.9.1. Controls over the System Development phases and Auditor’s Role**

The SDLC phases define an agenda of issues that stakeholders (management, users, and software developers) in the system development process must address. The quality of the systems development will depend on how well the stakeholders come to grips with the issues in the context of the project. The following subsections will examine the controls that are important in the major system development phases.

### **3.9.2. Problem definition**

In this phase the stakeholders must attempt to come to an understanding of the nature of the problem or opportunity they are addressing. The information system requirement can be conceived through a formal process –systems planning or a need for the information system support need felt by chance.

### **3.40 Information Systems Control and Audit**

#### **Controls**

- The need for the information system in the preview of the business requirement.
- Support and priority for the information system by the management.
- Level of acceptance among the stakeholders on the need for change.
- The investigation and strategy by which the need for the system is justified.

#### **Auditor's Role**

The Auditors are concerned with-

- If the stakeholders have reached an agreement on the existence of a problem or opportunity.
- An understanding of the threats to asset safeguarding, data integrity, system effectiveness and system efficiency associated with the solutions proposed for the system.

### **3.9.3. Management of the change process**

Management of the change process runs parallel to all the phases of SDLC.

#### **Controls**

Project Management involves addressing matters as budgeting, exception reporting, checkpoints and user coordination.

Change-facilitation deals with the following critical activities-

- Preparing the organization for an unrestricted change by feedback, training, participatory decision making and promote the need for change.
- Complete changeover to the new system.
- To help users adapt to their new roles and re-freezing activities by providing positive feedback and behavioral patterns.

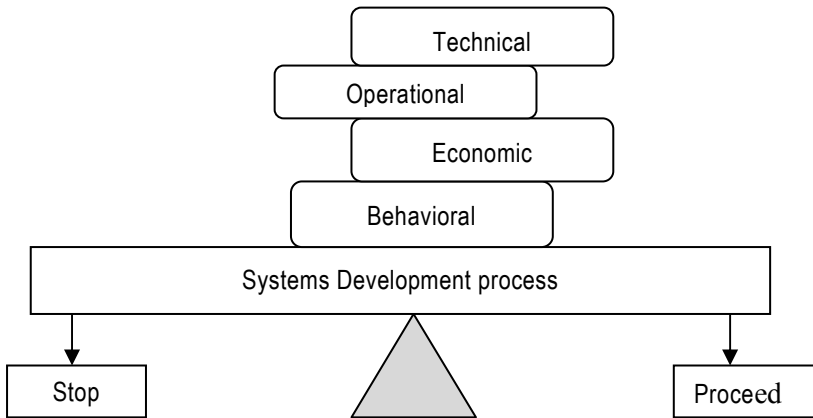
#### **Auditor's Role**

- To evaluate the quality of decisions made with respect to project management and change facilitation.
- If the proposed system is small, it has a localized impact on users and change management can be done in-house with less material concerns.
- If the proposed system is large, it has high-levels of requirements and technological uncertainty and organization structures and jobs will have significant effect.



### 3.9.4. Entry and feasibility assessment

The specific techniques used to evaluate the feasibility of systems depend on the type and size of the system being proposed as illustrated in the fig 3.11.



**Fig. 3.11 : Feasibility criteria for SDLC.**

#### Controls

- *Technical Feasibility* : Can technology be acquired, developed or available to support the proposed project?
- *Operational Feasibility* : Can the system be designed to process inputs and give required outputs?
- *Economic Feasibility* : The proposed system is deemed feasible only if the benefits exceed all the cost requirements.
- *Behavioral Feasibility* : Can the system improve the quality of work life of the users?

#### Auditor's Role

- If the change proposed is not imposed upon stakeholders.
- The behavioral impact on the users and the problems that arise in the proposed system.
- The material losses incurred as result of the development, implementation, operation or maintenance of the system.

### 3.9.5. Analysis of the existing system

To design a new system, first it is essential to understand the existing system. An analysis should include-

- A study of the existing organizational history, structure and culture
- A study of the existing information flows

## 3.42 Information Systems Control and Audit

### Controls

The study of the history of systems in an organization gives an idea of : the types of systems that have been extremely useful; issues that have not been addressed over a period; and new issues that require attention. The organizational structure gives an idea of the power equations within an organization.

The study of the existing information flows is done using formal methodologies like top-down structured analysis (waterfall), prototyping and agile models to understand the system. The formal methodology helps to analyze data flows and describes logic and policy. These methodologies and tools were discussed in detail in chapter 2.

### Auditor's Role

- The need to study the aspects of the present organizational structure, history and culture.
- The context in which the decisions for the new proposed system choice was made and its implications for the conduct of the remainder of the audit.
- To evaluate the quality of methodologies used and strengths of the decisions taken.
- The usage of high-quality tools in analysis and documentation of the existing product.

### 3.9.6. Formulation of strategic Requirements (System Design)

The strategic requirements also called as the SRS (System Requirements Specification) document identifies the perceived deficiencies in the existing system of the existing or perceived new system are evaluated.

### Controls

Align the business requirements with the preview of management's objectives, user's goals and elicitation of the requirements and system-design work concurrently.

### Auditor's Role

- Evaluate the quality of the SRS design work.
- The feasibility of the system-design proposed.
- To assess the identified procedures and substantial behavioral impact on the users within the proposed system.

### 3.9.7. Organizational and job design

Adapting the organizational structures and job responsibility with respect to the proposed system often leads to behavioral problems among its stakeholders and may result in implementation failure.

### Controls

- The roles and responsibilities of users of the system are to be defined using formal traditional mechanisms or open-ended structures to facilitate adaptation.
- A clear design of the responsibilities in the initial design phase is critical in achieving the goals; a detail discussion on the roles of responsibilities during SDLC is given in chapter 2.

### Auditor's Role

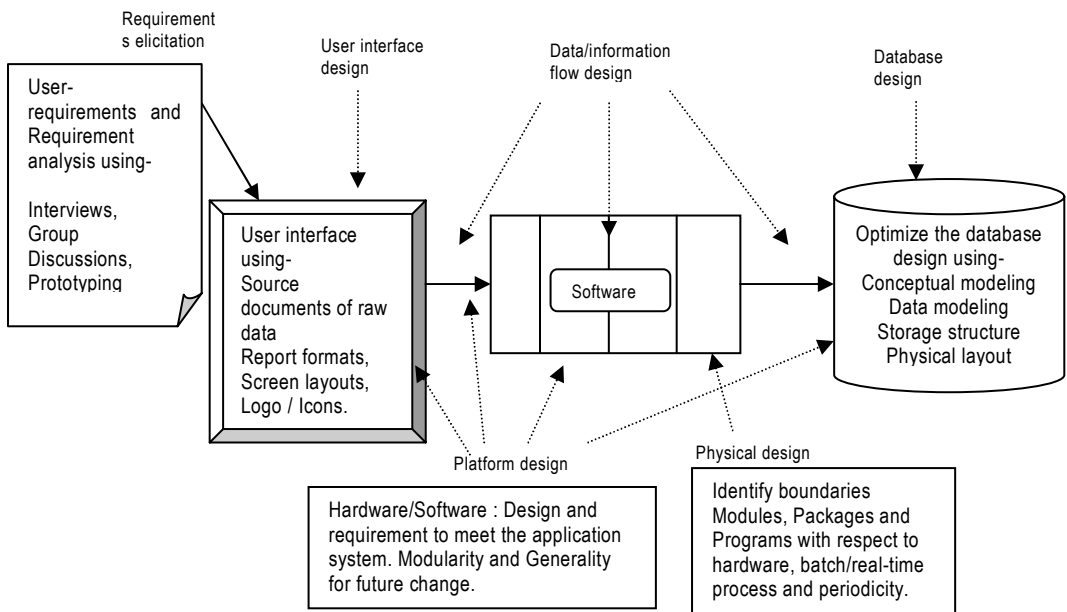
- The auditor is to assess the assigned responsibility and process used to resolve conflicts.
- To assess the control risk associated with the responsibilities during SDLC with substantive testing.

### 3.9.8. Information processing systems design

From efficiency viewpoint the reliability of the controls designed into the system are to be evaluated to meet the strategic requirements of the proposed system.

### Controls

The major control activities in the processing systems design phase are depicted in the Fig. 3.12.



**Fig. 3.12 : Controls in processing systems design**

### Auditor's Role

- To evaluate the appropriateness of the requirements-elicitation strategy in the scope of the stakeholder and the quality of the requirements document.
- The system design needs to capture all data/information flow within the system.
- The structure of the database design and cost evaluation of the data model is to be evaluated.
- User interface is the source of user interactivity with the system and is a critical activity. The design and quality of the interface needs to follow best design practices.

### **3.44 Information Systems Control and Audit**

- The efficiency of the tasks assigned to the appropriate hardware and software resources of the physical design of the system. The performance of a critical system can be evaluated with simulations.

#### **3.9.9. Application Software Acquisition/Selection Process**

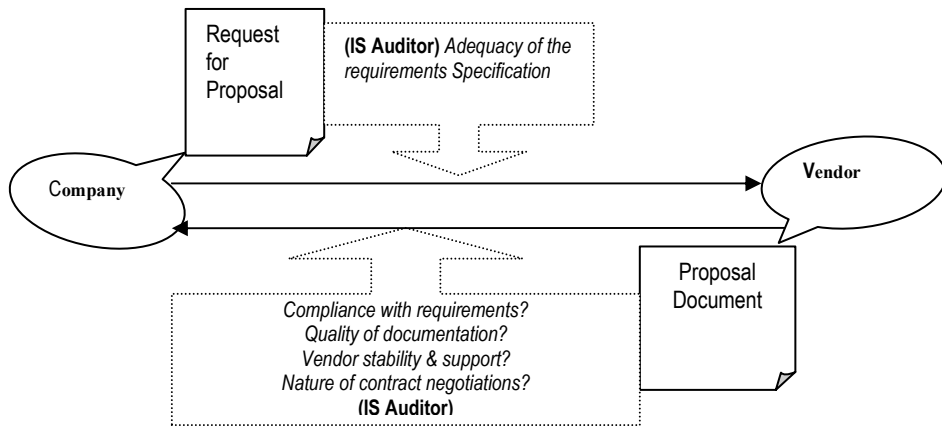
Once the information flow and processing within a system is identified and designed then the application software may be acquired or developed in-house.

#### **Controls**

In case of acquisition of a software system the following controls need to be in place:

- Information and system requirements need to meet business and system goals, system processes to be accomplished, and the deliverables and expectations for the system. The techniques are interviews, deriving requirements from existing systems, identifying characteristics from related system, and discovering them from a prototype or pilot system.
- A feasibility analysis to define the constraints or limitations for each alternative system from a technical as well as a business perspective. It should also include economic, technical, operational, schedule, legal or contractual, and political feasibility of the system within the organization scope.
- A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, and contractual) as well as the evaluation criteria used in the vendor selection process. The selection criteria should prevent any misunderstanding or misinterpretation.
- While identifying various alternatives software acquisition involves the critical task of vendor evaluation. The vendor evaluation process considers the following:
  - ◆ Stability of the supplier company,
  - ◆ Volatility of system upgrades,
  - ◆ Existing customer base,
  - ◆ Supplier's ability to provide support,
  - ◆ Cost-benefits of the hardware/software in support of the supplier application, and
  - ◆ Customized modifications of the application software.

## Auditor's Role



**Fig. 3.13 : Auditor's Role : Hardware/Software Acquisition**

- To highlight risks before a vendor contract or a software agreement contract is signed.
- Ensure that the decision to acquire software should flow from the thorough feasibility study, vendor evaluation and RFP (Request for proposal) adequacy checked for.
- A RFP would include transaction volume, data base size, turnaround time and response time requirements and vendor responsibilities.
- The auditor needs to also check the criteria for pre-qualification of vendors and sufficient documentation available to justify the selection of the final vendor / product.
- The auditor may also collect information through his own sources on vendor viability, support infrastructure, service record and the like.
- Thorough review of the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures such as, source code availability and third party maintenance support.
- To ensure that the contract went through legal scrutiny before it was signed.

### 3.10 CONTROL OVER SYSTEM AND PROGRAM CHANGES

#### 3.10.1. Management of the change process

One of the most critical areas of control in an information systems environment is change control. The complexity of hardware, software, and application relationships in the operating environment needs well defined, planned, coordinated, tested, and implemented change management. Management of the change process runs parallel to all the phases of SDLC. The change process involves the following tasks:

- Provide feedback to the system stakeholders
- Prevents system disruptions which may lead to business losses

### 3.46 Information Systems Control and Audit

- Accepted changeover to a new system across the organization
- Helps users to adapt to new roles
- Documentation and follow up on the recommended and implemented process changes.
- The proposed change need to be reviewed to identify potential conflicts with other systems.
- The change management process is to be reviewed periodically to evaluate its effectiveness.

All requests for change are set on priority of urgency is the responsibility of a change control board or IT steering committee. The change board and steering committee communicate their views through an individual given the role of the change manager. The priority of changes is determined by assessing the cost of the change and its impact on the business and its resources.

Quality assurance, security, audit, regulatory compliance, network, and end-user personnel should be appropriately included in change management processes. Risk and security review should be done whenever a system modification is implemented to ensure controls remain in place.

Change management (sometimes referred to as configuration management) involves establishing baseline versions of products, services, and procedures and ensuring all changes are approved, documented, and disseminated. Change controls should address all aspects of an organization's technology environment including software programs, hardware and software configurations, operational standards and procedures, and project management activities. Management should establish change controls that address major, routine, and emergency software modifications and software patches.

#### 3.10.2 System Change Controls

Project Management involves addressing matters as budgeting, exception reporting, checkpoints and user coordination.

Change-facilitation deals with the following critical activities-

- Preparing the organization for an unrestricted change by feedback, training, participatory decision making and promote the need for change.
- Complete changeover to the new system.
- To help users adapt to their new roles and re-freezing activities by providing positive feedback and behavioral patterns.

#### Auditor's Role

- To evaluate the quality of decisions made with respect to project management and change facilitation.
- If the proposed system is small, it has a localized impact on users and change management can be done in-house with less material concerns.

If the proposed system is large, it has high-levels of requirements and technological uncertainty and organization structures and jobs will have significant effect.

<b>CHANGE FACILITATION</b>	<b>SDLC Phases</b>	<b>PROJECT MANAGEMENT</b>
	Planning-Problem Definition	
	System Analysis	
	System Design	
	System Development	
	System Implementation	

**Fig. 3.14 : Change Management and Control Process**

The Change Control process of a system under development is to address the problems not detected during system design or testing and change in user requirements. A change control evaluation includes checks on problems reporting, tracking, prioritizing, and resolving, and if changes are authorized, tested, documented, and communicated through a legitimate management responsibility. The risks the change control processes deal with are:

- System outages due to error, omissions, or malicious intent,
- Data loss or errors due to error, omissions, or malicious intent,
- Unauthorized changes,
- Fraud/abuse to company systems and/or data,
- Repeated errors, and
- Reruns of system or application processes.

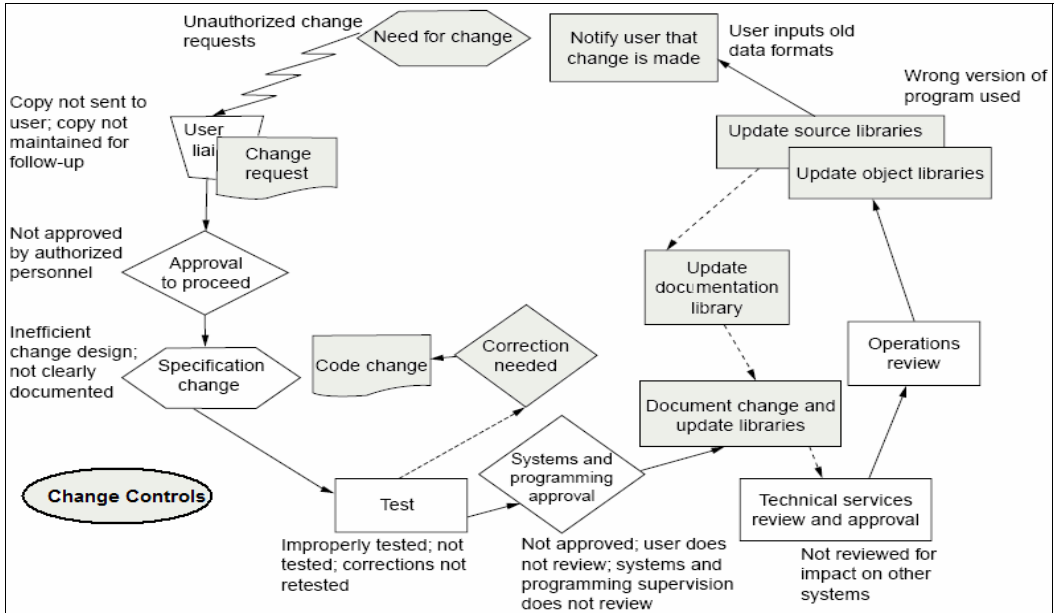
The objective of a change management review are to ensure that changes made to the system and programs do not adversely affect system, application, or data availability or integrity. Auditors need to verify that all changes made to the systems and programs are appropriately authorized and documented.

### 3.10.3 Program Change Controls

Application software programs are designed to support a specific business operation such as payroll or loan accounting. Implementing controls over the modification of application software programs is to ensure that only authorized programs and authorized modifications are implemented. Standard organization level policies, procedures, and techniques are to be followed to ensure that all programs and program modifications are properly authorized, tested, and approved and the responsibility of access to implement changes and distribution of programs is carefully controlled. Failure of proper controls leads to risks in software

### 3.48 Information Systems Control and Audit

security like virus threats deliberately omitted or turned off processing irregularities or malicious code.



**Fig. 3.15 : Program Change Controls and Potential Risks**

#### Auditor's Role

- To ensure maintenance of software program code libraries (archives of code and executable code) Software updating is to be done from a central repository.
- Appropriate backups of the system's data and programs to store the various versions of files should be made before the change.
- Tacking of program changes are to be accounted for through version procedure.
- A formal handover process so that authorized personnel are involved in the software changes testing and updation process with clearly assigned responsibilities skills, knowledge, and training to perform responsibilities.
- Standardized software updation (release) management policies, procedures, and tools;
- Updated technology inventory of all hardware, software, and services that are used based on the criticality of the vulnerability and importance of the system.
- Thorough testing before the any new software release is applied in a production environment.

#### 3.10.4 Authorization Controls

Authorization controls ensure all information and data entered or used in processing is authorized by management, and responsible representatives of events that actually occurred.



**Auditor's Role**

- Transactions in an application system are manually authorized, the controls that ensure that no unauthorized modifications take place after authorization and prior to establishing input controls? Determine if the proper level of management is authorizing the transaction activity.
- If transaction authorization is facilitated by logical access restrictions, select a sample of access rules applying to transaction input and update, and verify if the appropriate people have these capabilities.
- Identify any allowable overrides or bypasses of data validation and edit checks (authorization, monitoring, etc.) Determine who can do the overrides and verify that they are in a management position that should have this authority. Are all uses of the override features automatically logged so these actions can be subsequently analyzed for appropriateness?
- Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
- Review by IT management to monitor, and approve all changes to hardware, software, and personnel responsibilities.
- Assigned and authorized responsibilities to those involved in the change and monitor their work with adequate segregation of duties.

**3.10.5 Document Controls**

The need for procedures for recording all requests for change (RFC), preferably on standard documents to gain assurance and continuous monitoring that the systems do what they are supposed to do and the controls continue to operate as intended. The requests for changes in both hardware and software resource of the system should be logged and given a unique chronological reference number. All RFCs should be allocated a priority rating to indicate the urgency with which the change should be considered and acted upon.

Documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. A user instruction manual document defines responsibilities and actions :

- Input controls that identify all data entering the processing cycle;
- Processing control information that includes edits, error handling, audit trails and master file changes;
- Output controls that define how to verify the correctness of the reports;
- Separation of duties between preparing the input and balancing the output

### 3.50 Information Systems Control and Audit

To provide the user with the tools to achieve their responsibilities, the user instruction manual should include:

- A narrative description of the system (IT and Manual)
- A detailed flowchart of all clerical processes.
- A detailed document flowchart.
- A copy of each input document, completed as an example, together with instructions for preparation.
- A list of approvals required on each input document.
- A copy of any batch control forms or other transmittal forms used together with instructions on their preparation and reconciliation to batch edits reports.
- A listing of computerized input and processing edits performed the error messages that result there from, and instructions for correcting, resubmitting and balancing the resubmitted items.
- A copy of each report produced by the system with a description of its purpose, the number of copies, distribution and instructions for balancing output to original input
- A list of retention periods for : input source documents, data file (tape or disk), output report.
- A system recovery section including user responsibilities for assisting in the restoration of the system.

#### **Auditor's Role**

Assessing documentation involves evaluating the change boards efforts to complete the following critical procedures :

- There is sufficient documentation that explains how software/hardware is to be used.
- There are documented formal security and operational procedures.

To understand document flow, certain background information must be obtained through discussions with corporate officials, from previous audits or evaluations, or from system documentation files. The auditor will need to obtain documents with the following details:

- Name (title) of the computer product
- Purpose of the product System name and identification number
- Date the system was implemented
- Type of computer used (manufacturer's model) and location
- Frequency of processing and type of processing (batch, online)
- Person(s) responsible for the computer application and database that generates the computer output.

- Point of origin for each source document
- Each operating unit or office through which data is processed
- Destination of each copy of the source document and the action applied to each copy (filed, audited, entered into a computer, etc.)
- Actions taken by each unit or office in which the data is processed (for e.g. recorded in books of account, unit prices or extensions added, control numbers recorded and checked, etc.)
- Controls over the transfer of source documents between units or offices to assure that no documents are lost, added, or changed (controls include record counts, control totals, arithmetic totals of important data, etc.)

### **3.10.6 Testing and Quality Controls**

Testing commences during the design phase, during which designs and specifications should be subject to quality reviews (non-computer testing), and continues during the system development and acceptance testing phases of the SDLC.

Computer systems are tested to prove that they perform to the satisfaction of the various interested parties. This includes the developers, operations staff, and the end-users (including the System Owner) It may also include system administrators, security personnel, and auditors. In practice testing can only give reasonable assurance that all is well and that a system behaves as intended and as predicted; but it cannot give positive proof that any module/program/system is free from error. This is due in part to the extremely high number of possible program paths, and in part to the practical impossibility of generating test data that will adequately test all paths with all combinations of data.

The overall objective of the testing process is therefore to ensure that the delivered system is of adequate quality. To meet this objective it will be necessary to confirm that the new system:-

- conforms with the organization's technical policies and standards;
- performs all the required functions;
- can be used by the staff for whom it is intended;
- meets its performance objectives;
- is reliable in operation.

The requirement to demonstrate that a system is reliable implies that it should be tested, not to demonstrate that it works, but to uncover as many defects as possible. Tests must therefore be designed that attempt to demonstrate that the system:

- does not do what it is supposed to do;
- does what it is not supposed to do;

### 3.52 Information Systems Control and Audit

- is not operable by the staff for whom it is intended.

During the testing phase, the system is tested to verify that it works as intended and meets design specifications. An overall testing strategy should be developed to define the individual test events, roles and responsibilities, test environment, problem reporting and tracking, and test deliverables. Although each project may define different test events, in general, test events include unit testing, integration testing, technical testing, functional testing, and acceptance testing. Other important principles that should govern testing - and indeed any quality control - activities are that there is :

- no testing without measurable objectives;
- no testing without recording;
- no recording without analysis;
- no analysis without action.

Defects uncovered during testing might be corrected if they are considered to be of sufficient importance to justify the cost and time involved in taking remedial action. But it may be preferable to live with a defect if it is trivial, or defer remedial action until a more convenient time, for example by including a fix in a later release of the software. If a defect is corrected, the system (or perhaps parts of it) will probably need to be re-tested to ensure that the change has not introduced other unforeseen problems. This process is known as “regression testing”.

### 3.11 QUALITY CONTROL

Quality control management is a process that impacts the effectiveness, efficiency, integrity, and availability of information systems and involves IT resources that include people, applications, technology, and facilities. It describes the controls over the IT process of managing quality that meets the business requirement. Quality controls encompass the following:

- Establishment of a quality culture
- Quality plans
- Quality assurance responsibilities
- Quality control practices
- System development life cycle methodology
- Program and system testing and documentation
- 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

This control requires regular reviews and audits of the software products and activities to verify that process and personal within the organization comply with the applicable procedures and standards. Standards and procedures need to be established for valid quality assurance measurement processes in a project and its processes. These processes must be documented and controlled.

### 3.11.2 Quality Standards

Quality management controls are implemented in-order to drive maturity into the organizational processes. The best practices that identify the quality and assurance are governed by two key standards:

(i) *Capability Maturity Model Integration (CMMI®)* : by Software Engineering Institute(SEI); is a framework for organizing and assessing the maturity level of IT processes for software development and maintenance of products and services. The software process maturity is the extent, to which a specific process is explicitly defined, managed, measured, and controlled, and is effective. A detail discussion on this standard is given in chapter 8.

(ii) *9000 Quality Management and Quality Assurance Standards (ISO)* : Defines quality control as the “operational techniques and activities that are used to fulfill requirements for quality”.

As quality control is concerned with the quality of individual products produced during the project - in other words confirming that they fit for their intended purpose - it follows that it is the responsibility of the Project Manager to ensure that effective quality control is carried out. Quality control mechanisms include both formal and informal reviews, walkthroughs, testing, and inspection.

Quality control costs both time and money, and Project Managers are often tempted to dispense with it, particularly when working to an unrealistic, imposed deadline or where slippage has occurred in the project time-table. Removing what appears to be a “non-productive” activity apparently brings the project back on schedule. **This is a false economy.** It stores up greater problems for both the later stages of the system and for the maintenance and operations activities following project delivery. And there is growing evidence that quality control and productivity gains, far from being mutually exclusive, are complementary.

### 3.11.3 Quality Reviews

Quality review covers various non-computer testing activities. For example, it determines whether a product is:

- complete and free from cosmetic and mechanical defects;
- is correct (e.g. a specification or plan), is sufficiently comprehensive and is targeted at the appropriate skill level for each category of user;
- Complies with relevant standards.

## **3.54 Information Systems Control and Audit**

### **3.11.4 Auditor's Role :**

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

- Does the system design follow a defined and acceptable standard?
- Are completed designs discussed and agreed with the users?
- Does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization's technical standards and policies, and the User Requirements Specification;
- Do quality reviews follow a defined and acceptable standard?
- Are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
- Are auditors/security staffs invited to comment on the internal control aspects of system designs and development specifications?
- Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
- Are defects uncovered during quality reviews always corrected?
- Are all system resources (hardware, software, documentation) that have passed quality review been placed under change control management and version control?
- Has a System Installation Plan been developed and quality reviewed?
- Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid "skills stagnation", the delivery of training will need to be carefully scheduled);

### **3.11.5 Copyright Violations**

Software programs can easily be copied or installed on multiple computers. It is necessary for organizations to specifically address software piracy in training, in policy and procedures, or in the application of general internal controls. Violation of copyright laws may lead to potential risk. The computing environment needs controlling to prevent software piracy and copyright violations.

The scope of a Copyright Act is:

- The illegal copy of computer programs except for backup or archival purposes.
- Any business or individual convicted of illegally copying software is liable for both compensatory and statutory damages for each illegal copy of software in the premises.

- The information from annoyed employees and consultants about organizations that use illegal software are documented.

The Copyright Notice:

Any information owned/created by the company and considered its intellectual property in a written, printed, or stored as data, must be labeled with a copyright notice in the following format : Copyright © 2003 [Company Name], Inc. All Rights Reserved.

### **3.11.6 Contract / Warranties**

On Acquisition of Software systems organizations enter into contracts for computer hardware, software, and services. The need for familiarity and informed decision with the products and contract terms is mandatory. The management is responsible for thorough review as today's information systems support strategic and day-to-day operations.

IT contracts are to address these issues:

- Meet IT users expectations and the systems need to perform as intended;
- Able to file litigation in response to dissatisfaction with products or services on the failure of the selection or acquisition process.

IT auditors can help companies avoid contract failures, especially those lacking in-house computer contracting expertise in areas as first-time purchases, contract services for computer maintenance, custom applications, and multiple supplier procurements. The evidence gathered by auditors can assist the organization in specifying both performance standards and remedies for nonperformance.

The review areas of IT-related contracts are:

- Review of supplier contract terms that limit supplier liability.
- Review of contract objectives and performance measurements to ensure objectives have been met.
- Review and inclusion in future contracts of contract clauses for protecting customer interests.
- In the development or review of any IT contract, the objectives of the contracting process are to focus on preparing or examining the acceptance criteria.
- The three key goals to achieve while contracting for computer goods and services are:
  - ◆ Preparation of explicit criteria that can be used for acceptance with respect to user requirements,
  - ◆ The process of negotiating the contract and the inclusion of clauses that assure supplier compliance, and
  - ◆ The process of monitoring contract compliance is the responsibility of the entire organization.

### 3.56 Information Systems Control and Audit

- To identify a major control weakness, problems and contract issues which require immediate management and organizational attention.
- Does the contract reflect the organization's requirements and have appropriate levels within the organization verified them?
- Have the requirements been translated into measurable acceptance criteria that can be monitored and verified?
- To ensure that the RFP contains the needs and requirements and how they are met.
- Was the legal counsel or contracting officer present at all meetings and documentation of proceedings recorded?
- What changes or agreements were reached in refining contract terms and were they verified with management?
- The contract has been executed and monitored to assure customer's rights.
- Acceptance tests are performed on all products or services provided and tests are documented and reviewed by management.
- Acceptance tests are documented, evaluated, and the results are reviewed and signed off by customers at affected levels including management.
- The organization exercises its right to accept or decline the contract, and documentation supports its decision.

#### 3.11.7 Service Level Agreements (SLA)

The SLA is a formal agreement between a customer requiring services and the organization that is responsible for providing those services. It is not a legal contract in itself, but an essential component of it. An SLA is to state the required performance of the system in terms of its availability to users, response times, and numbers of transactions processed and any other suitable criteria meaningful to the user. Performance indicators are to be agreed, and the delivered level of service is to be regularly monitored against that specified.

- Service : A set of deliverables that passes between a provider and a consumer.
- Level : The measurement of services agreed upon and delivered and the gap between the two.
- Agreement : Contract between two entities—the one providing the service and the recipient.

An SLA carried out by an organization could include the organization's IT Department, a facilities management contractor, an external bureau, a telecommunications supplier, or a hardware maintenance contractor. Users and providers are to formally agree the standards of service to be provided, and the levels of user demand to be satisfied, before the system is implemented.



An SLA should also define:

- The level of technical support to be provided to users.
- The procedures for proposing changes to the system.
- Standards of security provision and administration that includes system and data access controls and monitoring system and network use.
- Emergency requirements
- And a schedule of charges for the services to be provided.

The auditor is to ensure that the following form a part of the service level agreement:

- Service provider should comply with all legal requirements that are applicable to the outsourced activity.
- Should provide for a right to audit clause and requirement of control responsibilities.
- Responsibility of the service provider to establish performance monitoring procedures.
- Business continuity measures to be put in place to ensure continuity of service.
- Non disclosure requirements as regards information and processes of the audited organization handled and control stipulations in this regard.
- Insurance requirements.

### **3.12 CONTROLS OVER SYSTEM IMPLEMENTATION**

The final step to implementing the system includes conversion, documentation, training, and support. To ensure smooth implementation, it is important that users and technical support people receive adequate training. To facilitate this training, both system and user documentation need to define the functionality of the system. Activities during Implementation stage are discussed below.

#### **3.12.1 Procedures Development**

Covers who, what, when, where, and how of the implementation process. Installation of new hardware / software of the new system interfaces with the other systems or is distributed across multiple software platforms, some final commissioning tests of the production environment are carried out to prove end to end connectivity. The design of procedures must match the job/task responsibility of a user within the organizational functional framework. It should lay down the activities with respect to a task stating the input, process and output generated thereof.

The auditor is to assess the following in the procedure document design phase:

- The quality of the procedures design must meet the minimum user requirements and the SRS specifications of the system.
- Change management principles implemented and followed within the organization.

### 3.58 Information Systems Control and Audit

- The approach followed in testing and implementation of changes into the behavior and processes of the system.
- Quality of the procedures documentation, system manuals etc, in a consistent and formal style.

#### 3.12.2 Conversion

It involved the following activities :

- Defines the procedures for correcting and converting data into the new application, determining what data can be converted through software and what data manually.
- Performing data cleansing before data conversion,
- Identifying the methods to access the accuracy of conversion like record counts and control totals,
- Designing exception reports showing the data which could not be converted through software, and
- Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

The conversion strategies are :

- Direct implementation / Abrupt change-over : The old system is suspended on a specific day and the new system is implemented. It reduces cost of redundant processing but in case of a failure due to say a system crashes, the old system is also not available for recovery. In case of small applications, or when migrating from a manual to computer system, this may be used.
- Parallel implementation : Both the old and new systems are run in parallel to verify if their output is the same. Then the old system is suspended. Here redundant processing is costly but reduces risks associated with conversion. But users will face problems in working with both systems.
- Phased implementation : This strategy consists of implementing the new system in parts. This makes implementation more manageable. This is also called the phase-in conversion and provides a steady transition.
- Pilot implementation : The new systems is first implemented in modules of non-critical units and then moved to larger unit.

Except direct implementation, others strategies are not mutually exclusive. A cautious combination of the strategies can be adopted, depending on the type of application/system.

#### 3.12.3 Auditor's Role

- Has a Data Conversion Plan been drawn up?

- Does the Data Conversion Plan :
  - ◆ Describe the data conversion strategy to be followed (e.g. the procedures for reconciling differing charts of accounts; the sequence of files to be converted; the conversion timetable; keeping converted data up-to-date)?
  - ◆ Allocate staff to each task (the users should be fully involved) and define specific roles and responsibilities, including that of signing off successful completion of each task?
  - ◆ Set out the criteria for identifying and resolving problems on the quality of the existing data (e.g. undertake file interrogation to identify missing or incompatible data items in the existing system; define procedures to deal with the correction of data rejected by the new system)?
  - ◆ Acceptance tests any custom-built software that has been developed to support the data conversion task?
  - ◆ Define the controls that are to give assurance that data has been transferred completely and accurately, and correctly posted (e.g. hash and control totals, and record counts; checking a sample of detailed records back to the old system; reconciling balances between the two systems)?
  - ◆ Implement an effective separation of roles between those involved in transferring data and those involved in verifying that it has been correctly transferred (information security should not be neglected, particularly where financial data is involved)?
  - ◆ Define procedures to ensure that converted data is kept up-to-date following its transfer to the new system?
  - ◆ Define backup and recovery procedures for the converted data on the new system (these procedures will not relate to any processing cycle so they may differ from the eventual operational procedures)?
  - ◆ Define how the audit trail is to be preserved after cut over; also, how archived data from the old system will be processed after de-commissioning?

#### 3.12.4 User Final Acceptance testing

The user acceptance test is performed in a secured testing environment where both source and executable codes are protected. This helps to ensure that unauthorized or last minute change to the system does not take place without going through the standard system maintenance process. Here testing is a complete end-to-end test of the operational system including all manual procedures. It aims to provide the system users with confirmation that:

- the User Requirement Specification (including system performance criteria) has been met;
- end user and operational documentation is accurate, comprehensive, and usable;

### 3.60 Information Systems Control and Audit

- supporting clerical procedures work effectively;
- a production-line support functions operate correctly in-line with user expectations;
- Back-up and recovery procedures work effectively.

The acceptance testing is to be undertaken by the end users supported by IT staff and expert consultants as necessary, and should continue until no errors or shortcomings remain. In addition to testing system functions, acceptance testing must also test responsiveness with respect to the performance criteria defined during the Specification Stage. The acceptance test plan involves :

- Performance testing should address:
  - ◆ average response time : usually defined as the time between the user depressing the transmit key, and the first character of the reply appearing on the screen, with a further maximum time specified for the screen to be completed;
  - ◆ maximum response time : the response time that must not be exceeded;
  - ◆ other response times : for example the time to : load an application, accept or move between fields on the screen, perform a single or multiple update or to run a complex enquiry
- Volume testing : subjects the system to heavy volumes of data to test whether it can handle the volume of data specified in a acceptable time-frame;
- Stress testing : subjects the system to heavy loads or stresses (a heavy stress is a peak volume of data encountered over a short period)
- Security testing : attempts to subvert the system's security and internal control checks;
- Clerical procedures checking : aims to confirm that all supporting clerical procedures have been documented and work effectively;
- Back-up and recovery : aims to confirm that software, configuration files, data and transaction logs can be backed up, either completely or selectively; and also restored from backup;

On satisfactory completion of user acceptance testing, the Project Board should sign off a System Acceptance Document to signify that the development process has been completed, and hand over all the items that will comprise the operational system to the System Owner (in practice the bulk of it will pass to the computer operations and software maintenance teams)

#### 3.12.5 Auditor's Role

The auditor is to assure management that both developers and users have thoroughly tested the system to ensure that it:

- possesses the built-in controls necessary to provide reasonable assurance of proper operation;

- provides the capability to track events through the systems and thus supports audit review of the system in operation;
- meets the needs of the user and management;
- If the level of testing does not meet standards, the auditor must notify the development team or management who will then take corrective action;
- What arrangements have been made to ensure that the system has been correctly built (installed, configured, loaded, etc) before user acceptance testing commences?
- Has an Acceptance Test Plan been drawn up to cover all aspects of testing?
- allocate adequate resources in terms of manpower, time and equipment to acceptance testing? (A common problem in IT projects is to reduce the time available for acceptance testing in order to recover from slippage in the overall project timetable. This can easily result in the implementation of an inadequately tested system and defective system);
- allocate individual roles and responsibilities for :
  - ◆ managing the test environment? (i.e. environment design; configuration management; operation and maintenance)
  - ◆ undertaking individual tests and test cycles?
  - ◆ recording test result?
  - ◆ analysing test results and prioritising errors?
- fully involve the end-users in the design and execution of the acceptance testing programme?
- include ancillary procedures? (e.g. clerical control checks, the Help Desk, Network Support, System Administration);
- require the manager in charge to sign off individual tests and test cycles on successful completion?
- Is there an adequate separation of roles to help guard against unauthorized changes taking place during testing and error correction? (e.g. between individuals involved in building and modifying items; those involved in testing them; and those involved in releasing them into live use);
- Have test data been prepared for each test? Have the anticipated results for each test been fully defined?
- Do tests cover events that ought not to happen, as well as those that should? (e.g. do they include out of range tests; tests on processing acceptable items occurring in unacceptable combinations; duplicate transaction processing; incomplete master and standing data files);

## 3.62 Information Systems Control and Audit

- Does user the Acceptance Testing Plan cover all aspects of the User Requirements Specification?
- Is an adequate audit trail of changes maintained? (is it possible to back-track on a change to see how it occurred and whether it was correctly authorized?)
- Are regression tests carried out to ensure that previously accepted areas of the new system continue to work after significant changes have been implemented?
- Has the acceptance-testing programme been signed off by the Project Board on successful completion? If not, is appropriate remedial action being taken?

### 3.12.6 User training

Training both the end-users and the IS operations personnel is critical for the efficient and effective implementation of a system being seamless integrated within the organization business process. Training would involve manager's training on overview and application systems, operational user training on how to use the software, enter the data, and generate the output and systems training on the technical aspects. Support along with training, ongoing user support with trained personnel for problem tracking is another important component needed to ensure a successful implementation.

## 3.13 SYSTEM MAINTENANCE

System maintenance is an important phase during the implementation of system; day-to-day operations bring out the strength and weaknesses which may need periodic modification to meet its objective. Maintenance can be undertaken under the following three categories:

*Corrective maintenance* : Emergency program fixes and routine debugging-logical errors.

*Adaptive maintenance* : Accommodations of change-in the user environment.

*Perfective maintenance* : User enhancements, improved documentation, and recoding for improving processing efficiency.

The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness. It includes making changes to improve a system's performance, correct problems, enhance security, or address user requirements. To ensure modifications do not disrupt operations or degrade a system's performance or security, organizations should establish appropriate change management standards and procedures. Maintaining accurate, up-to-date hardware and software inventories is a critical part of all change management processes. Management should carefully document all modifications to ensure accurate system inventories. (If material software patches are identified but not implemented, management should document the reason why the patch was not installed.)

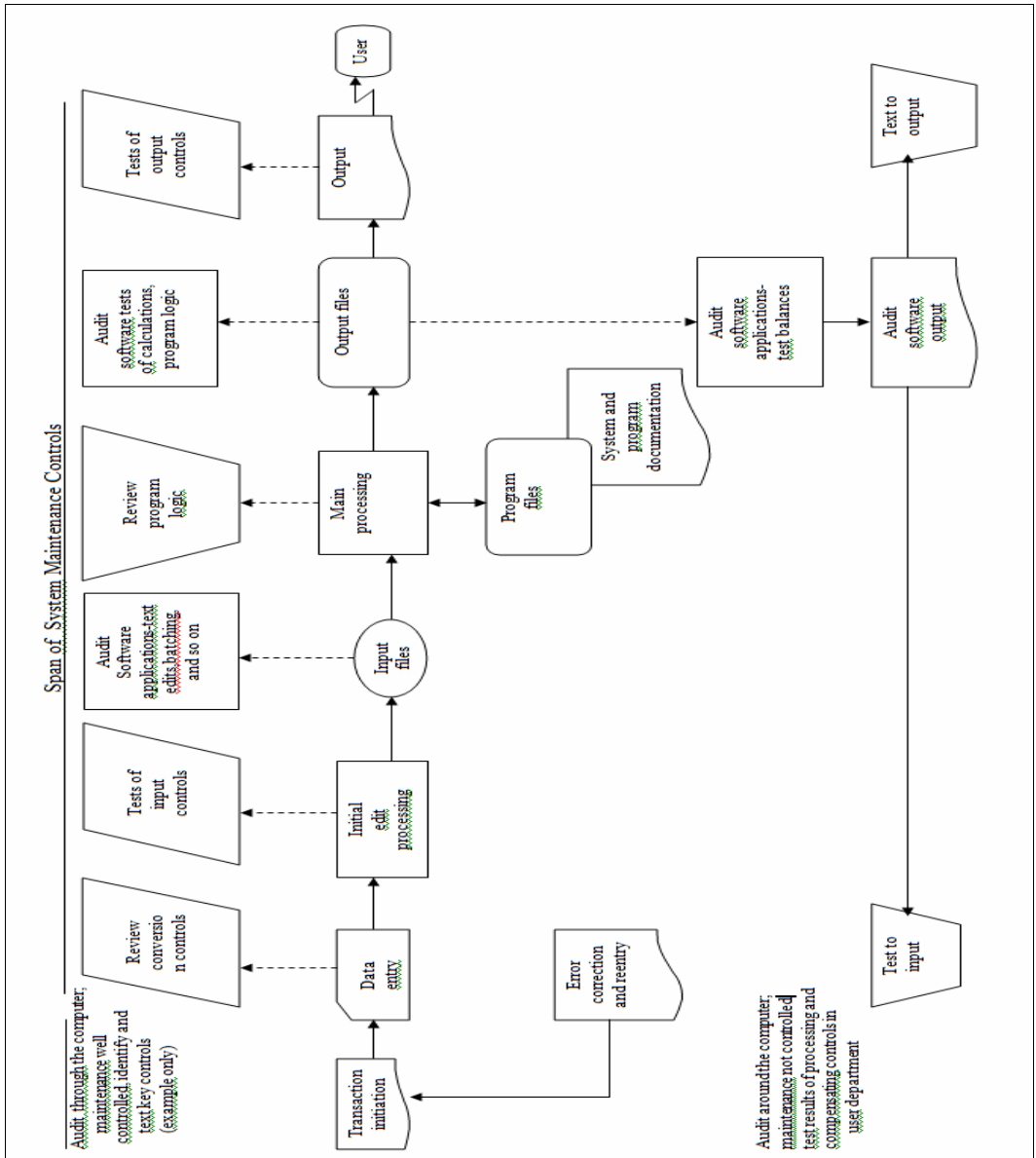
### 3.13.1 Auditor's Role

The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:

- The ratio of actual maintenance cost per application/operation versus the average of all applications/process.
- Average time to deliver change requests.
- The number of change requests for the system application that were related to bugs, critical errors, and new functional specifications.
- The number of production problems per application and per respective maintenance changes
- The instances of divergence from standard procedures such as undocumented applications, unapproved design, and testing reductions.
- The quantity of modules returned to development due to errors discovered in acceptance testing.
- Time elapsed to analyze and fix problems.

The span of maintenance of the information systems is to ensure effective and timely reporting of the maintenance needs and being carried out in a controlled manner. The Fig. 3.16 highlights the maintenance control activities widely dispersed throughout the organization when the system involves end-user participation in the use of the information system. An auditor needs to satisfy the implementation of maintenance activities and substantial resource consumption.

### 3.64 Information Systems Control and Audit



**Fig. 3.16 : Maintenance Controls**

#### 3.13.2 Performance Measurement

Performance measurement is dependent on the business strategy and objectives of the organization. The factors for measurement metric would involve:

- the value delivered by the IT system;
- the ratio to the cost of IT to the per unit business function;
- the responsive time of the system for a new or change in operations; and



- the ongoing costs of the system to maintain its effectiveness.

For a system to be evaluated properly, it must be assessed using system performance measurements. Common measurements include throughput (Output per unit of time), Utilization (Percentage of time the system is being productively used, and response time (how long it takes the system to respond)

### 3.14 POST IMPLEMENTATION REVIEW

After a development project is completed a post implementation review should be performed to determine if the anticipated benefits were achieved. Reviews help to control project development activities and to encourage accurate and objective initial cost and benefit estimates. The full scope of a post implementation review ("PIR") will depend largely on the scale and complexity of the project. The post implementation review should be performed jointly by the project development team and the appropriate end users or alternatively, an independent group not associated with the development process, either internal or external, should carry out the audit, to meet the following objectives:

- Business objectives : delivered within budget and deadline; is producing predicted savings and benefits, etc.;
- User expectations : user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.;
- Technical requirements : capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.

The PIR is undertaken after any changes and tuning that are necessary to achieve a stable system have been completed, and any significant problems have had a chance to surface. Sufficient time should also be allowed for the system's users to become familiar with it. These criteria should be met between six and twelve months after implementation. If the PIR is delayed beyond twelve months there will be an increasing risk that changing requirements - leading to further releases of the system - will obscure the outcome from the original development; also, that the need for a PIR will be overtaken by other priorities.

If there are obvious and significant problems with a new system a PIR may need to be undertaken sooner than would otherwise have been the case in order to identify the nature of the problem(s), their case(s), and to recommend a suitable course of action.

#### 3.14.1 The PIR team

In order to achieve an impartial outcome, the team should be substantially independent of the original system development team. It may therefore be advisable to employ an external IS consultant to manage the review. It may also be necessary to employ other external support to assist in evaluating the delivery of technical (e.g. project management, system design) and specialized functions (e.g. in financial and management accountancy), and to make appropriate recommendations where necessary. Internal Audit might help assess the effectiveness of internal controls.

### **3.66 Information Systems Control and Audit**

In order to facilitate control, the PIR should have terms of reference, authorized by the approving authority, defining the:-

- scope and objectives of the review;
- criteria to be employed in measuring the achievement of objectives;
- management and organisation of the review team;
- Review budget and reporting deadline.

#### **3.14.2 Activities to be undertaken**

During a PIR, the team should, according to their terms of reference, review:-

- the main functionality of the operational system against the User Requirements Specification;
- system performance and operation;
- the development techniques and methodologies employed;
- estimated time-scales and budgets, and identify reasons for variations;
- changes to requirements, and confirm that they were considered, authorised and implemented in accordance with change and configuration management standards;
- set out findings, conclusions and recommendations in a report for the authorising authority to consider.
- In addition to reviewing the functionality delivered by the new system, the review team will also need to look back to the Business Case on which the system was originally based to confirm that all the anticipated benefits, both tangible and intangible, have been delivered. This will involve investigating the reasons behind benefits that were not achieved, perhaps involving recommendations for remedial action, and using survey techniques to establish the extent to which intangible benefits (such as improved staff morale) have been realised.

It is also possible that the PIR will identify benefits that were not anticipated in the Business Case. These should be included in the PIR Report as additional justification for the investment, and to identify benefits that might be realized in other IS development projects.

Following their deliberations on the PIR Report, the authorizing authority may either:

- endorse continuation of the system;
- approve plans to modify the system;
- terminate the system and made arrangements for a new course of action.

#### **3.14.3 Auditor's Role**

The following issues should be considered when judging the effectiveness either of a PIR, or to form the basis for the auditor to undertake one.

- Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.

- Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.
- Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reason(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
- Confirm that the previous system has been de-commissioned or establish the reason(s) why it remains in use.
- Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.
- Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
- Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.
- Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.
- Review the Business Case and determine whether:-
  - anticipate benefits have/are been achieved;
  - any unplanned benefits have been identified;
  - costs are in line with those estimated;
  - benefits and costs are falling with the anticipated time-frame.
- Review trends in transaction throughput and growth in storage use to identify the anticipated growth of the system is in line with that forecast.

<b>Control Category</b>	<b>Threats/Risks</b>	<b>Controls</b>
System development and acquisition controls	System development projects consume excessive resources.	Long-range strategic master plan, data processing schedules, assignment of each project to a manager and team, project development plan, project milestones, performance evaluations, system performance measurements (throughput, utilization, response time), and post-implementation reviews.

### 3.68 Information Systems Control and Audit

Change management controls	Systems development projects consume excessive resources, unauthorized systems changes.	Change management control policies and procedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability, categories and rank all changes, procedures to handle urgent matters, communicate changes to management and users, management approval of changes, assign specific responsibilities while maintaining adequate segregation of duties, control go through all appropriate steps, these all changes, develop plan for backing out of mission-critical system changes, implement a quality assurance functions and update documentation and procedures.
----------------------------	---	---

**Table 3.5 : Summary of Key Maintainability Controls**

### 3.15 CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY

#### 3.15.1 Information Classification

Information classification is the conscious decision to assign a level of sensitivity to information as it is being created, amended, enhanced, stored, or transmitted. The classification of the information should then determine the extent to which it needs to be controlled / secured and is also indicative of its value in terms of Business Assets.

The classification of information and documents is essential if one has to differentiate between that which is of little (if any) value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. For many organizations, a simple 5 scale grade will suffice as follows:

Information Classification	Description
<b>Top Secret</b>	Highly sensitive internal information relating to e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level is the highest possible.

<b>Highly Confidential</b>	Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.
<b>Proprietary</b>	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level is high.
<b>Internal only Use</b>	Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.
<b>Public Documents</b>	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

**Table 3.6 : Classification of Information**

### 3.15.2 Data Integrity

Once the information is classified, the organization has to decide about various data integrity controls to be implemented. The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through the various stages of a specific data processing program. In other words, they ensure the integrity of a specific application's inputs, stored data, programs, data transmissions, and outputs. Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that the information meets expectations about its quality and integrity. Assessing data integrity involves evaluating the following critical procedures :

- Virus detection and elimination software is installed and activated.
- Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended

Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data. A primary objective in ensuring integrity is to protect the data against erroneous input from authorized users. An auditor should be concerned with the testing of user-developed systems; changes or the release of data, unknown to the user, could occur because of flawed design. A user may assume that the visible output is the only system activity. The possibility that erroneous data could infest the system is strong. A person other than the designer or user should test any application that has access to the organization's data in more than a read-only

### 3.70 Information Systems Control and Audit

format. Again, this is a critical area if the service desk is outsourcing to an application service provider. Release of customer information to such an entity must be controlled through contractual requirements with stiff remedies or penalties if data is compromised.

There are six categories of integrity controls summarized in Table 7.

<b>Control Category</b>	<b>Threats/Risks</b>	<b>Controls</b>
<b>Source data control</b>	Invalid, incomplete, or inaccurate source data input	Forms design; sequentially prenumbered forms, turnaround documents; cancellation and storage of documents, review for appropriate authorization; segregation of duties, visual scanning; check-digit verification; and key verification.
<b>Input validation routines</b>	Invalid or inaccurate data in computer-processed transaction files	As transaction files are processed, edit programs check key data fields using these edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks. Enter exceptions in an error log; investigate, correct, and resubmit them. On a timely basis; re-edit them, and prepare a summary error report.
<b>On-line data entry controls</b>	Invalid or inaccurate transaction input entered through on-line terminals	Field, limit, range, reasonableness, sign, validity, and redundant data checks; user IDs and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, pre-formatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error messages, and data retention sufficient to satisfy legal requirements.
<b>Data processing and storage controls</b>	Inaccurate or incomplete data in computer-processed master files	Policies and procedures (governing the activities of data processing and storage personnel; data security and

		<p>confidentiality, audit trails, and confidentiality agreements); monitoring and expediting data entry by data control personnel; reconciliation of system updates with control accounts or reports; reconciliation of database totals with externally maintained totals; exception reporting, data currency checks, default values, data marching; data security (data library and librarian, backup copies of data files stored at a secure off-site location, protection against conditions that could harm stored data); use of file labels and write protection mechanisms, database protection mechanisms (date wise administrators, date dictionaries, and concurrent update controls); and data conversion controls.</p>
<p><b>Output controls</b></p>	<p>Inaccurate or incomplete computer output</p>	<p>Procedures to ensure that system outputs conform to the organization's integrity objectives, policies, and standards, visual review of computer output, reconciliation of batch totals; proper distribution of output; confidential outputs being delivered are protected from unauthorized access, modification, and misrouting; sensitive or confidential out-put stored in a secure area; users review computer output for completeness and accuracy, shred confidential output no longer needed; error and exception reports.</p>

### 3.72 Information Systems Control and Audit

<b>Data transmission controls</b>	Unauthorized access to data being transmitted or to the system itself; system failures; errors in data transmission	Monitor network to detect weak points, backup components, design network to handle peak processing, multiple communication paths between network components, preventive maintenance, data encryption, routing verification (header labels, mutual authentication schemes, callback systems), party checking; and message acknowledgement procedures (echo checks, trailer labels, numbered batches)
-----------------------------------	---	---

**Table 3.7 : Summary of data Integrity Controls**

#### 3.15.3 Data Integrity Policies

- Virus-Signature Updating : Virus signatures must be updated immediately when they are made available from the vendor.
- Software Testing : All software must be tested in a suitable test environment before installation on production systems.
- Division of Environments : The division of environments into Development, Test, and Production is required for critical systems.
- Version Zero Software : Version zero software (1.0,2.0, and so on) must be avoided whenever possible to avoid undiscovered bugs.
- Offsite Backup Storage : Backups older than one month must be sent offsite for permanent storage.
- Quarter-End and Year-End Backups : Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
- Disaster Recovery : A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

#### 3.15.4 Data Security

Data security encompasses the protection of data against accidental or intentional disclosure to unauthorized persons as well as the prevention of unauthorized modification and deletion of the data. Many levels of data security are necessary in an information systems environment; they include database protection, data integrity, and security of the hardware and software controls, physical security over the user, and organizational policies. An IS auditor is responsible to evaluate the following when reviewing the adequacy of data security controls:



- Who is responsible for the accuracy of the data?
- Who is permitted to update data?
- Who is permitted to read and use the data?
- Who is responsible for determining who can read and update the data?
- Who controls the security of the data?
- If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
- Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
- The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

### 3.16 SECURITY CONCEPTS AND TECHNIQUES

#### 3.16.1 Cryptosystems

A **cryptosystem** refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms : one for key generation, one for encryption, and one for decryption. The term *cipher* (sometimes *cypher*) is often used to refer to a pair of algorithms, one for encryption and one for decryption. Therefore, the term "cryptosystem" is most often used when the key generation algorithm is important. For this reason, the term "cryptosystem" is commonly used to refer to public key techniques; however both "cipher" and "cryptosystem" are used for symmetric key techniques.

#### 3.16.2 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. A key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte.

Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithm specified in this standard is commonly known among those using the standard. The unique key chosen for use in a particular application makes the results of encrypting data using the algorithm unique. Selection of a

### 3.74 Information Systems Control and Audit

different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data. Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES) In some documentation, a distinction is made between DES as a standard, and the algorithm, which is referred to as the **DEA** (the **Data Encryption Algorithm**)

#### 3.16.3 Public Key Infrastructure (PKI)

Public key infrastructure, if properly implemented and maintained, can provide a strong means of authentication. By combining a variety of hardware components, system software, policies, practices, and standards, PKI can provide for authentication, data integrity, defenses against customer repudiation, and confidentiality. The system is based on public key cryptography in which each user has a key pair—a unique electronic value called a **public key** and a mathematically related **private key**. The **public key** is made available to those who need to verify the user's identity.

The **private key** is stored on the user's computer or a separate device such as a smart card. When the key pair is created with strong encryption algorithms and input variables, the probability of deriving the private key from the public key is extremely remote. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclosure. The private key is used to create an electronic identifier called a **digital signature** that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.

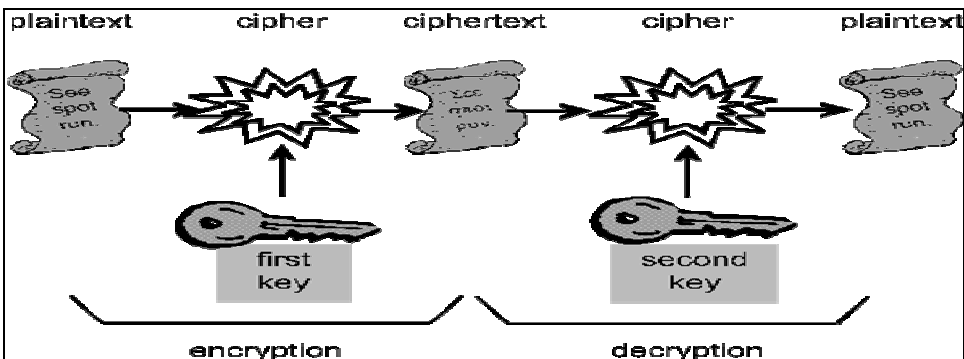


Fig. 3.17 : Public key Infrastructure

The *certificate authority* (CA), which may be the financial institution or its service provider, plays a key role by attesting with a *digital certificate* that a particular public key and the corresponding private key belongs to a specific user or system. It is important when issuing a digital certificate that the registration process for initially verifying the identity of users is adequately controlled. The CA attests to the individual user's identity by signing the digital certificate with its own private key, known as the *root key*. Each time the user establishes a communication link with the financial institution's systems, a digital signature is transmitted with a digital certificate. These electronic credentials enable the institution to determine that the digital certificate is valid, identify the individual as a user, and confirm that transactions entered into the institution's computer system were performed by that user.

The user's private key exists electronically and is susceptible to being copied over a network as easily as any other electronic file. If it is lost or compromised, the user can no longer be assured that messages will remain private or that fraudulent or erroneous transactions would not be performed. User AUPs and training should emphasize the importance of safeguarding a private key and promptly reporting its compromise.

PKI minimizes many of the vulnerabilities associated with passwords because it does not rely on shared secrets to authenticate customers, its electronic credentials are difficult to compromise, and user credentials cannot be stolen from a central server. The primary drawback of a PKI authentication system is that it is more complicated and costly to implement than user names and passwords. Whether the financial institution acts as its own CA or relies on a third party, the institution should ensure its certificate issuance and revocation policies and other controls discussed below are followed.

When utilizing PKI policies and controls, financial institutions need to consider the following:

- Defining within the certificate issuance policy the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure—expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;
- Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user accounts;
- Updating the database of revoked certificates frequently, ideally in real-time mode;
- Employing stringent measures to protect the root key including limited physical access to CA facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and back-up keys on computers that do not connect with outside networks;

### **3.76 Information Systems Control and Audit**

- Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

### **3.17 DATA SECURITY AND PUBLIC NETWORKS**

Historically, only large companies could afford secure networks, which they created from expensive leased lines. Everyone else had to make do with the relatively unsecure Internet. Nowadays, even huge corporations have to go outside their private nets, because so many people telecommute or log in while they're on the road. Network administrators as well as managers must balance security concerns with employees' demand for easy accessibility to data-grappling with the question : "how do you provide a low-cost, secure electronic network for your organization?"

One solution is a virtual private network (VPN) : a collection of technologies that creates secure connections or "tunnels" over regular Internet lines-connections that can be easily used by anybody logging in from anywhere. Key advantages offered by a VPN include universal connectivity, security, and low cost.

#### **3.17.1 Firewalls**

A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs)

They are four primary firewall types from which to choose : packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic

rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring the IP is not on a “white list”, creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

**(i) Packet Filter Firewalls :** Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet-filtering capabilities.

Dynamic packet filtering incorporates stateful inspection primarily for performance benefits. Before re-examining every packet, the firewall checks each packet as it arrives to determine whether it is part of an existing connection. If it verifies that the packet belongs to an established connection, then it forwards the packet without subjecting it to the firewall rule set.

Weaknesses associated with packet filtering firewalls include the following:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
- Logging functionality is limited to the same information used to make access control decisions.
- Most do not support advanced user authentication schemes.
- Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

Packet filtering offers less security, but faster performance than application-level firewalls. The former are appropriate in high-speed environments where logging and user authentication with network resources are not as important. They also are useful in enforcing security zones at the network level. Packet filter firewalls are also commonly used in small office/home office (SOHO) systems and default operating system firewalls.

Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening.

**(ii) Stateful Inspection Firewalls :** Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial “handshake” communicated through TCP flags in the header information. When a connection is

### 3.78 Information Systems Control and Audit

established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

**(iii) Proxy Server Firewalls** : Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits.

Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and e-mail proxy servers, for example, are capable of filtering for potential malicious code and application-specific commands (see “Malicious Code”) They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution’s security policy.

Proxy servers are increasing in importance as protocols are tunneled through other protocols. For example, a protocol-aware proxy may be designed to allow Web server requests to port 80 of an external Web server, but disallow other protocols encapsulated in the port 80 requests.

**(iv) Application-Level Firewalls** : Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

The primary disadvantages of application-level firewalls are as follows:

- The time required to read and interpret each packet slows network traffic. Traffic of certain types may have to be split off before the application-level firewall and passed through different access controls.
- Any particular firewall may provide only limited support for new network applications and protocols. They also simply may allow traffic from those applications and protocols to go through the firewall.

### 3.17.2 Firewall Services and Configuration

Firewalls may provide some additional services:

- Network address translation (NAT) : NAT readdresses outbound packets to mask the internal IP addresses of the network. Untrusted networks see a different host IP address from the actual internal address. NAT allows an institution to hide the topology and address schemes of its trusted network from untrusted networks.
- Dynamic host configuration protocol (DHCP) : DHCP assigns IP addresses to machines that will be subject to the security controls of the firewall.
- Virtual Private Network (VPN) gateways : A VPN gateway provides an encrypted tunnel between a remote external gateway and the internal network. Placing VPN capability on the firewall and the remote gateway protects information from disclosure between the gateways but not from the gateway to the terminating machines. Placement on the firewall, however, allows the firewall to inspect the traffic and perform access control, logging, and malicious code scanning.

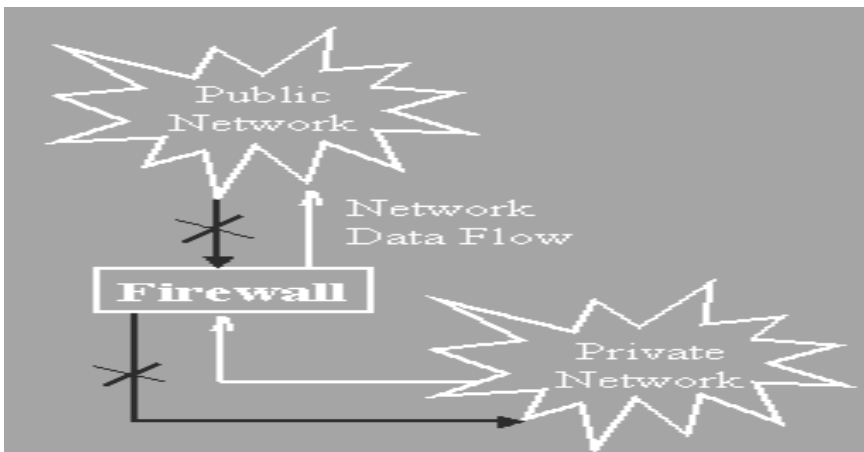


Fig. 3.18 : Firewall

Characteristics	Packet Filter Firewalls	Stateful Inspection Firewalls	Proxy Server Firewalls	Application-Level Firewalls
Inspection	Evaluate packet headers only	Monitors the State of TCP connection	Intermediary between internal and external networks	Like packet filters and validate packet content based on the application
Information Updating	Router Access Control Lists(ACL)	TCP connection state table	rewrite packet headers	Compare packets based on connection tables

### 3.80 Information Systems Control and Audit

Usage	Small office/Home Office (SOHO), Operating systems.	Network Inbound traffic	Domain Name Servers, Web server and Mail Servers	Telnet, FTP, HTTP and SMTP
Scope	Enforce security zones	Based on requests from the firewall	A layer of access control( content filtering)	Additional screening of packet payload- commands, protocols, packet length, authorization and content.
Advantages	Faster performance than application-level firewall	Like packet filters	Cache requests and responses to provide performance benefits	Strong level of security, complete packet interpretation.
Weakness	Unable to prevent application –specific vulnerabilities, easy to misconfigure, does not support advanced user authentication, basic security	Stateful filtering- predefined rules	Employed behind other firewall devices	Time to interpret the packet contents, limited support for new network applications and protocols.

**Table 3.8 : Comparative Analysis between types of firewalls.**

### 3.18 UNAUTHORISED INTRUSION

Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise the system and network resources of an organization. Simply put, it works like this : The computer systems on an organization are attached to a network, and perhaps even to the internet. The organization would allow access to that computer system from the network, by authorized people, for acceptable reasons. For example, if there is a web server, attached to the internet, only clients, staff, and potential clients, are allowed to access the web pages stored on that web server. It does not allow unauthorized access to that system by anyone, be that staff, customers, or unknown third parties. For example, it does not want people (other than the web designers that the company has employed) to be able to change the web pages on that computer. Typically, a firewall or authentication system of some kind will be employed to prevent unauthorized access.

Sometimes, however, simple firewall or authentication systems can be broken. Intrusion detection is the set of mechanisms that should be put in place to warn of attempted



unauthorized access to the computer. Intrusion detection systems can also take some steps to deny access to would-be intruders.

### 3.18.1 Why use Intrusion Detection?

The underlying reasons why one might use intrusion detection systems are relatively straight forward : One wants to protect the data and systems integrity. The fact that one cannot always protect that data integrity from outside intruders in today's Internet environment using mechanisms such as ordinary password and file security, leads to a range of issues. Adequate system security is of course the first step in ensuring data protection. For example, it is pointless to attach a system directly to the Internet and hope that nobody will break into it, if it has no administrator password! Similarly, it is important that the system prevents access to critical files or authentication databases (such as the NT SAM or the Unix /etc/password or /etc/shadow files) except by authorized systems administrators.

Further measures beyond those normally expected of an intranet system should always be made on any system connected to the internet. Firewalls and other access prevention mechanisms should always be put in place. While it may be acceptable to allow NT logon, file sharing, or telnet access to a system that is entirely internal, an Internet server should always use more secure mechanisms

Intrusion detection takes that one step further. Placed between the firewall and the system being secured, a network based intrusion detection system can provide an extra layer of protection to that system. For example, monitoring access from the internet to the sensitive data ports of the secured system can determine whether the firewall has perhaps been compromised, or whether an unknown mechanism has been used to bypass the security mechanisms of the firewall to access the network being protected.

### 3.18.2 What types of Intrusion Detection systems are there?

Intrusion Detection systems fall into two broad categories. These are:

- *Network based systems.* These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.
- *Host based systems.* These types of systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

A more recent type of intrusion detection system are those that reside in the operating system kernel and monitor activity at the lowest level of the system. These systems have recently started becoming available for a few platforms, and are relatively platform specific.

## 3.19 HACKING?

Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works.

## 3.82 Information Systems Control and Audit

### 3.19.1 What are Hackers?

Technically, a hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer. However, most people understand a hacker to be what is more accurately known as a 'cracker'.

### 3.19.2 What are Crackers?

Crackers are people who try to gain unauthorized access to computers. This is normally done through the use of a 'backdoor' program installed on the machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer.

### 3.19.3 What damage can a Hacker do?

This depends upon what backdoor program(s) are hiding on the PC. Different programs can do different amounts of damage. However, most allow a hacker to smuggle another program onto your PC. This means that if a hacker can't do something using the backdoor program, he can easily put something else onto your computer. Hackers can see everything you are doing, and can access any file on your disk. Hackers can write new files, delete files, edit files, and do practically anything to a file that could be done to a file. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information.

### 3.19.4 How do Hackers hack?

There are many ways in which a hacker can hack. Some are as follows –

- NetBIOS
- ICMP Ping
- FTP
- rpc.statd
- HTTP

(i) **NetBIOS** : NetBIOS hackers are the worst kind, since they don't require you to have any hidden backdoor program running on your computer. This kind of hack exploits a bug in Windows 9x. NetBIOS is meant to be used on local area networks, so machines on that network can share information. Unfortunately, the bug is that NetBIOS can also be used across the Internet - so a hacker can access your machine remotely.

(ii) **ICMP 'Ping' (Internet Control Message Protocol)** : ICMP is one of the main protocols that make the Internet work. It stands for Internet Control Message Protocol. 'Ping' is one of the commands that can be sent to a computer using ICMP. Ordinarily, a computer would respond to this ping, telling the sender that the computer does exist. This is all pings are meant to do. Pings may seem harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer. Also, hackers can use pings to see if a computer exists and does not have a firewall (firewalls can block pings) If a computer

responds to a ping, then the hacker could launch a more serious form of attack against a computer.

(iii) **FTP (File Transfer Protocol)** :FTP is a standard Internet protocol, standing for File Transfer Protocol. It can be used for file downloads from some websites. If you have a web page of your own, you may use FTP to upload it from your home computer to the web server. However, FTP can also be used by some hackers. FTP normally requires some form of authentication for access to private files, or for writing to files. FTP backdoor programs, such as-

- Doly Trojan
- Fore
- Blade Runner

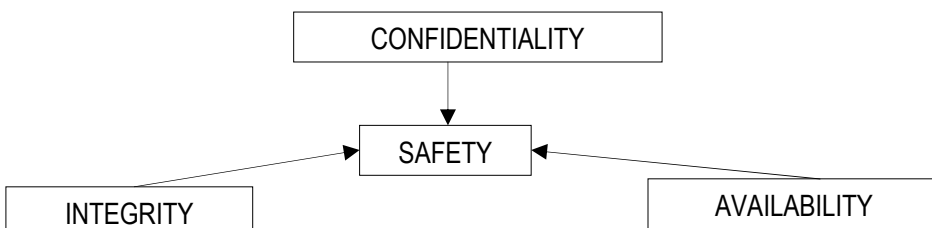
simply turn your computer into an FTP server, without any authentication.

(iv) **RPC statd** : This is a problem specific to Linux and Unix. The problem is the infamous unchecked buffer overflow problem. This is where a fixed amount of memory is set aside for storage of data. If data is received that is larger than this buffer, the program should truncate the data or send back an error, or at least do something other than ignore the problem. Unfortunately, the data overflows the memory that has been allocated to it, and the data is written into parts of memory it shouldn't be in. This can cause crashes of various different kinds. However, a skilled hacker could write bits of program code into memory that may be executed to perform the hacker's evil deeds.

(v) **HTTP** – HTTP stands for Hypertext Transfer Protocol : HTTP hacks can only be harmful if you are using Microsoft web server software, such as Personal Web Server. There is a bug in this software called an 'unchecked buffer overflow'. If a user makes a request for a file on the web server with a very long name, part of the request gets written into parts of memory that contain active program code. A malicious user could use this to run any program they want on the server.

#### 3.19.4 Auditor's Role

The focus of the IS Auditor is to examine all factors that adversely bear on the confidentiality, integrity and availability of the information, due to improper physical access. Confidentiality, Integrity and Availability (CIA Triad) are the core principles of information safety.



**Fig 3.19 : Principles of Information Safety**

### 3.84 Information Systems Control and Audit

- **Confidentiality**- Preventing disclosure of information to unauthorized individuals or systems.
- **Integrity**- Prevent modification of data by unauthorized personnel.
- **Availability**-Information must be available when it is needed.

The table below summarizes the detective, preventive, corrective and supportive control activities that can ensure the confidentiality, integrity and availability of information/data across information system networks.

Type of System		Intrusion Detection				Vulnerability		
System Control Features		Monitoring				Assessment		
Controls		Application Based	Host Based	Target Based	Network Based	Host Based	Network Based	Password Assessment
D- Detective								
P-Preventive								
C- Corrective								
S-Support								
Confidentiality	Unauthorized access to files and system resources		D			P	P	P
	Modification to files		D	D		P	P	P
	Violation of enterprise system access polices	D	D			P	P	
	Violation of security policies	D	D	D	D	P	P	
	Weak or non-existent passwords	D	D			D		D
Integrity	Placement of Trojan horse or malicious software		D	D		P	P	
	Presence of Trojan horse or malicious software			D				
	Attack Against network services				D		P	
	Script based attacks	D			D	P		
Availability	Denial of Services Attacks				D		P	
	Failure or Mis-configuration of firewalls	D			D	P	P	
	Attacks Happening Over Encrypted Links	D	D					
	Unusual activity or variation from normal data pattern		D		D			

Other	Errors in Network configuration		D			D P C	D P C	
	Liability Exposure associated with attacker using own resources to attack others	P	P	P	P	P	P	P
	Post incident damage assessment	S	S	S	S	S	S	S

Table 3.9 : Network Controls

### 3.20 DATA PRIVACY

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:

- Health information.
- Criminal justice.
- Financial information.
- Genetic information.
- Location information.

The challenge in data privacy is to share data while protecting the personally identifiable information. Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in the aggregate. The idea of sharing the data in the aggregate is to ensure that only non-identifiable data are shared.

The legal protection of the right to privacy in general and of **data privacy** in particular varies greatly around the world.

#### 3.20.1 Protecting data privacy in information systems

Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These falls into two categories : communication and enforcement.

### 3.86 Information Systems Control and Audit

#### (i) Policy Communication

- P3P - The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

#### (ii) Policy Enforcement

- XACML - The eXtensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

### 3.20.2 Data Privacy Policies

- Copyright Notice : All information owned by the company and considered intellectual property, whether written, printed, or stored as data, must be labeled with a copyright notice in the following format : Copyright © 2003 [Company Name], Inc. All Rights Reserved
- E-mail Monitoring : All e-mail must be monitored for the following activity :
- Non-business use inflammatory, unethical, or illegal content disclosure of company confidential information large file attachments or message sizes
- Customer Information Sharing : Corporate customer information may not be shared with outside companies or individuals.
- Encryption of Data Backups : All data backups must be encrypted.
- Encryption of Extranet Connection : All extranet connections must use encryption to protect the privacy of the information traversing the network.
- Data Access : Access to corporate information, hard copy, and electronic data is restricted to individuals with a need to know for a legitimate business reason. Each individual is granted access only to those corporate information resources required for them to perform their job functions.

### 3.21 CONTROLLING AGAINST VIRUSES AND OTHER DESTRUCTIVE PROGRAMS

Destructive programs such as viruses are responsible for huge amount of corporate losses annually. The losses are measured in terms of data corruption and destruction, degraded computer performance, hardware destruction, violations of privacy, and the personnel time devoted for repairing the damage. We have discussed below Virus- one of the more common type of destructive program. Worms, Trojan horse, logic bombs and back doors were discussed in previous sections :

### 3.21.1 Virus

A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating systems in a number of ways. One common technique is for the virus to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. One of the most insidious aspects of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts. Typically, a virus will have a built-in counter that will inhibit its destructive role until the virus has copied itself a specified number of times to other programs and systems. The virus thus grows geometrically, which makes tracing its origin extremely difficult.

Virus programs usually attach themselves to the following types of files:

- An .EXE or .COM program file
- The .OVL (overlay) program file
- The boot sector of a disk
- A device driver program

When a virus-infected program is executed, the virus searches the system for uninfected programs and copies itself into these programs. The virus in this way thus spreads to the applications of other users or to the operating system itself.

### 3.21.2 Anti-virus Software

Among the counter measures against virus attacks, anti-virus software are the most widely used techniques to detect viruses, and prevent their further propagation and harm. There are three types of anti-virus software.

(i) **Scanners** : The software looks for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables and systems fillies to find matching bit patterns. In this context it may be noted that on an average 1500 newer viruses emerge every month. Hence, it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.

(ii) **Active Monitor and Heuristic Scanner** : This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action. However this also makes them inefficient since they cannot differentiate between genuine systems calls and virus action. These could be annoying and generally do not serve the purpose.

(iii) **Integrity Checkers** : These can detect any unauthorized changes to files on the system. They require the software to “take stock” of all files resident on the system and compute a binary check data called the Cyclic Redundancy Check (CRC) When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk. However, such checks assume that frequent changes to applications and systems utilities do not occur.

### **3.88 Information Systems Control and Audit**

Further, technical controls such as securing systems with hardware based password and encryption locks and remote booting are also used. However, there is no single control, which can act as a panacea for all virus attacks. Virus control is in fact a combination of management, technical, administrative, application and importantly operational controls.

The best policy for virus control is preventive control. Of course, detective and controls should be in place to ensure complete control over virus proliferation and damage control.

#### **3.21.3 Recommended policy and procedure controls**

- The Security Policy should address the virus threats, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degrees of risks and suitable controls thereof.
- Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning and quarantining should be given to all employees.
- Hardware installations and associated computing devices should be periodically verified for parameter settings.
- As part of SDLC Controls the development area should be free of viruses and sufficient safeguards must be in place to secure the area from viruses.
- Provision of drives to read media should be restricted to certain controlled terminals and should be write-protected.
- Network access to the Internet should be restricted preferably to stand-alone computers.
- Networks should be protected by means of firewalls that can prevent entry of known viruses.
- The servers and all terminals must have rated anti-virus software installed with sufficient number of user licenses.
- Procedures should ensure that systematic updates are applied to all anti-virus installations at frequent intervals.
- External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified by the Department.
- Vendors and consultants should not be allowed to run their demonstrations and presentations on organizational systems.
- All new software acquisitions should follow a controlled procedure of centralized acquisition and testing for viruses.
- Patches to operating systems and other software and upgrades thereof should be acquired from authentic sources and scanned before installation.
- Reporting and incident handling procedures should be in place to suitably handle virus incidents and eradicate them at the earliest.



- An effective backup plan must be implemented and monitored to ensure that back-up media is not infected and preferably encrypted. Only new media must be used for back-up purposes.

### 3.22 LOGICAL ACCESS CONTROLS

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Assessing logical access controls involves evaluating the following critical procedures :

- Logical access controls restrict users to authorized transactions and functions.
- There are logical controls over network access.
- There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

#### 3.22.1 Logical Access Paths

(i) *Online Terminals* -To access an online terminal a user has to provide a valid logon-ID and password. If additional authentication mechanisms are added along with the password, it will strengthen the security.

*Operator Console* – The operator console is one of the crucial places where any intruders can play havoc. Hence, access to operator console must be restricted. This can be done by

- Keeping the operator console at a place, which is visible, to all.
- By keeping the operator console in a protected room accessible to selected personnel.

(ii) *Batch Job Processing* : In a batch processing environment all jobs are processed in a batch. These batches are processed at regular intervals. The jobs are accumulated and sent as batches. Thus during an accumulation there is a possibility of an unknown job entering into a batch which may challenge security of the data. To avoid this access should be granted only to authorized people i.e., people who can accumulate transactions and who can initiate batch processing. Even the accumulated jobs, which are waiting to be processed, should be controlled appropriately.

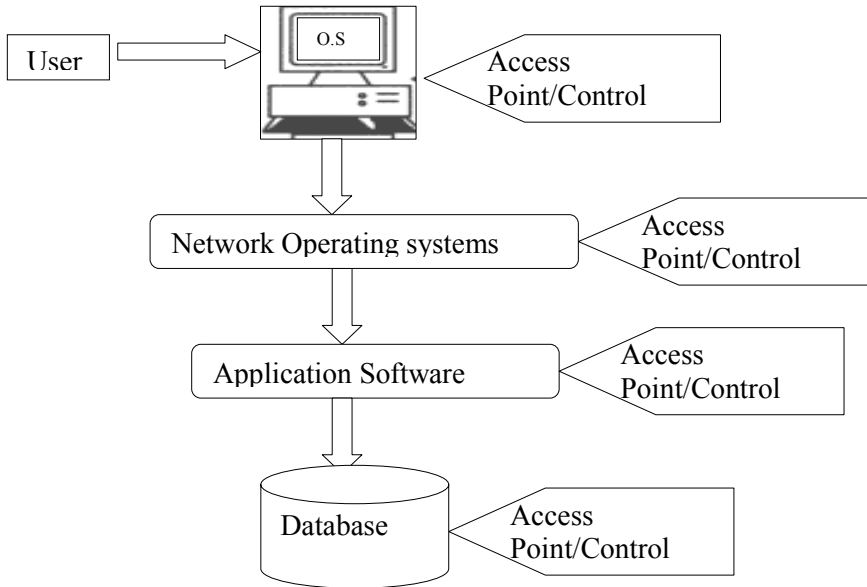
(iii) *Dial-up Ports* : Using a dial up port user at one location can connect remotely to another computer present at an unknown location via a telecommunication media. A modem is a device, which can convert the digital data transmitted to analog data (the one that the telecommunication device uses). Thus the modem can act as an interface between remote terminal and the telephone line. Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line ensures security by confirming the presence and exactness of the data sent.

(iv) *Telecommunication Network* : In a Telecommunication network a number of computer terminals, Personal Computers etc. are linked to the host computer through network or telecommunication lines. Whether the telecommunication lines could be private (i.e.,

### 3.90 Information Systems Control and Audit

dedicated to one user) or public, security is provided in the same manner as it is applied to online terminals.

Each of these routes has to be subjected to appropriate means of security in order to secure it from the possible logical access exposures.



**Fig. 3.20 : Logical Access Paths in an Enterprise Information System**

#### 3.22.2 Logical Access Issues and Exposures

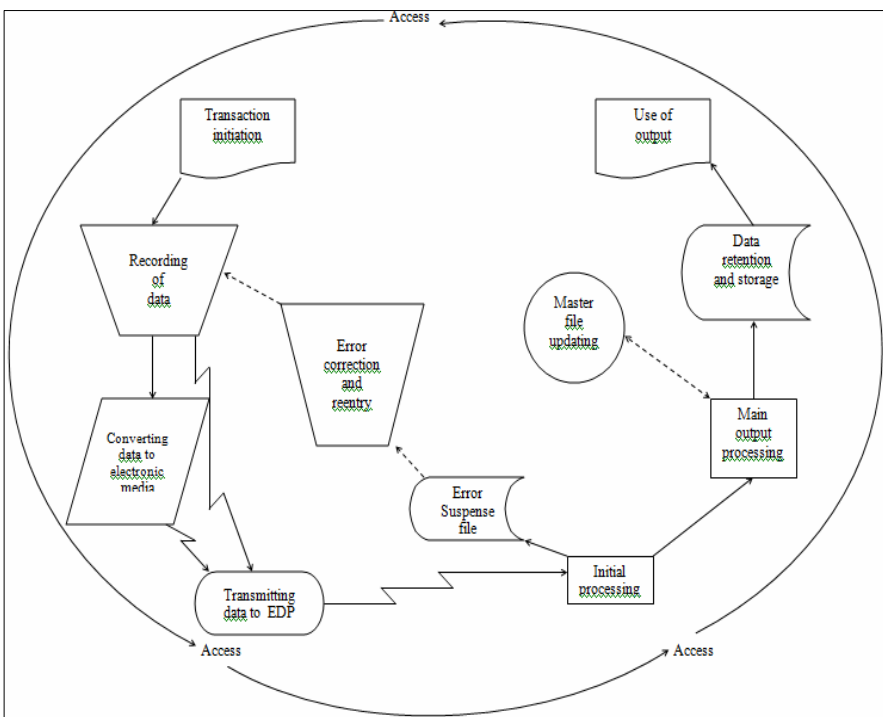
Controls that reduce the risk of misuse (intentional or unintentional), theft, alteration or destruction should be used to protect unauthorized and unnecessary access to computer files. Restricting and monitoring computer operator activities in a batch-processing environment provide this control. The avenues of access are more complex and direct in an online system and hence the level of control for this system must be more complex as shown in Fig.3.20.

Access control mechanisms should be applied not only to computer operators but also to end users, programmers, security administrators, management or any other authorized user. Access control mechanisms should provide security to the following applications:

- Access control software
- Application software
- Data
- Data dictionary/directory
- Dial-up lines
- Libraries
- Logging files

- Operator systems exists
- Password library
- Procedure libraries
- Spool queues
- System software
- Tape files
- Telecommunication lines
- Temporary disk files.
- Utilities.

The above-mentioned utilities should be properly secured to assure security to data.



**Fig. 3.21 : Transaction processing-activities subject to logical controls**

### 3.22.3 Issues and Revelations related to Logical Access

Logical access controls are used to increase the organization's potential for the losses that result due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposure of logical access control encourage technical exposures and computer crimes.

### 3.92 Information Systems Control and Audit

**(a) Technical Exposures** : Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include the following:

(i) *Data Diddling* : Data diddling involves the change of data before or as they are entered into the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect data.

(ii) *Bombs* : Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. Since these programs do not circulate by infecting other programs, chances of a widespread epidemic are relatively slim.

Bombs are generally of the following two types:

- *Time Bomb* : This name has been borrowed from its physical counterpart because of mechanism of activation. A physical time bomb explodes at the time it is set for (unless somebody forces it to explode early), like wise the computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.
- *Logic Bomb* : They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. For example, a code like; "If a file named DELETENOT is deleted then destroy the memory contents by writing ones." This code segment, on execution, may cause destruction of the contents of the memory on deleting a file named DELETENOT. These bombs can be set to go off at a future time or event.

(iii) *Trojan Horse* : These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it. A Trojan-may

- Change or steal the password or
- May modify records in protected files or
- May allow illicit users to use the systems.

Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. The Trojans may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program.

Christmas Card is a well-known example of Trojan. It was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half finished work.

(iv) *Worms* : A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses.

Worms can help to sabotage systems yet they can also be used to perform some useful tasks. For example, worms can be used in the installation of a network. A worm can be inserted in a network and we can check for its presence at each node. A node, which does not indicate the presence of the worm for quite some time, can be assumed as not connected to the network.

Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive.

Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

(v) *Rounding Down* : This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small it gets rarely noticed.

(vi) *Salami Techniques* : This involves slicing of small amounts of money from a computerized transaction or account and is similar to the rounding down technique. A Salami technique is slightly different from a rounding technique in the sense only last few digits are rounded off here. For example, in the rounding down technique, Rs. 21,23,456.39 becomes Rs. 21,23,456.35, while in the Salami technique the transaction amount Rs. 21,23,456.39 is truncated to either Rs. 21,23,456.30 or Rs. 21,23,456.00, depending on the calculation.

*Trap Doors* : Trap doors allow the They are exists out of an authorized program and allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

**(b) Computer Crime Exposures** : Computers can be utilized both constructively and destructively. Computer systems are used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made.

Crimes that are committed using computers and the information they contain can damage the reputation, morale and very existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations.

(i) *Financial Loss* : Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

(ii) *Legal Repercussions* : An organization has to adhere to many human rights laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there are no proper security measures. The IS auditor should take legal counsel while reviewing the issues associated with computer security.

(iii) *Loss of Credibility or Competitive Edge* : In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs

### 3.94 Information Systems Control and Audit

credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.

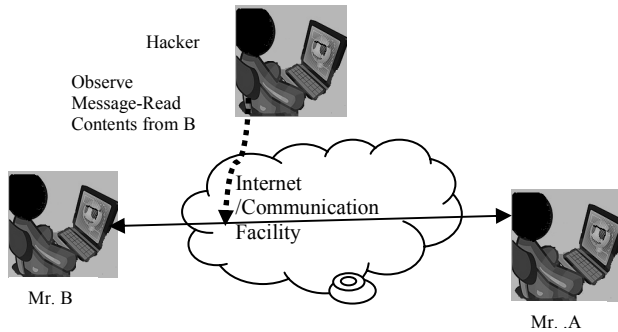
- (iv) *Blackmail/Industrial Espionage* : By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
- (v) *Disclosure of Confidential, Sensitive or Embarrassing Information* : These events can spoil the reputation of the organization. Legal or regulatory actions against the company are also a result of disclosure.
- (vi) *Sabotage* : People who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization or for their intemperance.

*Logical access violators* are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex.

- *Hackers* : Hackers try their best to overcome restrictions to prove their ability. They never try to misuse the computer intentionally.
  - *Employees* (authorized or unauthorized)
  - *IS Personnel* : they have easiest to access to computerized information since they are custodians of this information. Segregation of duties and supervision help to reduce the logical access violations.
  - *End Users*
  - *Former Employees* : should be cautious of former employees who have left the organization on unfavorable terms.
  - *Interested or Educated Outsiders.*
  - Competitors
  - Foreigners
  - Organized criminals
  - Crackers
  - Part-time and Temporary Personnel
  - Vendors and consultants
  - Accidental Ignorant – Violation done unknowingly.
- (vi) *Spoofing* : A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that he is interacting with the operating system. For example, a penetrator duplicates the logon procedure, captures the user's password, attempts for a system crash and makes the user login again. It is only the second time the user actually logs into the system.

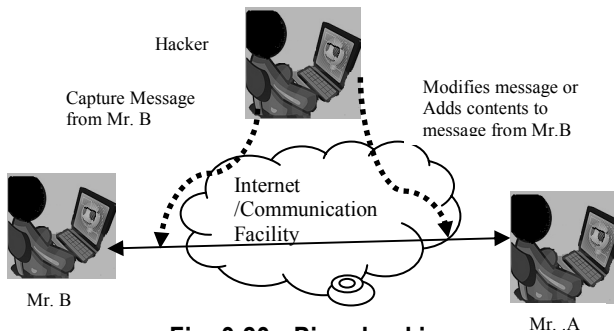
(c) **Asynchronous Attacks** : They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that are waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks.

- (i) *Data Leakage* : Data is critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- (ii) *Wire-tapping* : This involves spying on information being transmitted over telecommunication network.



**Fig. 3.22 : Wire Tapping**

- (iii) *Piggybacking* : This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication communications between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose.

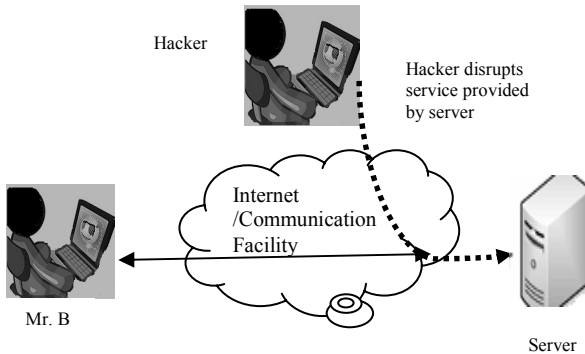


**Fig. 3.23 : Piggybacking**

- (iv) *Shut Down of the Computer/Denial of Service* : This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals who know the high-level systems log on-ID initiate shutting down process. This security measure will function effectively only if there are appropriate access controls on the

### 3.96 Information Systems Control and Audit

logging on through a telecommunication network. When overloading happens some systems have been proved to be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet.



**Fig 3.24 : Denial of Service**

**(d) Remote and distributed data processing** applications can be controlled in many ways.

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- In order to prevent the unauthorized users gain entry into the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

**(e) Physical and Environmental Protection :** Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing physical and environmental protection involves evaluating the following critical procedures :

- Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.
- Data is protected from interception.



- Mobile and portable systems are protected.

### 3.22.4 Logical Access Control Across the System

Logical access controls serve as one of the means of information security. The purpose of logical access controls is to restrict access to information assets / resources. They are expected to provide access to information resources on a need to know and need to have basis using principle of least privileges. It means that the access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused i.e. it should be just sufficient for one to perform one's duty without any problem or restraint. The data, an information asset, can be

- Resident on a machine (for use by an application)
- Stored in some medium (Back up)
- Or it may be in transit.(being transferred from one location to another)

Logical access controls is all about protection of these assets wherever they reside.

User access management	<p><b>User registration</b> Information about every user is documented. The following questions are to be answered : Why is the user granted the access? Has the data owner approved the access? Has the user accepted the responsibility? The de-registration process is also equally important.</p> <p><b>Privilege management</b> Access privileges are to be aligned with job requirements and responsibilities. For example, an operator at the order counter shall have direct access to order processing activity of the application system. He/she will be provided higher access privileges than others. However, misuse of such privileges could endanger the organization's information security. These privileges are to be minimal with respect to their job functions.</p> <p><b>User password management</b> Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password.</p> <p><b>Review of user access rights</b> A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.</p>
User responsibilities	<p>User awareness and responsibility is also an important factor:</p> <p><b>Password use</b> Mandatory use of strong passwords to maintain confidentiality.</p>

3.98 Information Systems Control and Audit

	<p><b>Unattended user equipment</b></p> <p>Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password, and should not leave it accessible to others.</p>
<p>Network access control</p>	<p>An Internet connection exposes an organization to the entire world. This brings up the issue of benefits the organization should derive along with the precaution against harmful elements. This can be achieved through the following means:</p> <p><b>Policy on use of network services</b></p> <p>An enterprise wide applicable internet service requirements aligned with the business need policy based on business needs for using the Internet services is the first step. Selection of appropriate services and approval to access them will be part of this policy.</p> <p><b>Enforced path</b></p> <p>Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; say for example internet access by employees will be routed through a firewall. And to maintain a hierarchical access levels for both internal and external user logging.</p> <p><b>Segregation of networks</b></p> <p>Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office this network is to be isolated from the internet usage service availability for employees.</p> <p><b>Network connection and routing control</b></p> <p>The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.</p> <p><b>Security of network services</b></p> <p>The techniques of authentication and authorization policy implemented across the organization's network.</p>
<p>Operating system access control</p>	<p>Operating system provides the platform for an application to use various IS resources and perform the specific business function. If an intruder is able to bypass the network perimeter security controls, the operating system is the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial.</p> <p><b>Automated terminal identification</b></p> <p>This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.</p> <p><b>Terminal log-on procedures</b></p> <p>The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.</p>

	<p><b>User identification and authentication</b></p> <p>The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.</p> <p><b>Password management system</b></p> <p>An operating system could enforce selection of good passwords. Internal storage of password should use one-way encryption algorithms and the password file should not be accessible to users.</p> <p><b>Use of system utilities</b></p> <p>System utilities are the programs that help to manage critical functions of the operating system—for example, addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.</p> <p><b>Duress alarm to safeguard users</b></p> <p>If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. An example could be forcing a person to withdraw money from the ATM. Many banks provide a secret code to alert the bank about such transactions.</p> <p><b>Terminal time out</b></p> <p>Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.</p> <p><b>Limitation of connection time</b></p> <p>Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday.</p>
Application and monitoring system access control	<p><b>Information access restriction</b></p> <p>The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items he is authorized to access. Controls are implemented on the access rights of users, For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.</p> <p><b>Sensitive system isolation</b></p> <p>Based on the critical constitution of a system in an enterprise it may even be necessary to run the system in an isolated environment.</p> <p>Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.</p>

### 3.100 Information Systems Control and Audit

	<p><b>Event logging</b></p> <p>In Computer systems it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly.</p> <p><b>Monitor system use</b></p> <p>Based on the risk assessment a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.</p> <p><b>Clock synchronization</b></p> <p>Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence the need for synchronizing clock time across as per a standard time is mandatory.</p>
Mobile computing	<p>In today's organizations computing facility is not restricted to a particular data centre alone. Ease of access on the move provides efficiency and results in additional responsibility on users and the need to maintain information security on the management.</p> <p><b>Mobile computing</b></p> <p>Theft of data carried on the disk drives of portable computers is a high risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.</p>

**Table 3.10 : Logical Access Controls**

#### 3.22.5 Role of an IS auditor in evaluating logical access controls

An IS auditor should keep the following points in mind while working with logical access control mechanisms.

- Reviewing the relevant documents pertaining go logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
- The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
- Deficiencies or redundancies must be identified and evaluated.
- By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning.

- He has to evaluate the access control mechanism, analyze the test results and other auditing evidences and verify whether the control objectives has been achieved.
- The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

**3.22.6 Security Policies**

Every organization should have a security policy that defines acceptable behaviors and the reaction of the organization when such behaviors are violated. Security policies are not unique and might differ from organization to organization. The electronic trading, viruses affecting organization’s security documents and the misuse of credit cards have increased and this has augmented the need for security management. Also, legislation relating to information technology is becoming more prolific, with many countries enacting laws on issues such as copyright and software privacy, intellectual property and personal data. These commercial, competitive and legislative pressures require the implementation of proper security policies.

<b>Control Activity</b>	<b>Control Techniques</b>	<b>Audit Procedures</b>
User accounts are appropriately controlled	Resource owners have a list of identified authorized users and the access they are authorized to have.  Passwords, tokens, biometric, smartcards etc are used to identify and authenticate users.  Security administration parameters are set for access to data files, software code libraries, security files and important operating system files.  Naming conventions are established for controlling access to data and programs.  Redundant accounts like default, guest are removed, disabled or secured.	Segregation of duties- To ensure that users do not have access to incompatible functions.  Review policies and procedures which spell out access authorization documentation and user rights and privileges in the information system.  Determine directory names for sensitive directories, files and their access levels and types of access.
	Review access to - shared files -emergency or temporary access to files and hosts These are to be controlled, documented, approved by managers and logged.	Review naming conventions and their use effectively. Verify logs of redundant accounts. Interview Security managers.

### 3.102 Information Systems Control and Audit

		<p>Periodic review with appropriate access documentation with comparisons on account expiry, termination, temporary access and timeliness authorization policies.</p>
<p>Process and Services are adequately controlled</p>	<p>Available processes and services –</p> <ul style="list-style-type: none"> <li>-Installing only required processes and services based on least functionality.</li> <li>-restrict the number of individuals with access to services based on least privileges.</li> </ul> <p>The function of processes and services are monitored, documented and approved by management.</p>	<p>Check procedures for optimized usage of processes and services.</p> <p>Interview the system administrator on –</p> <ul style="list-style-type: none"> <li>-Services installed and their requirement.</li> <li>-Who possess the access their rights and the need?</li> <li>- Monitoring and updation of services and processes.</li> <li>-Scan for inadequately configured, redundant and hazardous processes and services.</li> </ul>
<p>Access to sensitive system resources is restricted and monitored.</p>	<p>Access and use of sensitive/privileged accounts have justified need aligned with valid business purpose.</p> <p>Logical access to these are to be adequately controlled-</p> <ul style="list-style-type: none"> <li>-Remote maintenance.</li> <li>-System libraries.</li> </ul>	<p>Review policies and procedures used for sensitive/privileged accounts.</p> <p>Interview management personnel on access restrictions</p>

**Control Objectives 3.103**

		by testing the need and reasons for an access
	<p>-password/authentication services and directories are controlled and encrypted.</p> <p>-Access restriction based on time/location.</p> <p>-Segregation between user interface services and system management functionality.</p>	<p>Review the accessing system activity logs maintained for –</p> <p>-personnel accessing system software, controls acquired to gain access.</p> <p>-Attempt to access operating system software, system libraries etc.</p> <p>Interview officials along with review related system documentation and coordinate the vulnerability analysis.</p>
Appropriate and adequate media controls are to be implemented.	<p>Only authorized users have access to printed and digital media removal or movement from the information system.</p> <p>Systems media is securely stored with respect to its sensitivity.</p> <p>If sensitive data are protected by approved equipment, techniques and procedures for disposal or exchange of information.</p>	<p>Ensure entity practices and review selected access logs.</p> <p>Review selected media transport practices and receipts.</p> <p>Check if media storage practices are adequate and comply with security parameters associated with information exchange.</p>
Effective use of Cryptographic	For integrity and confidentiality of critical data and programs are protected using cryptographic	Evaluate the strength of

### 3.104 Information Systems Control and Audit

controls.	tools. Based on risk of data communication encryption procedures are implemented.	cryptographic tools by self or expert help. Capture passwords or data transmitted over the network to evaluate their effectiveness.
	Authentication methods are implemented within the information system along with online or manual procedures for cryptographic key exchange and key management.	Interview appropriate officials to compare policies and procedures followed along with supporting documents. Evaluate the practices followed for cryptographic key exchange and management.

**Table 3.11 : Logical Access Control Techniques and their Suggested Audit Procedures**

### 3.23 PHYSICAL ACCESS CONTROLS

This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths. The following issues are discussed:

- Physical Access Issues and Exposures
- Physical Access Controls
- Audit and evaluation techniques for physical access

Also various access control mechanisms are discussed in this section.

#### 3.23.1 Physical Access Issues and Exposures

The following points elucidate the results due to accidental or intentional violation of the access paths:

- Abuse of data processing resources.
- Blackmail
- Embezzlement
- Damage, vandalism or theft to equipments or documents.



- Modification of semester equipment and information.
- Public disclosure of sensitive information.
- Unauthenticated entry

(a) **Possible perpetrators** : Perpetrations may be because of employees who are:

- Accidental ignorant-someone who outrageously violates rules
- Addicted to a substance or gambling
- Discontented
- Experiencing financial or emotional problems
- Former employee
- Interested or informed outsiders, such as competitors, thieves, organized crime and hackers
- Notified of their termination
- On strike
- Threatened by disciplinary action or dismissal

Exposures to confidential matters may be in form the unaware, accidental or anonymous person, although the greatest impact may be from those with malicious or frequent intent.

Other questions and areas of concern include the following:

- How far the hardware facilities are controlled to reduce the risk of unauthorized access?
- Are the hardware facilities protected against forced entry?
- Are intelligent computer terminals locked or otherwise secured to prevent illegal removal of physical components like boards, chips and the computer itself?
- When there is a need for the removal of computer equipment from its normal secure surroundings, are authorized equipment passes required for the removal?

The facilities that need to be protected from the auditor's perspective are:

- Communication closed
- Computer room
- Control units and front-end processors
- Dedicated telephones/telephone lines
- Disposal sites
- Input/Output control room
- Local area networks

### 3.106 Information Systems Control and Audit

- Micro computers and personal computers
- Minicomputer establishments
- Off-site backup file storage facility
- On-site and remote printers
- Operator consoles and terminals
- Portable equipment
- Power sources
- Programming area
- Storage rooms and supplies
- Tape library, tapes, disks and all magnetic media
- Telecommunications equipment

Apart from the computer facility provided, there must be vulnerable access points within the organization, organizational restrictions, and external organization to ensure the effectiveness of the above-mentioned safeguards. Additionally, the IS has to confirm whether similar controls exist within service providers or other third parties and if there are access points, which have the possibility of being damaged so that information within the organization can be sensed.

**(b) Access control Mechanisms** : An access control mechanism associates with identified, authorized users the resources they are allowable to access and action privileges. The mechanism processes the users request for resources in three steps.

- Identification
- Authentication
- Authorization

The following is the sequence in which access control mechanisms operate :

- First and foremost, the users have to identify themselves, thereby indicating their intent to request the usage of system resources.
- Secondly, the users must authenticate themselves and the mechanism must authenticate itself.
- Third, the users request for specific resources, their need for those resources and their areas of usage of these resources.

The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request.

**(c) Identification and Authentication** : Users identify themselves to access control mechanism by providing information such a name or account number. To validate the user, his entry is matched with the entry in the authentication file. The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

Users may provide four classes of authentication information as described in table below:

Remembered information	Name, Account number, passwords
Objects Possessed by the user	Badge, plastic card, key
Personal characteristics	Finger print, voice print, signature
Dialog	Through/around computer

**Table 3.12 : Classes of Authentication**

**(d) Authorization** : There are two approaches to implementing the authorization module in an access control mechanism:

- (a) a “ticket oriented approach”
- (b) a “list oriented approach”

Considering the authorization function in terms of a matrix where rows represent the users and columns represent the resources and the element represents the users privilege on the resources we can see the distinction between these two approaches.

In a *ticket-oriented approach* to authorization, the access control mechanism assigns users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user.

In a *list-oriented approach*, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

This mechanism operates via a column in the matrix.

The table given below illustrates the authorization matrix in an access control mechanism

Resource \ User	File A	Editor	File B	Program
User P	Read	Enter		
User Q	Statistical Read only	Enter		Enter
User R		Enter	Append only	
User S		Enter		Read Resource Code only

**Table 3.13 : Authorization Matrix**

### 3.108 Information Systems Control and Audit

The *primary advantage of the ticket oriented* or capability system is its run-time efficiency.

When a user process is executing, its capability list can be stored in some fast memory device. When the process seeks access to a resource, the access control mechanism simply looks up the capability list to determine if the resource is present in the list and whether if the user is permitted to take the desired action.

The *advantage of list-oriented system* is that it allows efficient administration of capabilities.

Each user process has a pointer to the access control list for a resource. Thus the capabilities for a resource can be controlled since they are stored in one place. It is enough to examine the access control list just to know who has access over the resource and similarly to revoke access to a resource, a user's entry in the access control list simply needs to be deleted.

#### 3.23.2 Physical Access Controls

Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. The authorization given by the management may be explicit, as in a door lock for which management has authorized us to have a key; or implicit, like a job description which confirms the need to access confidential reports and documents.

Some of the more common access control techniques are discussed categorically as follows :

##### (a) Locks on Doors

*Cipher locks (Combination Door Locks)*- The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.

Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

*Bolting Door Locks* – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should be not be duplicated.

*Electronic Door Locks* – A magnetic or embedded chip-based plastics card key or token may be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism. The following points list the advantages of electronic door locks over bolting and combinational locks.

- Through the special internal code, cards can be made to identify the correct individual.
- Individuals access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to particular doors or to particular hours of the day.
- Degree of duplication is reduced.

- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted silent or audible alarms can be automatically activated.
- An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.

*Biometric Door Locks* : These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

**(b) Physical identification medium**

*Personal Identification numbers (PIN)* : A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His entry will be matched with the PIN number available in the security database.

*Plastic Cards* : These cards are used for identification purposes. Controls over card seek to ensure that customers safeguard their card so it does not fall into unauthorized hands.

*Cryptographic Control* : These types of controls help a lot in scheming

*Unauthorized access to data. Cryptography deals with transformation* of data into codes that are meaningless to anyone who does not possess the system for recovering initial data. Only a crypt analyst can do the translation.

*Identification Badges*-special identification badges can be issued to personnel as well as visitors. For easy identification purposes their colour of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys. Issuing accounting for and retrieving the badges administrative prices that must carefully controlled.

**(c) Logging on utilities**

*Manual Logging* : All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both the front reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before gaining entry inside the company.

*Electronic Logging* : This feature is a combination of electronic and biometric security systems. The users logging in can be monitored and the unsuccessful attempts being highlighted.

**(d) Other means of controlling Physical Access**

*Video Cameras* : Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.

### 3.110 Information Systems Control and Audit

*Security Guards* : Extra security can be provided by appointing guards aided with video cameras and locked doors. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.

*Controlled Visitor Access* : A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

*Bonded Personnel* : All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organization.

*Dead man Doors* : These systems encompasses are a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only person permitted in the holding area. Only a single person is permitted at a given point of time and this will surely reduce the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.

*Non-exposure of Sensitive Facilities* : There should be no explicit indication such as presence of windows or directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.

*Computer Terminal Locks* : These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.

*Controlled Single Entry Point* : All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.

*Alarm System* : Illegal entry can be avoided by linking alarm system to inactive entry point motion detectors and the reverse flows of enter or exit only doors, so as to avoid illegal entry. Security personnel should be able to hear the alarm when activated.

*Perimeter Fencing* : Fencing at boundary of the facility may also enhance the security mechanism.

*Control of out of hours of employee-employees* : Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently

*Secured Report/Document Distribution Cart* : Secured carts, such as mail carts, must be covered and locked and should always be attended.

**(e) Accounting Audit Trial** : All the activities taken at the boundary sub systems should be properly recorded in the accounting audit trial so the source and nature of all changes to the database can be identified. The following sorts of data must be kept:

- Action privileges requested.
- Action privileges allowed/deprived of.

- Authentication information supplied.
- Identity of the would-be user of the system.
- Number of log-on attempts.
- Resources requested.
- Resources provided/denied.
- Start and finish time.
- Terminal identifier.

This data allows management or auditor to recreate the time series of events that occurs when a user attempts to gain access to system resources. Periodical evaluation of the audit trail should happen to detect any control weaknesses in the system.

### **3.23.3 Audit and Evaluation Techniques for Physical Access**

Information Systems Processing Facility (IPF) is used to gain an overall understanding and perception of the installation being reviewed. This expedition provides the opportunity to be reviewing the physical access restriction.

Information processing facility (Computer room, programmers area, tape library, printer stations and management offices) and any off-site storage facilities should also be included in this tour.

Much of the testing of physical safeguards can be achieved by visually observation of the safeguards tested previously. Documents to assist with this effort include emergency evacuation procedures, inspection tags, fire suppression system test results and key lock logs. Testing should extend beyond the information processing.

The facility/computer room should include the following related facilities:

- Computer storage rooms (this includes equipment, paper and supply rooms)
- Location of all communication equipment identified on the network diagram.
- Location of all operator consoles.
- Off-site backup storage facility.
- Printer rooms.
- Tape library.
- UPS/generator.

To do thorough testing, we have to look above the ceiling panels and below the raised floor in the computer operations centre. Keen observation is done on smoke and water detectors, and special emphasis is given to general cleanliness and walls that extend all the way to the real ceiling.

### 3.112 Information Systems Control and Audit

The following paths of physical entry should be evaluated for proper security.

- All entrance points.
- Glass windows and walls
- Movable walls and modular cubicles.
- Above suspended ceilings and beneath raised floors.
- Ventilation systems.

These security points must be properly governed to avoid illegal entry.

#### 3.23.4 Role of IS Auditor in Physical Access Controls

Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- (i) *Risk assessment* : The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- (ii) *Controls assessment* : The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- (iii) *Planning for review of physical access controls*. It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.
- (iv) *Testing of controls* : The auditor should review physical access controls to satisfy for their effectiveness. This involves :
  - Tour of organizational facilities including outsourced and offsite facilities.
  - Physical inventory of computing equipment and supporting infrastructure.
  - Interviewing personnel can also provide information on the awareness and knowledge of procedures.
  - Observation of safeguards and physical access procedures. This would also include inspection of :
    - (i) Core computing facilities
    - (ii) Computer storage rooms
    - (iii) Communication closets
    - (iv) Backup and off site facilities
    - (v) Printer rooms



- (vi) Disposal yards and bins
- (vii) Inventory of supplies and consumables.

Some special considerations involve the following:

- (i) All points of entry/exit
  - (ii) Glass windows and walls
  - (iii) Moveable and modular cubicles
  - (iv) Ventilation/air-conditioning ducts
  - (v) False ceiling and flooring panels
- Review of physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices like smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization.
  - Examination of physical access logs and reports. This includes examination of incident reporting logs, problem resolution reports.

<b>Control Activities</b>	<b>Control Techniques</b>	<b>Audit Procedures</b>
Physical safeguards to commensurate with the risks of physical damage or access.	Identify facilities housing sensitive and critical resources. Identify all threats to physical well-being of sensitive and critical resources are being adequately secured using keys, alarm systems, security devices and other access control devices, including- - the badging system. - display and output devices. - data transmission lines. - power equipment and power cabling. - Mobile or portable systems. All deposits and withdrawals of tapes and other storage media from the library are authorized and logged. Emergency exit and reentry procedures ensure that only	Review the physical layout diagram of computer, telecommunications and cooling system facilities.  Walk through facilities.  Review risk analysis.  Review procedures for the removal and return of storage media from and to the library.  Review of written emergency procedures. Observe a fire drill.  Review the knowledge and awareness of emergency procedures by employees with respect to facilities using

### 3.114 Information Systems Control and Audit

	authorized personnel re allowed to reenter after fire drills, etc.	interviews, questionnaires etc.
Establish adequate security at entrance and exists based on risk	<p>All employee access is authorized and credentials (badges, ID cards, smart cards) are issued to allow access.</p> <p>Management conducts regular reviews of individuals with physical access to sensitive facilities.</p> <p>Visitors to the sensitive areas, such as the main computer room and tape/ media library, are formally signed in and escorted.</p> <p>Entry codes are changed periodically.</p>	<p>Review procedures and logs of employee entry and exists during and after normal business hours.</p> <p>Review Procedures used by management to ensure that individuals having access to sensitive facilities are adequately restricted and posses' physical access authorization.</p> <p>Review visitor entry logs.</p> <p>Interview guards at the facility entry.</p> <p>Review documentation on logs of entry, code changes and system maintenance.</p>
Perimeter Security	<p>Control/restrict vehicle and pedestrian traffic with measures like fences, gates, locks, guard posts and inspections.</p> <p>Installation of closed circuit system with recording and warning alarms - 24 hours.</p>	<p>Assess vehicle and pedestrian traffic around high risk facility.</p> <p>Inspect guard procedures and practices for controlling access to facility grounds.</p> <p>Inspect the facility surveillance system to assess its capability in protecting the facility.</p>
Security control policies and procedures are documented, approved and implemented by management.	<p>Security control policies and procedures at all levels-</p> <ul style="list-style-type: none"> <li>-Are document</li> <li>-Address purpose, scope, roles, responsibilities and compliance.</li> <li>-Ensure users can be held accountable for their actions.</li> <li>-are approved by management and</li> <li>- Periodically reviewed and updated.</li> </ul>	<p>Review security policies and procedures at the enterprise level, system level and process level are aligned with business/enterprise stated objectives.</p>

**Table 3.14 : Physical Control Techniques and their Audit Procedures**

### 3.24 ENVIRONMENTAL CONTROLS

This section deals with the external factors in the Information System and Preventive measures to overcome these conflicts. Issues covered are :

- Environmental Issues and exposures
- Audit and Evaluation Techniques for Environmental Controls

From the perspective of environmental exposures and controls, information systems resources may be categorized as follows, with the focus primarily on facilities which house:

(i) *Hardware and Media* : Includes Computing Equipment, Communication equipment, and Storage Media.

(ii) *Information Systems Supporting Infrastructure or Facilities* : This typically includes the following:

- Physical Premises, like Computer Rooms, Cabins, Server Rooms/Farms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas
- Communication Closets
- Cabling ducts
- Power Source
- Heating, Ventilation and Air Conditioning (HVAC)

(iii) *Documentation* : Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.

(iv) *Supplies* : The third party maintenance procedures for say air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.

(v) *People* : The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective information processing facility(IPF) Training of employees and other stake holders on control procedures is a critical component.

#### 3.24.1 Environmental Issues and Exposures

Environmental exposures are primarily due to elements of nature. However, with proper controls, exposure to these rudiments can be reduced.

Common occurrences are:

- Fire
- Natural disasters-earthquake, volcano, hurricane, tornado.
- Power spike
- Air conditioning failure

### 3.116 Information Systems Control and Audit

- Electrical shock
- Equipment failure
- Water damage/flooding-even with facilities located on upper floors of high buildings. Water damage is a risk, usually from broken water pipes
- Bomb threat/attack

*Other environmental issues and revelations include the following:*

- Is the power supply to the computer equipment properly controlled so as to ensure that it remains within the manufacturer's specification?
- Are the air conditioning, humidity and ventilation control systems protected against the effects of electricity using static rug or anti-static spray?
- Is consumption of food, beverage and tobacco products prohibited, by policy, around computer equipment?
- Are backup media protected from damage due to variation in temperatures or are they guarded against strong magnetic fields and water damage?
- Is the computer equipment kept free of dust, smoke and other particulate matter?

In the above section, environmental control is discussed and classifications based on the controls are illustrated. Also the preventive measures that should be taken are also discussed.

#### 3.24.2 Controls for Environmental Exposures

*Water Detectors* : In the computer room, even if the room is on high floor, water detectors should be placed under the raised floor and near drain holes. Water detectors should be present near any unattended equipment storage facilities. When activated, the detectors should produce an audible alarm that can be heard by security and control personnel. For easy identification and reach, the location of the water detectors should be marked on the raised computer room floor. A remedial action must be instantiated on hearing the alarm by notifying the specific individuals and allotting the responsibility for investigating the cause. Other staff should be made aware of the risk of a possible electrocution.

*Hand-Held Fire Extinguishers* ; Fire extinguishers should be in calculated locations throughout the area. They should be tagged for inspection and inspected at least annually.

*Manual Fire Alarms* : Hand-pull fire alarms should be purposefully placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station.

*Smoke Detectors* : Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example a fire station) Fire repression systems should be supplemented and not replaced by smoke detectors.

*Fire Suppression Systems* : These alarms are activated when extensive heat is generated due to fire. Like smoke alarms they are designed to produce audible alarms when activated and

should be regularly monitored. In addition to precautionary measures, the system should be segmented so that fire in one part of a large facility does not activate the entire system.

The fire suppression techniques vary depending upon the situation but its usually one of the following :

- Dry-Pipe sprinkling systems are typically referred to as sprinkler systems. These pipes remain dry and upon activation by the electronic fire alarm water is sent through the pipe. Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment.
- Water based systems also function similar to the sprinkler systems. These systems are effective but also are unpopular because they damage equipment and property. Changed systems are more reliable but the disadvantage is that in the case of leakage or breakage of pipes facilities are exposed to extensive water damage,
- An alternative method can be usage of Halon. Halon systems contain pressurized halon gases that remove oxygen from the air. Halon is preferred to others because of its inertness and it does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system. The drawback is, since halon adversely affects the ozone layer, its usage is restricted to some extent and alternative suppression methods are being explored.

*Strategically Locating the Computer Room* : The reduce the risk of flooding, the computer room should not be located in the basement of a multi-storey building. Studies reveal that the computer room located in the top floors are less prone to the risk of fire, smoke and water.

*Regular Inspection by Fire Department* : An annual inspection by the fire department should be carried out to ensure that all fire detection systems act in accordance with building codes. Also, the fire department should be notified of the location of the computer room, so it should be equipped with tools and appropriate electrical fires.

*Fireproof Walls, Floors and Ceilings surrounding the Computer Room* : Information processing facility should be surrounded by walls that should control or block fire from spreading. The surrounding walls should have at least a more than one-two-hour fire resistance rating.

*Electrical Surge Protectors* : The risk of damage due to power spikes can be reduced to a great extent using electrical surge protectors. The incoming current is measured by the voltage regulator and depending upon the intensity of electric current regulators can increase or decrease the charge of electricity and ensures that a consistent current passes through. Such protectors are typically built into the Uninterruptible Power Supply (UPS) system.

*Uninterruptible Power Supply (UPS) / Generator* : A UPS system consists of a battery or gasoline powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to ensure wattage into the computer is consistent. In case of a power failure, the UPS provides the back up by providing electrical power from the generator to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could

### 3.118 Information Systems Control and Audit

continue to flow for days or for just a few minutes to permit an orderly computer shutdown. A UPS system can be inbuilt or can be an external piece of equipment.

*Power Leads from Two Substations* : Electrical power lines that are exposed to many environmental dangers – such as waters fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply.

*Emergency Power-Off Switch* : When there arises a necessity of immediate power shut down during situations like a computer room fire or an emergency evacuation, a two emergency power-off switch one at computer room and other near but outside the computer room would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

*Wiring Placed in Electrical Panels and Conduit* : Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor.

*Prohibitions Against Eating, Drinking and Smoking within the Information Processing Facility* : These things should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

*Fire Resistant Office Materials* : The materials used in the information processing facility such as Wastebaskets, curtains, desks, cabinets and other general office materials should be fire pool.

*Documented and Tested Emergency Evacuation Plans* : Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation.

#### 3.24.3 Audit and Evaluation techniques for Environmental Controls

*Water and Smoke Detectors* : The presence of water and smoke detectors are verified on visiting the computer room. Also checks relating to adequacy of power supply to these detectors are done. A visual verification is done to test if the locations are clearly marked.

*Hand-Held Fire Extinguishers* : The presence of fire extinguishers in strategic locations throughout the facility is checked for.

*Fire Suppressions Systems* : Testing of suppressions system becomes more expensive, hence reviewing documentation that has been inspected and tested within the last year ensures it.

*Regular Inspection by Fire Department* : The person responsible for fire equipment maintenance is contacted and also the employees are queried, whether, fire department inspector has been invited to tour and inspected the facilities present in the organization.

*Fireproof Walls, Floors and Ceilings Surrounding the Computer Room* : The assistance of building management is taken and checks relating to the location and the documentation that

identifies the fire rating of the walls surrounding the information processing facility are done. These walls should have at least a two-hour fire resistance rating.

*Electrical Surge Protectors* : In this part the presence of electrical surge protectors for sensitive and expensive computer equipment is observed.

*Power Leads from Two Substations* : Checking the location and documentation concerning the use and replacement of redundant power lines into the information processing facility is performed.

*Fully Documented and Tested Business Continuity Plan* : This section will be discussed elaborately in chapter 6.

*Wiring Placed in Electrical Panels and Conduit* : Checking of whether the wiring in the information processing facility is placed in the fire-resistant panels and conduit is done.

*Documented and Tested Emergency Evacuation Plans* : A direct interview of the employees is conducted to test whether the emergency plans are posted through out the facilities, whether in an organizing manner, that does not leave the facilities physically unsecured.

*Humidity/Temperature Control* : Visit the information processing facility to visit on regular intervals and physically determine if temperature and humidity are adequate.

#### **3.24.4 Role of Auditor in Environmental Controls**

The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environmental controls it is understood should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should take into account while conducting his audit are given below:

#### **3.24.5 Audit planning and assessment**

As part of risk assessment

- The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risks that may arise.
- The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones are in place.
- The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
- Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.

### 3.120 Information Systems Control and Audit

- The IS auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
- Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

#### 3.24.6 Audit of technical controls

Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. He must verify:

- The IPF and the construction with regard to the type of materials used for construction.
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
- The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
- Emergency procedures, evacuation plans and marking of fire exists. If necessary, the IS Auditor may also use a mock drill to test the preparedness with respect to disaster.
- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors.
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power.
- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- Activities in the IPF. Identify undesired activities such as smoking, consumption of eatables etc.

#### 3.24.7 Documentation

As part of the audit procedures, the IS auditor should also document all findings. The working papers could include audit assessments, audit plans, audit procedures, questionnaires, interview sheets, inspection charts etc.

Control Activities	Control Techniques	Audit Procedures
Safeguards against the risks of heating, ventilation and air-conditioning systems.	Identify systems that provide constant temperature and humidity levels within the organization.	Review a heating, ventilation and air-conditioning design to verify proper functioning within an organization.



**Control Objectives 3.121**

Control of radio emissions affect on computer systems.	Evaluate electronic shielding to control radio emissions that affect the computer systems.	Review any shielding strategies against interference or unauthorized access through emissions.
Establish adequate interior security based on risk	Critical systems have emergency power supplies for alarm systems; monitoring devices, exit lighting, communication systems.	Verify critical systems (alarm systems, monitoring devices, entry control systems) have emergency power supplies.  Identify back -up systems and procedures and determine the frequency of testing. Review testing results.
Adequately protect against emerging threats, based on risk.	Appropriate plans and controls such as shelter in place or for a potential CBR attack(chemical, biological and radioactive attack) Restricting public access and protect critical entry points-air intake vents, protective grills and roofs.	Interview officials, review planning documents and related test results. Observe and document the controls in place to mitigate emerging threats. Observe location of these devices and identify security measures implemented.  Verify the controls existence and intrusion detection sensors.
Adequate environmental controls have been implemented	Fire detection and suppression devices are installed and working.(smoke detectors, fire extinguishers and sprinkle systems)  Controls are implemented to mitigate disasters, such as floods, earthquakes.  Redundancy exists in critical systems like, uninterrupted power supply, air cooling system, and backup generators  Humidity, temperature, and voltage control are maintained and acceptable levels Emergency lighting, power	Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, shut-off power switches, air -ventilation apparatus and other emergency devices.  Determine that humidity, temperature and voltage are controlled within the accepted levels.  Check cabling, plumbing, room ceiling smoke detectors, water detectors on the floor are installed and in proper working order.

### 3.122 Information Systems Control and Audit

	outages and evacuation routes are appropriately located.	
Staff have been trained to react to emergencies	Operational and support personnel are trained and understand emergency procedures.  Emergency procedures are documented and periodically tested- incident plan, inspection plan and maintenance plan.	Interview security personnel to ensure their awareness and responsibilities.  Review training records and documentation. Determine the scope and adequacy of training.  Review test policies, documentation and know-how of operational staff.  Review incident handling procedures and maintenance and inspection plan.

**Table 3.15. Environmental Controls and their Audit Procedures**

## Master Checklist on Logical Access Controls

The following is an illustrative questionnaire that could be used to review Logical Access Controls within application systems and databases.

No	Checkpoints
<b>User Access Management Policy and Procedure</b>	
1.	Whether the user access management policy and procedure are documented?
2.	Whether the user access management policy and procedure are approved by the management?
3.	Whether the user access management policy and procedure document includes: <ul style="list-style-type: none"> <li>- Scope and objective.</li> <li>- Procedure for user ID creation, approval, review, suspension, and deletion.</li> <li>- Granting access to third parties.</li> <li>- Password management.</li> <li>- User access rights assignment &amp; modifications.</li> <li>- Emergency access Granting.</li> <li>- Monitoring access violations.</li> <li>- Review and update of document.</li> </ul>
<b>User Access Management</b>	
1.	Whether User ID & access rights are granted with an approval from appropriate level of IS and functional head? <i>(Verify the user ID creation, granting of access right and approval process)</i>
2.	Whether the organization follows the principle of segregation of duties adequately in granting access rights? <i>(Verify Access rights should be given on need to know and need to do basis – without unchecked concentration of power.)</i>
3.	Whether User IDs are in a unique format? <i>(Verify the naming conventions for the user IDs)</i>
4.	Whether invalid log in attempts are monitored and User IDs are suspended on specific attempt? <i>(Verify the parameters set for unsuccessful log in attempt)</i>
5.	Whether the organisation follows complex composition for password parameters? <i>(Complex composition of password parameter should be used as to make it difficult for guess and prevent unauthorised users from access e.g. special character and numbers should be part of password, Restrict use of organisation's name, 123, xyz or other generic terms as password)</i>
6.	Whether granting access to the third parties is according to the User Access Management policy and procedure?

### 3.124 Information Systems Control and Audit

No	Checkpoints
	<i>(The organization should specify and implement a process for granting access to third parties like contractors, suppliers, auditors, consultants etc.)</i>
7.	Whether users are forced to change password on first log-on and at periodic intervals? <i>(Verify password parameters for first log on and password aging)</i>
8.	Whether the organisation implemented clear screen and clear desk policies? <i>(Terminals should be automatically logged off if remaining idle for specific time.)</i>
9.	Whether the organisation restricted concurrent log- on? <i>(One user ID should not be allowed to be logged-in for two different terminals at the same time)</i>
10.	Whether users' IDs are shared? <i>(Verify whether users' IDs are shared among the employees/ users or not?)</i>
11.	Whether multiple user IDs are allocated to a single individual?
12.	Are user access policy and procedure documents communicated / available to the respective users?
13.	Whether User IDs and Password are communicated to the user in a secured manner? <i>(Verify the procedure for communicating user ID and password for the first time and after suspension)</i>
14.	Whether the organisation reviews user IDs and access rights at periodic intervals?
15.	Whether the organisation monitors logs for the user access?
16.	Whether policy and procedure documents reviewed and updated at regular intervals?
17.	Whether the access to scheduled job is restricted to the authorised?
18.	Whether an emergency user creation is according to the policy and procedure for User Access Management? <i>(Verify the emergency access granting procedure, including approvals and monitoring)</i>
19.	Whether periodic review process ensures user accounts align with business needs and removal on termination/transfer? <i>(Review and evaluate procedures for creating user accounts and ensure that accounts are created only when there's a legitimate business need and that accounts are removed or disabled in a timely fashion in the event of termination or job change.)</i>
20.	Whether passwords are shadowed and use strong hash functions? <i>(Ensure the strength of passwords and access permission to password files. Review and evaluate the strength of system passwords and the use of password controls such as aging.)</i>
21.	Review the process for setting initial passwords for new users and communicating those passwords and evaluate the tracking of each account to a specific employee.

No	Checkpoints
22.	Whether the use of groups and access levels set for a specific group determines the restrictiveness of their use? (Evaluate the use of passwords, access rights at the group level)
23.	Ensure that the facility to logon as super/root user is restricted to system console for security reasons.
24.	Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.
25.	Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.
26.	Verify the parameters in the system to control automatic log-on from a remote system, concurrent connections a user can have, users logged on to the system at odd times (midnight, holidays, etc) and ensure whether they have been properly set according to security policy.
	Maintenance of sensitive user accounts
1.	Ascertain as to who is the custodian of sensitive passwords such as super/root user and verify if that person is maintaining secrecy of the password, whether the password has been preserved in a sealed envelope with movement records for usage in case of emergency.
2.	From the log file, identify the instances of use of sensitive passwords such as super user and verify if records have been maintained with reason for the same. Ensure that such instances have been approved/ authorized by the management.
3.	From the log file, identify the instances of unsuccessful logon attempts to super user account and check the terminal ID / IP address from which it is happening. Check if appropriate reporting and escalation procedures are in place for such violations

### Master Checklist for Physical and Environmental Security

To ensure IS assets are maintained in a secured manner within a controlled environment.

Sr. No.	Check points
<b>Secured Physical Access</b>	
1.	Whether Physical Access Control Policy is documented and approved?
2.	Whether the policy on the following is appropriate and covers: <ul style="list-style-type: none"> <li>- Lay out of facilities</li> <li>- Physical Security of the assets</li> <li>- Access to the assets</li> <li>- Maintenance of the assets</li> <li>- Signage on the facilities</li> <li>- Labels for assets</li> <li>- Visitors' authorization and recording</li> <li>- Entrance and exit procedures</li> <li>- Legal &amp; regulatory requirements</li> </ul>
3.	Whether critical IS facilities (like data center) are located appropriately? (Verify the location for the following as:- <ul style="list-style-type: none"> <li>- Protection against natural disasters like earthquakes, flooding, extreme weather etc.</li> <li>- Not in congested places</li> <li>- Not being on ground or top floor</li> <li>- Not being below ground level to avoid water leakage etc.</li> <li>- Not having a showcase window</li> <li>- Not having a direct access from the outside or through a public hallway</li> <li>- Place which is not obvious externally)</li> </ul>
4.	Whether the access to IS facilities is controlled through a secured mechanism? (Verify the access control mechanism - e.g. access card, lock and key or manned reception)
5.	Whether the access to the IS facilities is limited to approved persons only? (Approved persons may include employees, vendors and customers)
6.	Whether the physical access control procedures are adequate and appropriate for approved persons? (Access should be provided on need to do and need to know basis)
7.	Whether the visitor to critical IS facilities are escorted by employees? (Records for visitors' access should be maintained)
8.	Whether a periodical review of access rights is carried out?

9.	Whether the physical security is continually addressed?
10.	Whether all access routes are identified and controls are in place?
11.	Whether the security awareness is created not only in IS function but also across the organization?
12.	Whether the physical security is ensured at suppliers' facilities also in cases where organization's' assets (either physical or data) are processed at supplier's facilities?
13.	Whether the usage of any equipment outside the business premises for information processing is authorized by the management?
14.	Is the security provided to equipment used outside business premises similar to / same as that offered to equipment used inside the business premises?
15.	Whether adequate monitoring equipments are present to monitor the movements of the personnel inside the facility?
16.	In case of outsourced software, whether all maintenance work is carried out only in the presence of/ with the knowledge of appropriate IS staff?
17.	Whether appropriate access controls like password, swipe card, bio-metric devices etc. are in place and adequate controls exist for storing the data/ information on them? Are there controls to ensure that the issue and re-collection of such access devices are authorized and recorded?
18.	Whether access violations are recorded, escalated to higher authorities and appropriate action taken?
19.	Whether employees are required to keep the critical / sensitive documents in secured places?
20.	Check if facility IS related risks with respect to lighting, building orientation, signage and neighborhood characteristics are identified?
21.	Do the network, operating system and application monitoring procedures provide ample information to identify associated risks?
22.	Verify that surveillance systems are designed and operating properly?
23.	Ensure that physical access control procedures are comprehensive and being followed by security staff.
24.	Verify if the security controls in place are appropriate to prevent intrusion into sensitive IS facilities –data centre, communication hubs, emergency power services facilities?
25.	Review facility monitoring measures to ensure that alarm conditions are addressed promptly.

### **Environmental Controls**

1.	Whether the Environmental Control policy is documented and approved?
2.	Whether IS facilities are situated in a place that is fire resistant? (Verify for wall, floor, false ceiling, furniture and cabling being noncombustible / fire resistant / fire retardant)

### 3.128 Information Systems Control and Audit

3.	Whether smoking restrictions in IS facilities are in place?
4.	Whether adequate smoke / temperature detectors are installed, connected to the fire alarm system and tested?
5.	Whether fire instructions are clearly posted and fire alarm buttons clearly visible?
6.	Whether emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place?
7.	Whether fire prevention and control measures implemented are adequate and tested periodically?
8.	Whether fire drill and training are conducted periodically?
9.	Whether air-conditioning, ventilation and humidity control procedures are in place, tested periodically and monitored on an ongoing basis?
10.	Whether an adequate alternate power arrangement is available? If so, is it covered under maintenance?
11.	Whether alternative water, fuel, air-conditioning and humidity control resources are available?
12.	Check if heating, ventilation, and air-conditioning systems maintain constant temperatures within a data center and other IS facilities?
13.	Evaluate the data center's use of electronic shielding to verify that radio emissions do not affect computer systems or that system emissions cannot be used to gain unauthorized access to sensitive information.
14.	Verify if there are sufficient battery backup systems providing continuous power during momentary black-outs and brown-outs along with generators that protect against prolonged power loss and are in good working.
15.	Ensure that a fire alarm is protecting a critical IS facility like data center from the risk of fire, a water system is configured to detect water in high-risk areas of the data center and a humidity alarm is configured to notify data center personnel of either high or low-humidity conditions.
16.	Check logs and reports on the alarm monitoring console(s) and alarm systems which are to be monitored continually by data center/IS facility personnel.
17.	Verify that fire extinguishers are placed every 50ft within data center isles and are maintained properly with fire suppression systems are protecting the data center from fire.
18.	Whether there are emergency plans that address various disaster scenarios for example backup data promptly from off-site storage facilities?
19.	Ensure if there exists a comprehensive disaster recovery plan that key employees are aware of their roles in the event of a disaster and are updated and tested regularly.
20.	Ensure that detail part inventories and vendor agreements are accurate and current and maintained as critical assets.



**Self-examination questions**

1. Discuss the effect of computers on internal controls.
2. Write a short note on COBIT.
3. Write short notes on following:
  - (a) Preventive controls.
  - (b) Detective controls.
  - (c) Corrective controls.
  - (d) Compensatory control.
4. Discuss various security objectives of audit trails.
5. Write a short note on error correction.
6. Discuss Key Maintainability Controls.
7. What is acceptance testing? Discuss various types of acceptance testing.
8. Briefly discuss role of IS auditor in acceptance testing.
9. What is the scope of Post Implementation Review (PIR)? Discuss various activities to be undertaken during PIR.
10. Discuss change management control.
11. What do you understand by testing and quality control? Discuss the role of IS auditor for quality control.
12. How information can be classified?
13. Discuss various data integrity controls.
14. What are the procedures which are evaluated for assessing logical access control? Discuss.
15. What issues should be considered for physical access controls? Discuss.
16. Write short notes on the following:
  - (a) Crypto Systems
  - (b) Data encryption system
  - (c) Public key infrastructure
  - (d) Fire walls.
17. What do you understand by unauthorized intrusion? What is hacking?
18. What do you understand by term 'Virus'? Discuss various anti-virus softwares.
19. Discuss the role of IS auditor in
  - (i) Physical access control
  - (ii) Environmental controls.

### 3.130 Information Systems Control and Audit

#### Sources:

1. Information Technology Control and Audit, Sandra Senft & Frederick Gallegos, Third Edition, Auerbach Publications, 2009
2. Information System Control and Audit, Ron Weber
3. Technical Guide on IS Audit, ICAI, Second Edition, January, 2009
4. Federal Information System Controls Audit Manual (Fiscam)-Exposure Draft, Gao, July 2008
5. [www.itgi.org](http://www.itgi.org)-IT Governance Institute
6. [www.isaca.org](http://www.isaca.org)-Information Systems Audit and Control Association.

## TESTING – GENERAL AND AUTOMATED CONTROLS

---

### 4.1 INTRODUCTION TO BASICS OF TESTING (REASONS FOR TESTING)

**Testing** is a process used to identify the correctness, completeness and quality of developed computer software. In other words testing is nothing but CRITICISM or COMPARISON, i.e. comparing the actual value with expected one.

There are many approaches to software testing, but effective testing of complex products is essentially a process of investigation and not merely a matter of creating and following procedures. One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. Although most of the intellectual processes of testing are nearly identical to that of review or inspection, the word testing is connoted to mean the dynamic analysis of the product—putting the product through its paces. Testing helps in verifying and validating if the software is working as it is intended to be working.

### 4.2 SOFTWARE TESTING FUNDAMENTALS

#### 4.2.1 Testing objectives : It include

- Testing is a process of executing a program with the intent of finding an error.
- A good test case is one that has a high probability of finding a yet undiscovered error.
- A successful test is one that uncovers a yet undiscovered error.

Testing should systematically uncover different classes of errors in a minimum amount of time and with a minimum amount of effort. A secondary benefit of testing is that it demonstrates that the software is working as stated in the specifications. The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

**4.2.2 When testing should start:** Testing early in the life cycle reduces the errors. Test deliverables are associated with every phase of development. The goal of software tester is to find bugs, find them as early as possible, and make sure that they are fixed.

## 4.2 Information Systems Control and Audit

### Causes of Bugs :

- (i) The number one cause of software bugs is the **specification**. There are several reasons why specifications are the largest bug producer. In many instances a specification simply isn't written. Other reasons may be that the specification isn't thorough enough, it is constantly changing, or it is not communicated well to the entire team. Planning of the software is vitally important. If it is not done correctly, bugs will be created.
- (ii) The next largest source of bugs is the **design**, This is the stage where the programmers lay the plan for their Software. Compare it to an architect creating the blue print for the building, Bugs occur here for the same reason they occur in the specification i.e. when the design is rushed, changed, or not well communicated.
- (iii) **Coding errors** may be more familiar to you if you are a programmer. Typically these can be traced to the software complexity, poor documentation, schedule pressure or just plain dump mistakes. It is important to note that many bugs that appear on the surface to be programming errors can really be traced to specification. The other category is the catch-all for what is left. Some bugs can be blamed for false positives, conditions that were thought to be bugs but really weren't. There may be duplicate bugs, multiple ones that resulted from the square root cause. Some bugs can be traced to testing errors.

**4.2.3 Costs** : The cost increases tenfold as time increases. A bug found and fixed during the early stages when the specification is being written may cost. However, very less the same bug, if not found until the software is coded and tested would cost more to rectify and re-test.

**4.2.4 When to Stop Testing** : This can be difficult to determine. Many modern software applications are so complex, and run in such an interdependent environment, that complete testing can never be done. "When to stop testing" is one of the most difficult questions to a test engineer. Common factors in deciding when to stop are:

- Deadlines (release deadlines, testing deadlines.)
- Test cases completed with certain percentages passed
- Test budget depleted
- Coverage of code/functionality/requirements reaches a specified point
- The rate at which bugs are found is too small
- Beta or Alpha Testing period ends
- The risk in the project is under acceptable limit.

Practically, the decision of stopping testing is based on the level of the risk acceptable to the management. As testing is a never ending process we can never assume that 100 % testing has been done. The risk can be measured by Risk analysis but for small duration / low budget / low resources project, risk can be deduced by simply : -

- Measuring Test Coverage.
- Number of test cycles.
- Number of high priority bugs.

### 4.2.5 Test Strategy

A test strategy is the plan to cover the product in such a way so as to develop an adequate assessment of quality. A good test strategy is:

- Specific
- Practical
- Justified

The purpose of a test strategy is to clarify the major tasks and challenges of the test project. Test Approach and Test Architecture are other terms commonly used to describe test strategy. The strategy would include:

#### (I) Test Plan - Why

- Identify Risks and Assumptions up front to reduce surprises later.
  - Communicate objectives to all team members.
  - Foundation for Test Spec, Test Cases, and ultimately the Bugs we find.
- Failing to plan = planning to fail.

#### (II) Test Plan - What

- Derived from Test Approach, Requirements, Project Plan, Functional Spec., and Design Spec.
- Details out project-specific Test Approach.
- Lists general (high level) Test Case areas.
- Include testing Risk Assessment.
- Include preliminary Test Schedule
- Lists Resource requirements.

## 4.3 TEST PLAN

The test strategy identifies multiple test levels, which are going to be performed for the project. Activities at each level must be planned well in advance and it has to be formally documented. Based on the individual plans only, the individual test levels are carried out. Test Plans may be of different types e.g.

- Unit test Plan
- Integration test Plan
- System test Plan
- Acceptance Test Plan

#### 4.4 Information Systems Control and Audit

(i) **UNIT TEST PLAN {UTP}** : The unit test plan is the overall plan to carry out the unit test activities. The lead tester prepares it and it is distributed to the individual testers, which contains the following sections.

- **What is to be tested?** The unit test plan must clearly specify the scope of unit testing. In this, normally the basic input/output of the units along with their basic functionality will be tested. In this case mostly the input units will be tested for the format, alignment, accuracy and the totals. The UTP will clearly give the rules of what data types are present in the system, their format and their boundary conditions. This list may not be exhaustive; but it is better to have a complete list of these details.
- **Sequence of Testing** : The sequences of test activities that are to be carried out in this phase are to be listed in this section. This includes, whether to execute positive test cases first or negative test cases first, to execute test cases based on the priority, to execute test cases based on test groups etc. Positive test cases prove that the system performs what is supposed to do; negative test cases prove that the system does not perform what is not supposed to do. Testing the screens, files, database etc., are to be given in proper sequence.
- **Basic Functionality of Units** : How the independent functionalities of the units are tested which excludes any communication between the unit and other units. The interface part is out of scope of this test level. Apart from the above sections, the following sections are addressed, very specific to unit testing.
  - Unit Testing Tools
  - Priority of Program units
  - Naming convention for test cases
  - Status reporting mechanism
  - Regression test approach

(ii) **INTEGRATION TEST PLAN** : The integration test plan is the overall plan for carrying out the activities in the integration test level, which contains the following sections.

- **What is to be tested?** This section clearly specifies the kinds of interfaces which fall under the scope of testing viz., internal and external interfaces. There is no need to go deep in terms of technical details but the general approach i.e. how the interfaces are triggered is explained.
- **Sequence of Integration** : When there are multiple modules present in an application, the sequence in which they are to be integrated will be specified in this section. In this, the dependencies between the modules play a vital role. If a unit B has to be executed, it may need the data that is fed by unit A and unit X. In this case, the units A and X have to be integrated and then using that data, the unit B has to be tested. This has to be stated to the whole set of units in the program. Given this correctly, the testing activities will lead to the product, slowly building the product, unit by unit and then integrating them.

(iii) **SYSTEM TEST PLAN {STP}** : The system test plan is the overall plan carrying out the system test level activities. In the system test, apart from testing the functional aspects of the system, there are some special testing activities carried out, such as stress testing etc. The following are the sections normally present in system test plan.

- **What is to be tested?** This section defines the scope of system testing, very specific to the project. Normally, the system testing is based on the requirements. All requirements are to be verified in the scope of system testing. This covers the functionality of the product. Apart from this what special testing is performed are also stated here.
- **Functional Groups and the Sequence** : The requirements can be grouped in terms of the functionality. Based on this, there may also be priorities among the functional groups. For example, in a banking application, anything related to customer accounts can be grouped into one area, anything related to inter-branch transactions may be grouped into one area etc. Same way for the product being tested, these areas are to be mentioned here and the suggested sequences of testing of these areas, based on the priorities are to be described.

(iv) **ACCEPTANCE TEST PLAN {ATP}** : The client at their place performs the acceptance testing. It will be very similar to the system test performed by the software development unit. Since the client is the one who decides the format and testing methods as part of acceptance testing, there is no specific clue on the way they will carry out the testing. However, but it will not differ much from the system testing. It can be assumed that all the rules, which are applicable to system test, can be implemented to acceptance testing also.

Since this is just one level of testing done by the client for the overall product, it may include test cases including the unit and integration test level details.

#### 4.4 TEST PLAN OUTLINE

A sample Test Plan Outline along with their description is as shown below:

- **BACKGROUND** : This item summarises the functions of the application system and the tests to be performed.
- **INTRODUCTION**
- **ASSUMPTIONS** : Indicates any anticipated assumptions which will be made while testing the application.
- **TEST ITEMS** : List each of the items (programs) to be tested.
- **FEATURES TO BE TESTED** : List each of the features (functions or requirements) which will be tested or demonstrated by the test.
- **FEATURES NOT TO BE TESTED** : Explicitly lists each feature, function, or requirement which won't be tested and why not.

## 4.6 Information Systems Control and Audit

- **APPROACH** : Describe the data flows and test philosophy, simulation or live execution, etc. This section also mentions all the approaches which will be followed at the various stages of the test execution.
- **ITEM PASS/FAIL CRITERIA** : Blanket statement - Itemised list of expected output and tolerances
- **SUSPENSION/RESUMPTION CRITERIA** : Must the test run from start to completion? Under what circumstances it may be resumed in the middle? Establish check-points in long tests.
- **TEST DELIVERABLES** : What, besides software, will be delivered? Test report  
Test software
- **TESTING TASKS** : Functional tasks (e.g., equipment set up) Administrative tasks
- **ENVIRONMENTAL NEEDS** : Security clearance Office space & equipment  
Hardware/software requirements
- **RESPONSIBILITIES** : Who does the tasks? What does the user do?
- **STAFFING & TRAINING**
- **SCHEDULE**
- **RESOURCES**
- **RISKS & CONTINGENCIES**
- **APPROVALS**

## 4.5 TYPES OF SOFTWARE TESTING

- **Static testing** : The verification activities fall into the category of Static Testing. During static testing, you have a checklist to check whether the work you are doing is going as per the set standards of the organisation. These standards can be for Coding, Integrating and Deployment. Review's, Inspection's and Walkthrough's are static testing methodologies.
- **Dynamic Testing** : Dynamic Testing involves working with the software, giving input values and checking if the output is as expected. These are the Validation activities. Unit Tests, Integration Tests, System Tests and Acceptance Tests are few of the Dynamic Testing methodologies. As we go further, let us understand the various Test Life Cycle's and get to know the Testing Terminologies.



Testing could be classified based on the methodology involved. Some of the common testing methodologies are described below:

#### 4.6 BLACK BOX TESTING

Black box testing attempts to derive sets of inputs that will fully exercise all the functional requirements of a system. It is not an alternative to white box testing. This type of testing attempts to find errors in the following categories:

1. incorrect or missing functions,
2. interface errors,
3. errors in data structures or external database access,
4. performance errors, and
5. initialisation and termination errors.

Tests are designed to answer the following questions:

- How is the function's validity tested?
- What classes of input will make good test cases?
- Is the system particularly sensitive to certain input values?
- How are the boundaries of a data class isolated?
- What data rates and data volume can the system tolerate?
- What effect will specific combinations of data have on system operation?

**Equivalence Partitioning** : This method divides the input domain of a program into classes of data from which test cases can be derived. Equivalence partitioning strives to define a test case that uncovers classes of errors and thereby reduces the number of test cases needed. It is based on an evaluation of equivalence classes for an input condition. An equivalence class represents a set of valid or invalid states for input conditions.

Equivalence classes may be defined according to the following guidelines:

1. If an input condition specifies a range, one valid and two invalid equivalence classes are defined.
2. If an input condition requires a specific value, then one valid and two invalid equivalence classes are defined.
3. If an input condition specifies a member of a set, then one valid and one invalid equivalence class are defined.
4. If an input condition is Boolean, then one valid and one invalid equivalence class are defined.

## 4.8 Information Systems Control and Audit

**Boundary Value Analysis (BVA)** : This method leads to a selection of test cases that exercise boundary values. It complements equivalence partitioning since it selects test cases at the edges of a class. Rather than focusing on input conditions solely, BVA derives test cases from the output domain also. BVA guidelines include:

1. For input ranges bounded by a and b, test cases should include values a and b and just above and just below a and b respectively.
2. If an input condition specifies a number of values, test cases should be developed to exercise the minimum and maximum numbers and values just above and below these limits.
3. Apply guidelines 1 and 2 to the output.
4. If internal data structures have prescribed boundaries, a test case should be designed to exercise the data structure at its boundary.

**Cause-Effect Graphing Techniques** : Cause-effect graphing is a technique that provides a concise representation of logical conditions and corresponding actions. There are four steps:

1. Causes (input conditions) and effects (actions) are listed for a module and an identifier is assigned to each.
2. A cause-effect graph is developed.
3. The graph is converted to a decision table.
4. Decision table rules are converted to test cases.

## 4.7 WHITE BOX TESTING

White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived that

- guarantee that all independent paths within a module have been exercised at least once,
- exercise all logical decisions on their true and false sides,
- execute all loops at their boundaries and within their operational bounds, and
- exercise internal data structures to ensure their validity.

**4.7.1 The Nature of Software Defects** : Logic errors and incorrect assumptions are inversely proportional to the probability that a program path will be executed. General processing tends to be well understood while special case processing tends to be prone to errors.

We often believe that a logical path is not likely to be executed when it may be executed on a regular basis. Our unconscious assumptions about control flow and data lead to design errors that can only be detected by path testing.

Typographical errors are random.

**4.7.2 Basis Path Testing** : This method enables the designer to derive a logical complexity measure of a procedural design and use it as a guide for defining a basis set of execution paths. Test cases that exercise the basis set are guaranteed to execute every statement in the program at least once during testing.

**4.7.3 Flow Graphs** : Flow graphs can be used to represent control flow in a program and can help in the derivation of the basis set. Each flow graph node represents one or more procedural statements. The edges between nodes represent flow of control. An edge must terminate at a node, even if the node does not represent any useful procedural statements. A region in a flow graph is an area bounded by edges and nodes. Each node that contains a condition is called a predicate node.

**4.7.4 Loop Testing** : This white box technique focuses exclusively on the validity of loop constructs. Four different classes of loops can be defined:

- **Simple loops** : The following tests should be applied to simple loops where  $n$  is the maximum number of allowable passes through the loop:
  1. skip the loop entirely,
  2. only pass once through the loop,
  3.  $m$  passes through the loop where  $m < n$ ,
  4.  $n - 1, n, n + 1$  passes through the loop.
- **Nested loops** : The testing of nested loops cannot simply extend the technique of simple loops since this would result in geometrically increasing number of test cases. One approach for nested loops:
  1. Start at the innermost loop. Set all other loops to minimum values.
  2. Conduct simple loop tests for the innermost loop while holding the outer loops at their minimums. Add tests for out-of-range or excluded values.
  3. Work outward, conducting tests for the next loop while keeping all other outer loops at minimums and other nested loops to typical values.
  4. Continue until all loops have been tested.
- **Concatenated loops** : Concatenated loops can be tested as simple loops if each loop is independent of the others. If they are not independent (e.g. the loop counter for one is the loop counter for the other), then the nested approach can be used.
- **Unstructured loops** : This type of loop should be redesigned not tested!!!

Other white box testing techniques include:

1. Condition testing exercises the logical conditions in a program.
2. Data flow testing selects test paths according to the locations of definitions and uses of variables in the program.

## 4.10 Information Systems Control and Audit

### 4.8 UNIT TESTING

In computer programming, a unit test is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.

**4.8.1 Benefits :** The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. It provides a written contract that the piece must satisfy. This isolated testing provides following main benefits:

- **Encourages change :** Unit testing allows the programmer to re-factor code at a later date, and make sure the module still works correctly (regression testing). This provides the benefit of encouraging programmers to make changes to the code since it is easy for the programmer to check if the piece is still working properly.
- **Simplifies Integration :** Unit testing helps eliminate uncertainty in the pieces themselves and can be used in a bottom-up testing style approach. By testing the parts of a program first and then testing the sum of its parts will make integration testing easier.
- **Documents the code :** Unit testing provides a sort of "living document" for the class being tested. Clients wishing to learn to use the class can look at the unit tests to determine how to use the class to fit their needs.

**4.8.2 Limitations :** It is important to realise that unit-testing will not catch every error in the program. By definition, it only tests the functionality of the units themselves. Therefore, it will not catch integration errors, performance problems and any other system-wide issues. In addition, it may not be trivial to anticipate all special cases of input the program unit under study may receive in reality. Unit testing is only effective if it is used in conjunction with other software testing activities.

### 4.9 REQUIREMENT TESTING

#### Usage

- To ensure that system performs correctly
- To ensure that correctness can be sustained for a considerable period of time.
- System can be tested for correctness through all phases of SDLC but incase of reliability the programs should be in place to make system operational.

#### Objectives

- Successful implementation of user requirements,
- Correctness maintained over considerable period of time
- Processing of the application complies with the organisation's policies and procedures.

- Secondary users needs are fulfilled: Security officer, DBA, Internal auditors, Record retention, Comptroller

**How to Use :**

- These test conditions are generalised ones, which becomes test cases as the SDLC progresses until system is fully operational.
- Test conditions are more effective when created from user's requirements.
- It must be noted that if test conditions are created from documents then in case of any error in the documents, these errors are likely to get incorporated in Test conditions and consequently testing would not be able to find those errors.
- Test conditions, if created from other sources (other than documents), makes error trapping more effective.
- Functional Checklist created.

**When to Use**

- Every application should be Requirement tested
- Should start at Requirements phase and should progress till operations and maintenance phase.
- The method used to carry requirement testing and the extent of it is important.

**4.10 REGRESSION TESTING**

**Usage**

- All aspects of system remain functional after testing.
- Change in one segment does not change the functionality of other segment.

**Objectives**

- System documents remain current
- System test data and test conditions remain current
- Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

**How to Use**

- Test cases, which were used previously for the already tested segment is, re-run to ensure that the results of the segment tested currently and the results of same segment tested earlier are same.
- Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious.

## 4.12 Information Systems Control and Audit

- In this case of testing cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum.

### When to Use

- When there is high risk that the new changes may affect the unchanged areas of application system.
- In development process: Regression testing should be carried out after the pre-determined changes are incorporated in the application system.
- In Maintenance phase : regression testing should be carried out if there is a high risk that loss may occur when the changes are made to the system

## 4.11 ERROR HANDLING TESTING

### Usage

- It determines the ability of applications system to process the incorrect transactions properly
- Errors encompass all unexpected conditions.
- In some systems a large part of programming effort will be devoted to handling error condition.

### Objectives

The objective of error handling testing is to determine that:

- Application system recognises all expected error conditions
- Accountability of processing errors has been assigned and procedures provide a high probability that errors will be properly corrected
- During correction process reasonable control is maintained over errors.

### How to Use

- A group of knowledgeable people is required to anticipate what can go wrong in the application system.
- It is needed that all the application knowledgeable people assemble to integrate their knowledge of user area, auditing and error tracking.
- Then logical test error conditions should be created based on this assimilated information.

### When to Use

- Throughout SDLC.
- Impact from errors should be identified and should be corrected to reduce the errors to acceptable level.
- Used to assist in error management process of system development and maintenance.

## 4.12 MANUAL SUPPORT TESTING

### Usage

- It involves testing of all the functions performed by the people while preparing the data and using these data from automated system.

### Objectives

- Verify that manual support documents and procedures are correct.
- Determine that manual support responsibility is correct
- Determine that manual support people are adequately trained.
- Determine that manual support and automated segment are properly interfaced.

### How to Use

- Process evaluated in all segments of SDLC.
- Execution can be done in conjunction with normal system testing.
- Instead of preparing, execution and entering actual test transactions the clerical and supervisory personnel can use the results of processing from application system.
- To test people it requires testing the interface between the people and application system.

### When to Use

- Verification that manual systems function properly should be conducted throughout the SDLC.
- Should not be done at later stages of SDLC.
- Best done at installation stage so that the clerical people do not get used to the actual system just before system goes to production.

## 4.13 INTER SYSTEM TESTING

### Usage

- To ensure interconnection between application functions correctly.

### Objective

- Proper parameters and data are correctly passed between the applications
- Documentation for involved system is correct and accurate.
- Proper timing and coordination of functions exists between the application systems.

## 4.14 Information Systems Control and Audit

### How to Use

- Operations of multiple systems are tested.
- Multiple systems are run from one another to check that they are acceptable and processed properly.

### When to Use

- When there is change in parameters in application system
- The parameters, which are erroneous then risk associated to such parameters, would decide the extent of testing and type of testing.
- Intersystem parameters would be checked / verified after the change or new application is placed in the production.

## 4.14 CONTROL TESTING

### Usage

- Control is a management tool to ensure that processing is performed in accordance to what management desire or intents of management.

### Objective

- Accurate and complete data
- Authorised transactions
- Maintenance of adequate audit trail of information.
- Efficient, effective and economical process.
- Process meeting the needs of the user.

### How to Use

- To test controls risks must be identified.
- Testers should have negative approach i.e. should determine or anticipate what can go wrong in the application system.
- Develop risk matrix, which identifies the risks, controls; segment within application system in which control resides.

### When to Use

- Should be tested with other system tests.



## 4.15 PARALLEL TESTING

### Usage

- To ensure that the processing of new application (new version) is consistent with respect to the processing of previous application version.

### Objective :

- Conducting redundant processing to ensure that the new version or application performs correctly.
- Demonstrating consistency and inconsistency between 2 versions of the application.

### How to Use

- Same input data should be run through 2 versions of same application system.
- Parallel testing can be done with whole system or part of system (segment).

### When to Use

- When there is uncertainty regarding correctness of processing of new application where the new and old version are similar.
- In financial applications like banking where there are many similar applications the processing can be verified for old and new version through parallel testing.

## 4.16 VOLUME TESTING

It is the testing of the behaviour when the maximum number of users is concurrently active and when the database contains the greatest data volume.

The creation of a volume test environment requires considerable effort. It is essential that the correct level of complexity exists in terms of the data within the database and the range of transactions and data used by the scripted users, if the tests are to reliably reflect the production environment. Once the test environment is built it must be fully utilised. Volume tests offer much more than simple service delivery measurement. The exercise should seek to answer the following questions:

1. What service level can be guaranteed? How can it be specified and monitored?
2. Are changes in user behaviour likely? What impact will such changes have on resource consumption and service delivery?
3. Which transactions/processes is resource hungry in relation to their tasks?
4. What are the resource bottlenecks? Can they be addressed?
5. How much spare capacity is there?

## 4.16 Information Systems Control and Audit

The purpose of volume testing is to find weaknesses in the system with respect to its handling of large amount of data during extended time periods

### 4.17 STRESS TESTING

The purpose of stress testing is to find defects in the system capacity of handling large numbers of transactions during peak periods. For example, a script might require users to login and proceed with their daily activities while, at the same time, requiring that a series of workstations emulating a large number of other systems are running recorded scripts that add, update, or delete from the database.

### 4.18 PERFORMANCE TESTING

System performance is generally assessed in terms of response time and throughput rates under differing processing and configuration conditions. To attack the performance problems, there are several questions should be asked first:

1. How much application logic should be remotely executed?
2. How much updating should be done to the database server over the network from the client workstation?
3. How much data should be sent in each transaction?

### 4.19 CONCURRENT OR CONTINUOUS AUDIT AND EMBEDDED AUDIT MODULES

Today, organisations produce information on a real-time, online basis. Real-time recordings needs real-time auditing to provide continuous assurance about the quality of the data, thus, continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.

Errors in a computerised system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least. Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

**Types of audit tools** : Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available which could be used for selecting and testing data. Many audit tools are also available some of which are described below:

- (I) **Snapshots** : Tracing a transaction in a computerised system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilised to assess

the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are 1) to locate the snapshot points based on materiality of transactions 2) when the snapshot will be captured and 3) the reporting system design and implementation to present data in a meaningful way.

- (II) **Integrated Test Facility (ITF)** : The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

**Methods of Entering Test Data** : The transactions to be tested have to be tagged. The application system has to be programmed to recognise the tagged transactions and have them invoke two updates, one to the application system master file record and one to the ITF dummy entity. Auditors can also embed audit software modules in the application system programs to recognise transactions having certain characteristics as ITF transactions. Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing. However, use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing.

The auditors may also use test data that is specially prepared. Test transactions would be entered along with the production input into the application system. In this approach the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way. However, preparation of the test data could be time consuming and costly.

**Methods of Removing the Effects of ITF Transactions** : The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed. The application system may be programmed to recognise ITF transactions and to ignore them in terms of any processing that might affect users. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal. The effects of the transactions are not really removed.

- (III) **System Control Audit Review File (SCARF)** : The system control audit review file (SCARF) technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

## 4.18 Information Systems Control and Audit

Auditors might use SCARF to collect the following types of information:

- **Application system errors** : SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
  - **Policy and procedural variances** : Organisations have to adhere to the policies, procedures and standards of the organisation and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
  - **System exception** : SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
  - **Statistical sample** : Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
  - **Snapshots and extended records** : Snapshots and extended records can be written into the SCARF file and printed when required.
  - **Profiling data** : Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
  - **Performance measurement** : Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.
- (IV) **Continuous and Intermittent Simulation (CIS)** : This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:
- The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
  - CIS replicates or simulates the application system processing.
  - Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
  - Exceptions identified by CIS are written to a exception log file.

- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

**Advantages and Disadvantages of Continuous Auditing :** Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. Continuous auditing has a number of potential benefits including:

- (1) reducing the cost of the basic audit assignment by enabling auditors to test a larger sample (up to 100 percent) of client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;
- (2) reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;
- (3) increasing the quality of audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structure; and
- (4) specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

Audit evidence gathered by performing tests of controls can be used as a basis for reducing more costly substantive tests, analytical procedures, transactions analysis, access and data flow. With continuous auditing, auditors may conduct tests of controls simultaneously with substantive tests, analytical procedures, etc. to gather persuasive evidence regarding the quality and integrity of the client's electronic system in producing reliable and credible information. CATTs can be used in performing tests of transactions continuously throughout the year in order to reduce the extent of substantive tests to be performed at the end of a period.

Some of the advantages of continuous audit techniques are as under:

- *Timely, comprehensive and detailed auditing* : Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- *Surprise test capability* : As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- *Information to system staff on meeting of objectives* : Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- *Training for new users* :Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

## **4.20 Information Systems Control and Audit**

The following are some of the disadvantages and limitations of the use of the continuous audit system :

- Auditors should be able to obtain resources required from the organisation to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

### **4.20 HARDWARE TESTING**

Hardware testing may be done to the entire system against the Functional Requirement Specification(s) (FRS) and/or the System Requirement Specification (SRS). Focus is to have almost a destructive attitude and test not only the design, but also the behaviour and even the believed expectations. It is also intended to test up to and beyond the bounds defined in the software/hardware requirements specification(s).

#### **Types of Hardware Testing**

- Functional testing
- User Interface testing
- Usability testing
- Compatibility testing
- Model Based testing
- Error exit testing
- User help testing
- Security testing
- Capacity testing
- Performance testing
- Reliability testing
- Recovery testing
- Installation testing

- Maintenance testing
- Accessibility testing

#### 4.21 REVIEW OF HARDWARE

- Review the capacity management procedures for hardware and performance evaluation procedures to determine:
  - ◆ Whether they ensure continuous review of performance and capacity in terms of hardware, software, networks, user needs, business needs, management objectives and service levels.
  - ◆ Whether historical data and analysis obtained from the Information System (IS) trouble logs, processing schedules, job accounting system reports, preventative maintenance schedules and reports are used in Information System (IS) management's hardware performance monitoring.

Ensure that the technical management's decision to acquire or dispose off computing related hardware and software are indeed based on results of capacity planning models and workload forecasts tempered with good business judgement.

- Review the hardware acquisition plan to determine :
  - ◆ Whether the IS management has issued written policy statements regarding the acquisition of hardware.
  - ◆ Whether the criteria for the acquisition of hardware are laid out and procedures and forms established to facilitate the acquisition approval process.
  - ◆ Whether the hardware acquisition plan is in concurrence with the strategic business plan of management.
  - ◆ Whether there is awareness of the budget constraints.
  - ◆ Whether the requests for the acquisition of hardware are supported by cost benefit analysis.
  - ◆ Whether all hardware are purchased through the IS purchasing department to take advantage of volume discounts or other quality benefits.
  - ◆ Whether the environment is conducive and space is adequate to accommodate the current and new hardware.
  - ◆ Whether IS management's hardware acquisition plan has taken into consideration technological obsolescence of the installed equipped, as well the new equipment in the acquisition plan.
  - ◆ Whether there has been a consideration of lease expirations on current equipment.

## 4.22 Information Systems Control and Audit

- ◆ Whether documentation for hardware and software specifications, installation requirements, warranties, guarantees and likely lead-time associated with planned acquisitions is properly maintained.
- Review the change in management controls for the following :
  - ◆ Determine if changes to hardware configuration are planned and timely information is given to the individual responsible for scheduling.
  - ◆ Determine whether the change schedules allow time for adequate installation and testing of new hardware.
  - ◆ Verify that the operator documentation is appropriately updated to reflect changes in hardware.
  - ◆ Select samples of hardware changes that have affected the scheduling of IS processing and determine if the plans for changes are being addressed in a timely manner.
  - ◆ Ensure there is a cross-reference between the change and its cause, i.e. the problem.
  - ◆ Ascertain whether the system programmers, application programmers and the IS staff have been informed of all hardware changes to ensure that changes are co-ordinated properly.
- Review the preventive maintenance practices to evaluate the adequacy and the timeliness of preventive maintenance as under:
  - ◆ Understand the frequency of scheduled preventive maintenance work performed by the hardware vendors and the in-house staff.
  - ◆ Compare this frequency to hardware maintenance contract. Note any exceptions.
  - ◆ Determine compliance with maintenance contractual agreements by examining maintenance log.
  - ◆ Ascertain whether scheduled maintenance has had any adverse effect on the production schedule during peak season.
  - ◆ Determine whether preventive maintenance logs are retained. Identify any abnormal hardware or software problems.
  - ◆ Ensure that the hardware maintenance period commences on the same day as the warranty or guarantee expires. This prevents additional maintenance charges while in warranty period and also eliminates the time gap between the expiry of the warranty period and the commencement of maintenance.
  - ◆ Verify whether the maintenance agreement has a maintenance call response time defined. It is the maximum time allowed between notification of a problem and the arrival of the maintenance staff.



## 4.22 OPERATING SYSTEM REVIEW

When testing operating software development, acquisition or maintenance, the following approach may be adopted:

- Interview technical service manager, system programming manager, and other personnel regarding:
  - ◆ Review and approval process of option selection
  - ◆ Test procedures for software implementation
  - ◆ Review and approval procedures for test results
  - ◆ Implementation procedures
  - ◆ Documentation requirements
  - Review the feasibility study and selection process to determine the following:
    - ◆ Proposed system objectives and purposes are consistent with the request/proposal
    - ◆ Same selection criteria are applied to all proposals
- Review cost /benefit analysis of system software procedures to determine they have addressed the following areas:
  - ◆ Direct financial costs associated with the product
  - ◆ Cost of product maintenance
  - ◆ Hardware requirements and capacity of the product
  - ◆ Training and technical support requirements
  - ◆ Impact of the product on processing reliability
  - ◆ Impact on data security
  - ◆ Financial stability of the vendor's operations
- Review controls over the installation of changed system software to determine the following :
  - ◆ That all appropriate levels of software have been implemented and that predecessor updates have taken place
  - ◆ System software changes are scheduled when they least impact IS processing.
  - ◆ A written plan was established for testing changes to system software.
  - ◆ Tests are being completed as planned.
  - ◆ Problems encountered during testing were resolved and the changes were re-tested.

#### 4.24 Information Systems Control and Audit

- ◆ Test procedures are adequate to provide reasonable assurance that changes applied to the system correct known problems and do not create new problems .
- ◆ Software will be identified before it is placed into the production environment.
- ◆ Fallback or restoration procedures are in place in case of production failure.
- Review system software maintenance activities to determine the following:
  - ◆ Changes made to the system software are documented.
  - ◆ The vendor supports current versions of the software.
- Review system software change controls to determine the following :
  - ◆ Access to the libraries containing the system software is limited to individual(s) needing to have such access.
  - ◆ Changes to the software must be adequately documented and tested prior to implementation.
  - ◆ Software must be properly authorised prior to moving from the test environment to the production environment.
- Review systems documentation specifically in the areas of:
  - ◆ Installation control statements
  - ◆ Parameter tables
  - ◆ Exit definitions
  - ◆ Activity logs/reports
- Review and test systems software implementation to determine adequacy of controls in :
  - ◆ Change procedures
  - ◆ Authorisation procedures
  - ◆ Access security features
  - ◆ Documentation requirements
  - ◆ Documentation of system testing
  - ◆ Audit trails
  - ◆ Access controls over the software in production.
- Review authorisation documentation to determine whether :
  - ◆ Additions, deletions or changes to access authorisation have been documented.
  - ◆ Attempted violation reporting and follow-up have been documented.
- Review system software security for the following:

- ◆ Procedures have been established to restrict the ability to circumvent logical security access controls.
- ◆ Procedures have been established to limit access to the system interrupt capability.
- ◆ Existing physical and logical security provisions are adequate to restrict access to the master consoles.
- ◆ System software vendor-supplied installation passwords were changed at the time of installation.
- Review database supported information system controls to determine the following :
  - ◆ Access to shared data is appropriate.
  - ◆ Data organisation is appropriate.
  - ◆ Adequate change procedures are utilised to ensure the integrity of the database management software.
  - ◆ Integrity of the database management system's data dictionary is maintained.
  - ◆ Data redundancy is minimised by the database management system where redundant data exists, appropriate cross-referencing is maintained within the system's data dictionary or other documentation.

#### 4.23 REVIEWING THE NETWORK

The review of controls over LANs is done to ensure that standards are in place for designing and selecting a LAN architecture and for ensuring that the costs of procuring and operating the LAN do not exceed the benefits.

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 and network design
- Significant LAN components (such as servers and modems)
- Network topology (including internal LAN configuration as well as interconnections to other LANs, WANs or public networks).
- LAN uses, including significant traffic types and main applications used over the network.
- LAN administrator
- Significant groups of LAN users

In addition, the reviewer should gain an understanding of the following:

- Functions performed by the LAN Administrator
- The company's division or department procedures and standards relating to network design support, naming conventions and data security.
- LAN transmission media and techniques, including bridges, routers and gateways.

## 4.26 Information Systems Control and Audit

Understanding the above information should enable the reviewer to make an assessment of the significant threats to the LAN, together with the potential impact and probability of occurrence of each threat. Having assessed the risks to the LAN, the reviewer should evaluate the controls used to minimise the risks.

Physical controls should protect LAN hardware and access points to the LAN by limiting access to those individuals authorised by management. Unlike most mainframes, the computers in a LAN are usually decentralised. Company data stored on a file server is easier to damage or steal than when on a mainframe and should be physically protected. The reviewer should review the following:

LAN hardware devices, particularly the file server and documentation, should be located in a secure facility and restricted to the LAN administrator. The wiring closet and cabling should be secure.

Keys to the LAN file server facility should be controlled to prevent or minimise the risk of unauthorised access.

LAN file server housing should be locked or otherwise secured to prevent removal of boards, chips and the computer itself.

To test physical security, a reviewer should perform the following:

- Inspect the LAN wiring closet and transmission wiring and verify they are physically secured.
- Observe the LAN file server computer and verify it is secured in a manner to reduce the risk of removal of components and the computer itself.
- Obtain a copy of the key logs for the file server room and the wiring closet, match the key logs to actual keys that have been issued and determine that all keys held are assigned to the appropriate people, for example, the LAN Administrator and support staff.
- Select a sample of keys held by people without authorised access to the LAN file server facility and wiring closet and determine that these keys do not permit access to these facilities.
- Look for LAN operating manuals and documentation not properly secured.
- Environmental controls for LANs are similar to those considered in the mainframe environment. However, the equipment may not require as extensive atmospheric controls as a mainframe. The following should be considered:
  - LAN file server equipment should be protected from the effects of static electricity (anti-static rug) and electrical surges (surge protector)
  - Air conditioning and humidity control systems should be adequate to maintain temperatures within manufacturers' specifications.

- The LAN should be equipped with an uninterrupted power supply (UPS) that will allow the LAN to operate in case of minor power fluctuations or in case of a prolonged power outage.
- The LAN file server facility should be kept free of dust, smoke and other matter particularly food.
- Backup diskettes and tapes should be protected from environmental damage and the effects of magnetic fields.

To test environmental controls, a reviewer should visit the LAN file server facility and verify:

- Temperature and humidity are adequate.
- Static electricity guards are in place.
- Electric surge protectors are in place.
- Fire extinguishers are nearby.
- Observe the LAN file server facility, looking for food and beverage containers and tobacco products in the area and in the garbage cans.
- Observe the storage methods and media for backup and verify they are protected from environmental damage.
- LAN logical security controls should be in place to restrict, identify and report authorised and unauthorised users of the LAN.
- Users should be required to have unique passwords and be required to change them periodically. Passwords should be encrypted and not displayed on the computer screen when entered.
- LAN user access should be based on written authorisation, on a need to know/need to do basis. This should include documenting requests for adds, changes and detection of LAN logical access.
- A LAN workstation should be disabled automatically after a short period of inactivity.
- Remote access to the system supervisor should be prohibited. For maximum security an individual should only be able to logon to the supervisor account on the console terminal. This combination of physical security over consoles and logical security over the supervisor account provides for maximum protection against unauthorised access.
- All logon attempts to the supervisor account should be logged on in the computer system.
- The LAN supervisor should maintain up-to-date information about all communication lines connected to the outside.

## 4.28 Information Systems Control and Audit

To test logical security, a reviewer should interview the person responsible for maintaining LAN security to ensure that person is:

- Aware of the risks associated with physical and logical access that must be minimised.
- Aware of the need to actively monitor logons and to account for employee changes.
- Knowledgeable in how to maintain and monitor access.

The reviewer should also perform the following interview users to access their awareness of management policies regarding LAN security and confidentiality.

- Evaluate a sample of LAN users' access /security profiles to ensure access is appropriate and authorised based on the individual's responsibilities.
- Review a sample of the security reports to :
- Ensure only authorised access is occurring.
- Verify timely and effective review of these reports is occurring and that there is evidence of the review.
- Look for unauthorised users. If found, determine the adequacy and timeliness of follow-up procedures
- Attempt to gain access using variety of unauthorised logon-IDs/passwords. Verify that access is denied and logged. Logon to and briefly use the LAN. Then, verify that access and use are properly recorded on the automated activity report.
- If the LAN logon session automatically logs off after a short period of inactivity, logon to the terminal and visually verify the automatic logoff feature.
- Visually search for written passwords in the general areas of the computer that utilise the LAN.
- If the LAN is connected to an outside source through a modem or dial-up network, attempt to gain access to the LAN through these telecommunications mediums using authorised and unauthorised management.
- Review a sample of LAN access change requests and determine if the appropriate management authorises them and that the standard form has been utilised.

### Self - Examination Questions

1. What are the objectives of software testing?
2. How are the commencement and the cessation of testing determined?
3. What are the different types of test plans?
4. How does a unit test plan differ from an acceptance test plan?
5. What are the components of a unit test plan?

6. Describe the components of a test plan?
7. How does black box testing differ from white box testing?
8. What are the kinds of errors that a black box testing finds out?
9. What is equivalence partitioning?
10. Describe boundary wall analysis?
11. Describe loop testing?
12. What are the benefits and limitations of unit testing?
13. When and how is requirement testing used? What are its objectives?
14. Error Handling technique, inter system testing, manual support testing are useful in what areas of testing?
15. What is control testing? Describe with example.
16. Why is parallel testing used? How is it done?
17. What is performance testing?
18. Continuous audit may be performed without embedded audit modules. Comment?
19. Describe various concurrent audit tools?
20. What are the advantages and disadvantages of continuous auditing?
21. Describe in short the review methodology for hardware?
22. What are the various kinds of hardware testing?
23. How would an operating system test be performed?
24. Testing the LAN and its environment is a vital part of IS Audit? Give an overview of the procedure to do so?

## RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

---

### LEARNING OBJECTIVES :

- To perform risk assessment and develop counter measures.
- To prepare action plan for risk mitigation.

### 5.1 INTRODUCTION

Risk assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exists, that can cause an unplanned interruption of business processes, and what costs accrue due to an interruption.

There are various analytical procedures that are used to determine the various risks, threats, and exposures faced by an organization. These are known by various names, such as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) and so on.

Risk assessment consists of two basic components they are data collection and its analysis. The data collected in risk assessment should include a comprehensive list of business processes and their resource dependencies. The purpose of risk analysis involves threat identification and risk mitigation.

### 5.2 RISK, THREAT, EXPOSURE, AND VULNERABILITY

**Risk** : A risk is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:

- (a) Widespread use of technology.
- (b) Interconnectivity of systems.
- (c) Elimination of distance, time and space as constraints.
- (d) Unevenness of technological changes.



## 5.2 Information Systems Control and Audit

- (e) Devolution of management and control.
- (f) Attractiveness of conducting unconventional electronic attacks against organisations.
- (g) External factors such as legislative, legal and regulatory requirements or technological developments.

This means there are new risk areas that could have a significant impact on critical business operations, such as:

- (a) External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information.
- (b) Growing potential for misuse and abuse of information system affecting privacy and ethical values.
- (c) Increasing requirements for availability and robustness.

Because new technology provides the potential for dramatically enhanced business performance, improved and demonstrated information risk reduction and security measures. Technology can also add real value to the organisation by contributing to interactions with the trading partners, closer customer relations, improved competitive advantage and protected reputation.

A **threat** is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organisation. Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services



**Fig. 5.2.1 : Risk and Vulnerabilities**

**Vulnerability** is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially “allow” a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Here are two more vulnerability examples:

- Leaving your front door unlocked makes your house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make your automated information system vulnerable to password cracking or guessing routines.

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

An **exposure** is the extent of loss the organisation has to face when a risk materialises. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources.

**Likelihood** of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

**Attack** is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. Simply, it is the act of trying to defeat IS safeguards. The type of attack and its degree of success will determine the consequence of the attack.

Any risk still remaining after the counter measures are analysed and implemented is called **Residual Risk**. An organisation's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimised, but it can seldom be eliminated. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk can be managed.

### 5.3 THREATS TO THE COMPUTERISED ENVIRONMENT

Any computerised environment is dependent on people. They are a critical links in making the entire enterprise computing happen. As such threats emanate from people themselves. The special skill sets such as IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers to the user requirements. Social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. Threats also arise on account of dependence on external agencies. IT computing services are significantly dependant on various vendors and service providers e.g., equipment supply and support, consumables, systems and program maintenance, air-conditioning, hot-site providers, utilities, etc. A few common threats to the computerised environment can be:

- (a) **Power failure** : Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- (b) **Communication failure** : Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organisation depends on public communication lines e.g. for e-banking, communication failure present a significant threat that will have a direct impact on operations.
- (c) **Disgruntled Employees** : A disgruntled employee presents a threat since, with access to sensitive information of the organisation, he may cause intentional harm to the information processing facilities or sabotage operations.
- (d) **Errors** : Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to "allow"

## 5.4 Information Systems Control and Audit

attachments instead of “deny” may result in the entire organisation network being compromised with virus attacks.

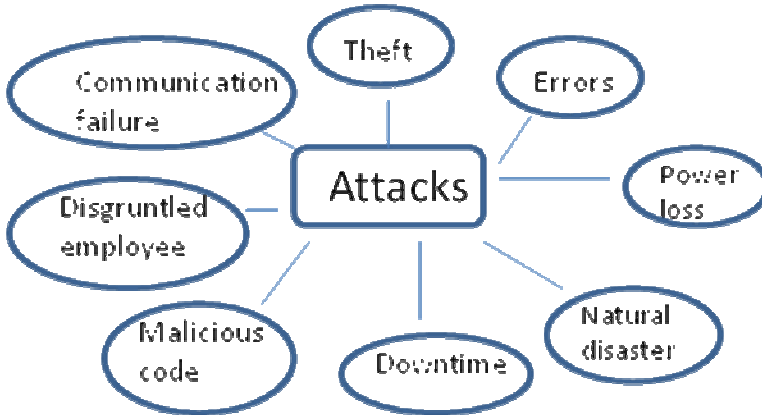


Fig. 5.3.1 : Types of attacks

- (e) **Malicious Code** : Malicious code such as viruses and worms which freely access the unprotected networks may affect organisational and business networks that use these unprotected networks.
- (f) **Abuse of access privileges by employees** : The security policy of the company authorises employees based on their job responsibilities to access and execute select functions in critical applications.
- (g) **Natural disasters** : Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the Information System operations due to damage to Information System facilities.
- (h) **Theft or destruction of computing resources** : Since the computing equipments form the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organisation.
- (i) **Downtime due to technology failure** : Information System facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time. However the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.
- (j) **Fire, etc.** : Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.

### 5.4 THREATS DUE TO CYBER CRIMES

- **Embezzlement** : It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
- **Fraud** : It occurs on account of intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic

means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

- *Theft of proprietary information* : It is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
- *Denial of service* : There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service those results in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
- *Vandalism or sabotage* : It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- *Computer virus* : A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.
- *Other* : Threat includes several other cases such as intrusions, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

5.5 RISK ASSESSMENT

A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess, and then mitigate the risk. Such an analysis entails the development of a clear summary of the current situation and a systematic plan for risk identification, characterisation, and mitigation.

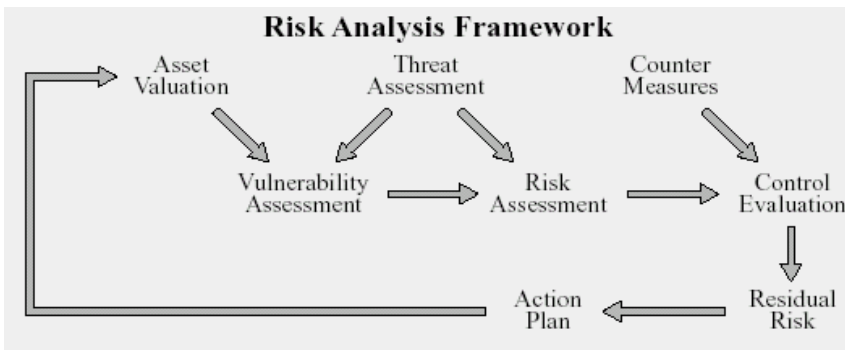


Fig. 5.5.1 : Risk analysis framework

**5.5.1 Risk assessment** is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and

## 5.6 Information Systems Control and Audit

services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritise applications, identify exposures and develop recovery scenarios. The areas to be focussed upon are:

(a) *Prioritisation* : All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organisation, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.

(b) *Identifying critical applications* : Amongst the applications currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.

(c) *Assessing their impact on the organisation* : Business continuity planning should not concentrate only on business disruption but should also take into account other organisational functions which may be affected. The areas to be considered include:

- Legal liabilities.
- Interruptions of customer services.
- Possible losses.
- Likelihood of fraud and recovery procedures.

(d) *Determining recovery time-frame*: Critical recovery time period is the period of time in which business processing must be resumed before the organisation incurs severe losses. This critical time depends upon the nature of operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.

(e) *Assess Insurance coverage* : The information system insurance policy should be a multi-peril policy, designed to provide various types of coverage. Depending on the individual organisation and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:

- (i) **Hardware facilities** : The equipments should be covered adequately. Provision should be made for the replacement of all equipments with a new one by the same vendor.
- (ii) **Software reconstruction** : In addition to the cost of media, programming costs for recreating the software should also be covered.
- (iii) **Extra expenses** : The cost incurred for continuing the operations till the original facility is restored should also be covered.
- (iv) **Business interruption** : This applies mainly to centres performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.

- (v) **Valuable paper and records** : The actual cost of valuable papers and records stored in the insured premises should be covered.
- (vi) **Errors and omissions** : This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.
- (vii) **Fidelity coverage** : This coverage is for acts of employees, more so in the case of financial institutions which use their own computers for providing services to clients.
- (viii) **Media transportation** : The potential loss or damage to media while being transported to off-site storage/premises should be covered.
- (f) *Identification of exposures and implications*: It is not possible to accurately predict as to when and how a disaster would occur. So it is necessary to estimate the probability and frequency of disaster.
- (g) *Development of recovery plan*: The plan should be designed to provide for recovery from total destruction of a site.

## **5.6 RISK MANAGEMENT**

One needs to classify the risks as systematic and unsystematic. **Systematic risks** are unavoidable risks - these are constant across majority of technologies and applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter what technology is used. Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus a systematic risk can be mitigated not by technology but by management process. Hence one would not make any additional payment for technological solution to the problem. To put in other words there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

**Unsystematic risks** are those which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus by making additional investment one can mitigate these unsystematic risks.

The management issue would be whether the additional payment to mitigate the risk is justifiable considering the possibility of loss that may or may not occur. The answer lies in identification of whether the overall risk exposure of the organisation is coming down because of the additional investment.

It may be noted that every business has its inherent risk - the cost of running the business. In case of a technology driven business, the risks induced by technology failure is a part of the

## 5.8 Information Systems Control and Audit

operating risk. The issue is how much of the risk is acceptable and what should be the price that one would pay to reduce a certain part of the risk.

Cardinal to this issue is the ability to measure risk. Until the organisation has developed a process of risk and exposure measurement – it will be difficult to develop a model for risk management. Following this issue will be the risk appetite of the organisation – does it want to be risk aggressive or risk averter. The comparison will have to be made within the framework of the industry for ensuring usage of a consistent and relevant yardstick. For example, the risk appetite of risk aggressive bank may be far lower than that of a risk averse foreign exchange dealer.

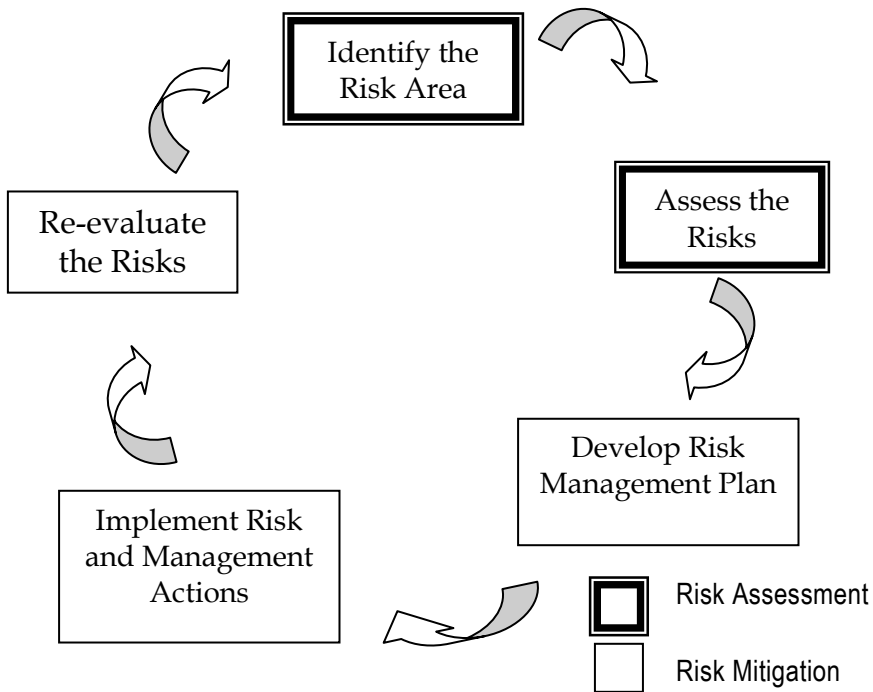
**5.6.1 Risk Management Process :** The broad process of risk management will be as follows:

1. Identify the technology related risks under the scope of operational risks.
2. Assess the identified risks in terms of probability and exposure.
3. Classify the risks as systematic and unsystematic.
4. Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
5. Look out for technological solutions available to mitigate unsystematic risks
6. Identify the contribution of the technology in reducing the overall risk exposure. The analysis should not be restricted to the instant area of application of the technology but should be extended across the entire organisation. This is necessary since many technologies may mitigate a specific type of risk but can introduce other kinds of risks.
7. Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
8. Match the analysis with the management policy on risk appetite and decide on induction of the same.

**5.6.2 The Risk Management Cycle :** It is a process involving the following steps: identifying assets, vulnerabilities and threats; assessing the risks; developing a risk management plan; implementing risk management actions, and re-evaluating the risks.

These steps are categorised into three primary functions –

- (i) Risk Identification,
- (ii) Risk Assessment and
- (iii) Risk Mitigation.



**Fig. 5.6.1 : Risk management cycle**

## 5.7 RISK IDENTIFICATION

The purpose of the risk evaluation is to identify the inherent risk of performing various business functions especially with regard to usage of information technology enabled services. Management and audit resources will be allocated to functions with highest risks. The risk evaluation will directly affect the nature, timing and extent of audit resources allocated.

A risk is anything that could jeopardize the achievement of an objective. For each of the department's objectives, risks should be identified. Asking the following questions helps to identify risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative uses?
- How could someone steal from the department?



## 5.10 Information Systems Control and Audit

- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

It is important that risk identification be comprehensive, Individuals, primarily from the business unit, are the main source of data on all aspects of business operations and assets. For this reason, identifying knowledge individuals to be interviewed and developing interview questions are critical parts of the planning process that require careful attention and close coordination between the business unit manager and senior management. In addition, the risk evaluation of the information technology interface would itself be a part of the audit report on information technology system.

The two primary questions to consider when evaluating the risk inherent in a business function are:

- What is the probability that things can go wrong? (**Probability**) This view will have to be taken strictly on the technical point of view and should not be mixed up with past experience. While deciding on the class to be accorded, one has to focus on the available measures that can prevent such happening.
- What is the cost if what can go wrong does go wrong? (**Exposure**)

Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. Risk is the probability times the exposure.

The purposes of a risk evaluation is to

- (1) identify the probabilities of failures and threats,
- (2) calculate the exposure, i.e., the damage or loss to assets, and
- (3) make control recommendations keeping the cost-benefit analysis in mind.

**5.7.1 Techniques for Risk Evaluation** : Following are some of the techniques that are available to assess and evaluate risks.

- Judgement and intuition
- The Delphi approach

- Scoring
- Quantitative Techniques
- Qualitative Techniques

(a) In many situations the auditors have to use their **judgement and intuition** for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it is required a systematic education and ongoing professional updating.

(b) The **Delphi Technique** was first used by the Rand Corporation for obtaining a consensus opinion. Here a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

(c) In the **Scoring approach** the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

(d) **Quantitative techniques** involve the calculating an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organisation to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavourable events, keeping in mind how often such an event may occur.

(e) **Qualitative techniques** are by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements:

- **Threats** : These are things that can go wrong or that can 'attack' the system. Examples, might include fire or fraud. Threats are ever present for every system.
- **Vulnerabilities** : These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).
- **Controls** : These are the countermeasures for vulnerabilities. There are four types:
  - i) Deterrent controls reduce the likelihood of a deliberate attack
  - ii) Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact

## 5.12 Information Systems Control and Audit

- iii) Corrective controls reduce the effect of an attack
- iv) Detective controls discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model:

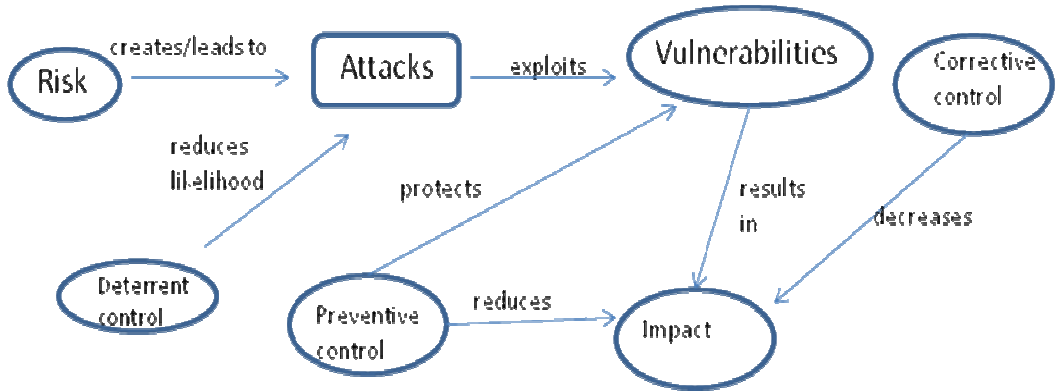


Fig. 5.7.1 : Risk evaluation

## 5.8 RISK RANKING

The planning process should identify and measure the likelihood of all potential risks and the impact on the organisation if threat occurred. To do this, each department should be analysed separately. Although the main computer system may be the single greatest risk, it is not the only important concern. Even in the most automated organisations, some departments may not be computerised or automated at all. In fully automated departments, important records remain outside the system, such as legal files, computer data, software stored on diskettes, or supporting documentation for data entry.

Organisations have to devise their own ranking methods. For example, the impact can be rated as: 0 = No impact or interruption in operations, 1 = Noticeable impact, interruption in operations for up to 8 hours, 2 = Damage to equipment and/or facilities, interruption in operations for 8 - 48 hours, 3 = Major damage to the equipment and/or facilities, interruption in operations for more than 48 hours. All main office and/or computer centre functions must be relocated.

Certain assumptions may be necessary to uniformly apply ratings to each potential threat. Following are typical assumptions that can be used during the risk assessment process:

Although impact ratings could range between 1 and 3 for any facility given a specific set of circumstances, ratings applied should reflect anticipated, likely or expected impact on each area.

Each potential threat should be assumed to be "localised" to the facility being rated.

Although one potential threat could lead to another potential threat (e.g., a hurricane could aet off tornados), no domino effect should be assumed.

If the result of the threat would not warrant movement to an alternate site(s), the impact should be rated no higher than a “2.”

**5.8.2 How to perform Risk Assessment :** The risk assessment should be performed by facility. To measure the potential risks, a weighted point rating system can be used. Each level of probability can be assigned points as follows:

<b>Probability</b>	<b>Points</b>
High	10
Medium	5
Low	1

To obtain a weighted risk rating, probability points should be multiplied by the highest impact rating for each facility. For example, if the probability of hurricanes is high (10 points) and the impact rating to a facility is “3” (indicating that a move to alternate facilities would be required), then the weighted risk factor is 30 (10 x 3). Based on this rating method, threats that pose the greatest risk (e.g., 15 points and above) can be identified.

**5.7.1 Considerations in analysing risk** include:

1. Investigating the frequency of particular types of disasters (often versus seldom).
2. Determining the degree of predictability of the disaster.
3. Analysing speed of onset of the disaster (sudden versus gradual).
4. Determining the amount of forewarning associated with the disaster.
5. Estimating the duration of the disaster.
6. Considering the impact of a disaster based on two scenarios:
  - a. Vital records are destroyed.
  - b. Vital records are not destroyed.
7. Identifying the consequences of a disaster, such as:
  - a. Personnel availability.
  - b. Personal injuries.
  - c. Loss of operating capability.
  - d. Loss of assets.
  - e. Facility damage.
8. Determining the existing and required redundancy levels throughout the organisation to accommodate critical systems and functions, including:
  - a. Hardware.
  - b. Information.
  - c. Communication.

## 5.14 Information Systems Control and Audit

- d. Personnel.
  - e. Services.
9. Estimating potential loss:
- a. Increased operating costs.
  - b. Loss of business opportunities.
  - c. Loss of financial management capability.
  - d. Loss of assets.
  - e. Negative media coverage.
  - f. Loss of stockholder's confidence.
  - g. Loss of goodwill.
  - h. Loss of income.
  - i. Loss of competitive edge.
  - j. Legal actions.
10. Estimating potential losses for each business function based on the financial and service impact and the length of time the organisation can operate without this business function. The impact of a disaster related to a business function depends on the type of outage that occurs and the time that elapses before normal operations can be resumed.
11. Determining the cost of contingency planning.

## 5.9 RISK MITIGATION

Factor or casual analysis can help relate characteristics of an event to the probability and severity of the operational losses. This will enable the organisation to decide whether or not to invest in information system or people (hazards) so events (frequency) or the effect of events (severity) can be minimised.

A causal understanding is essential to take appropriate action to control and manage risks because causality is a basis for both action and prediction. Knowing '*what causes what*' gives an ability to intervene in the environment and implement the necessary controls. Causation is different from correlation, or constant conjunction, in which two things are associated because they change in unison or are found together.

Predictive models (such as loss models) often use correlation as a basis for prediction, but actions based on associations are tentative at best. Simple cause and effect relationships are known from experience, but more complex situations such as those buried in the processes of business operations may not be intuitively obvious from the information at hand. An Information System audit and control professional may be required to establish the cause. Cause models help in the implementation of risk mitigation measures. Cause analysis

identifies events and their impact on losses. In addition to establishing causal relationship, other risk mitigation measures are:

- Self assessment.
- Calculating reserves and capital requirements.
- Creating culture supportive of risk mitigation.
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance).
- Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations).
- Setting up independent operational risk management departments.
- Establishing a disaster recovery plan and backup systems.
- Insurance.
- Outsourcing operations with strict service level agreements so operational risk is transferred.

**5.9.1 Common risk mitigation techniques :** Mitigation and measurement techniques are applied according to the event's losses, and are measured and classified according to the loss type. Some of the common risk mitigation techniques are as under:

1. **Insurance :** An organisation may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy. Under the Advanced Management Approach under Basel II norms (AMA), a bank will be allowed to recognise the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA.

2. **Outsourcing :** The organisation may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organisation remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organisation has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organisation has successfully mitigated the risk.

3. **Service Level Agreements :** Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the

## 5.16 Information Systems Control and Audit

customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organisation for any loss suffered by the customer and user consequent to the technological failure. Thus a bank may state that services at ATM are subject to availability of service there and customers need to recognise that such availability cannot be presumed before claiming the service. The delivery of service is conditional upon the system functionality. Whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

It must be recognised that the organisation should not be so obsessed with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business. The risk mitigation tools available should not eat so much into the economics of business that the organisation may find itself in a position where it is not earning adequate against the efforts and investments made.

## 5.10 RISK AND CONTROLS

Risk is the probability that an event or action will adversely affect the organization. The primary categories of risk are errors, omissions, delay and fraud. In order to achieve goals and objectives, management needs to effectively balance risks and controls. Therefore, control procedures need to be developed so that they decrease risk to a level where management can accept the exposure to that risk. By performing this balancing act "reasonable assurance" can be attained. As it relates to financial and compliance goals, being out of balance can cause the following problems:

<b>Excessive Risks</b>	<b>Excessive Controls</b>
Loss of assets, donor or grants	Increased bureaucracy
Poor business decisions	Reduced productivity
Non-compliance	Increased complexity
Increased regulations	Increased cycle time
Public scandals	Increase of no-value activities

In order to achieve a balance between risk and controls, internal controls should be proactive, value-added, cost-effective and address exposure to risk.

## 5.11 RISK ANALYSIS AND ASSESSMENT FORM

A form may be used to list out severity of different elements posing risk. This will help in clearly assessing the overall organisational exposure and give an idea how to mitigate the risk. A typical form is given below:

<b>Physical Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
1. Are acceptable standards, policies and guidelines about physical security distributed to employees and are they adequate and up-to-date? (a) Yes, fully adequate and up-to-date. (b) Yes, reasonably adequate but needs improvement. (c) No, not available.	 1.0 2.0 3.0	 4.0 4.0 4.0	
2. Are physical access controls (like identity badges, security cards etc.) available? Are they fully adequate and effective? (a) Yes, fully adequate and effective. (b) Yes, reasonably adequate and effective. (c) Totally ineffective.	 1.0 2.0 4.0	 5.0 5.0 5.0	
3. Status of environmental controls (air conditioners, smoke detectors. etc.) (a) Always up to the standards. (b) Not always up to the standards. (c) Not Monitored.	 1.0 2.0 4.0	 4.0 4.0 4.0	
4. Are good housekeeping procedures distributed to employees and are they kept up-to-date? (a) Yes, strictly followed and kept up-to-date. (b) Yes, mostly followed and reasonably up-to-date. (c) No procedure available.	 1.0 2.0 3.0	 4.0 4.0 4.0	
5. Have physical security aspects been audited? (a) Yes, less than a year ago. (b) Yes, more than a year ago. (c) Never.	 1.0 2.0 4.0	 4.0 4.0 4.0	



## 5.18 Information Systems Control and Audit

<b>Personnel Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
6. Are acceptable standards, policies and guidelines about personnel security distributed to employees and are they adequate and up-to-date? (a) Yes, adequate and up-to-date (b) Yes, reasonably adequate but needs improvement. (c) Not available.	 1.0  2.0  3.0	 4.0  4.0  4.0	
7. Are employment verifications performed prior to hiring? (a) Yes. (b) Yes, sometimes. (c) Never.	 1.0  2.0  4.0	 5.0  5.0  5.0	
8. Are employees required to sign conflict of interest or code of conduct statements at the time of hiring? (a) Yes, always. (b) Yes, sometimes. (c) Never.	 1.0  2.0  4.0	 3.0  3.0  3.0	
9. Are employees required to sign non-disclosure statements with respect to passwords and other important information at the time of hiring? (a) Yes, always. (b) Yes, sometimes. (c) Never.	 1.0  2.0  4.0	 6.0  6.0  6.0	
10. Are all employees often reminded about the importance of computer security? (a) Yes, always. (b) Yes, regularly. (c) Never.	 1.0  2.0  3.0	 3.0  3.0  3.0	

11. Has personnel security aspects been audited?			
(a) Yes, less than a year ago.	1.0	5.0	
(b) Yes, more than a year ago.	2.0	5.0	
(c) No.	4.0	5.0	

<b>Data Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
12. Are acceptable standards, policies and guidelines about data security distributed to all employees and are they adequate and up-to-date?  (a) Yes, fully adequate and up-to-date. (b) Yes, reasonably adequate but needs improvement. (c) Never, not available.	1.0  2.0 3.0	4.0  4.0 4.0	
13. Are the security aspects of the operating systems adequate and used effectively to control access to data files?  (a) Yes, used effectively. (b) Not used effectively. (c) Security features not adequate.	1.0 2.0 4.0	6.0 6.0 6.0	
14. Are access rules and privileges for gathering data files always in line with employees' job duties?  (a) Yes, always. (b) Mostly. (c) No.	1.0 2.0 4.0	6.0 6.0 6.0	

## 5.20 Information Systems Control and Audit

<p>15. Are data/system owners established for all important data files?</p> <p>(a) Yes, always.</p> <p>(b) Yes, mostly.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>6.0</p> <p>6.0</p> <p>6.0</p>	
<p>16. Are data/system custodians established for all critical and sensitive data files?</p> <p>(a) Yes, always.</p> <p>(b) Yes, mostly.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>5.0</p> <p>5.0</p> <p>5.0</p>	
<p>17. Are data/system users established for all important data files?</p> <p>(a) Yes, always.</p> <p>(b) Yes, but not always.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>4.0</p> <p>4.0</p> <p>4.0</p>	
<p>18. Do data/system users need permission from data system owners before making changes to all critical and sensitive data files and programs?</p> <p>(a) Yes.</p> <p>(b) Yes, permission is delegated.</p> <p>(c) No permission needed.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>4.0</p> <p>4.0</p> <p>4.0</p>	
<p>19. Have data security aspects been audited?</p> <p>(a) Yes, less than a year ago.</p> <p>(b) Yes, more than a year ago.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>4.0</p> <p>4.0</p> <p>4.0</p>	

<b>System Software Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
20. Are updated and acceptable standards, policies and guidelines about system software security distributed to concerned employees and are they adequate? (a) Yes. (b) Yes, reasonably adequate but needs improvement. (c) Not available.	1.0 2.0 3.0	4.0 4.0 4.0	
21. Are proper files for monitoring security violation listed and reviewed? (a) Yes, listed and reviewed. (b) Listed but not reviewed. (c) Neither listed nor reviewed.	1.0 2.0 3.0	4.0 4.0 4.0	
22. Are powerful utility programs prescribed and controlled properly? (a) Yes. (b) Normally yes. (c) Never.	1.0 2.0 3.0	4.0 4.0 4.0	
23. Have systems software security aspects being audited? (a) Yes, less than a year ago. (b) Yes, more than a year ago. (c) Never.	1.0 2.0 3.0	4.0 4.0 4.0	

## 5.22 Information Systems Control and Audit

<b>Application Software Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
24. Are updated and acceptable standards, policies and guidelines about application software security distributed to concerned employees and are they adequate? (a) Yes, fully adequate and up-to-date. (b) Yes, reasonably adequate but needs improvement. (c) No, not available.	1.0 2.0 3.0	4.0 4.0 4.0	
25. Are computer security requirements made explicit during new system development and maintenance work (a) Yes. (b) Yes, but not always. (c) Never.	1.0 2.0 4.0	6.0 6.0 6.0	
26. Do functional users and auditors participate in system development and maintenance? (a) Yes, users and auditors participate. (b) Yes, sometimes the users but not the auditors. (c) No users or auditors participate.	1.0 2.0 4.0	4.0 4.0 4.0	
27. Is there any standard system development and maintenance methodology and is it followed? (a) Yes. (b) Not always. (c) No methodology exists.	1.0 2.0 4.0	5.0 5.0 5.0	
28. Are software packages purchased and used? (a) Used with major changes. (b) With minor changes. (c) With major changes combined with in-house development.	1.0 2.0 4.0	5.0 5.0 5.0	

29. Do end-users develop and maintain systems using fourth generation languages? (a) No. (b) Yes, with the help of system development personnel. (c) Yes, without the help of system development personnel.	1.0  2.0  4.0	7.0  7.0  7.0	
30. Have the application software aspects been audited? (a) Yes, less than a year ago. (b) Yes, more than a year ago. (c) Never.	1.0  2.0  4.0	4.0  4.0  4.0	

<b>Computer Operations Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
31. Are updated and acceptable standards, policies and guidelines about computer operation security distributed to concerned employees and are they adequate? (a) Yes, fully adequate and up-to-date. (b) Yes, reasonably adequate but needs improvement. (c) No, not available.	1.0  2.0  3.0	4.0  4.0  4.0	
32. Are access control systems built into the operating system adequate, and are they used effectively to control computer operation staff's access to application and system software and data files? (a) Yes, used effectively. (b) Yes, not used effectively. (c) No, not enabled.	1.0  2.0  4.0	6.0  6.0  6.0	

## 5.24 Information Systems Control and Audit

<p>33. Are access rules and privileges established for computer operations staff accessing applications and software programs and data files always in line with the employees' job duties?</p> <p>(a) Yes, always.</p> <p>(b) Generally.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>6.0</p> <p>6.0</p> <p>6.0</p>	
<p>34. Are back-up procedures for data and software adequate and well documented and are they being followed?</p> <p>(a) Yes, being followed very rigidly.</p> <p>(b) Procedures are not followed regularly.</p> <p>(c) No such procedures.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>4.0</p> <p>4.0</p> <p>4.0</p>	
<p>35. Have fire controls and other emergency tests been conducted?</p> <p>(a) Yes, less than six months ago.</p> <p>(b) Yes, more than two years ago.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>3.0</p>	<p>4.0</p> <p>4.0</p> <p>4.0</p>	
<p>36. Have computer operations security aspects been audited?</p> <p>(a) Yes, less than a year ago.</p> <p>(b) Yes, more than a year ago.</p> <p>(c) Never.</p>	<p>1.0</p> <p>2.0</p> <p>4.0</p>	<p>5.0</p> <p>5.0</p> <p>5.0</p>	

<b>Telecommunications Security</b>			
<b>Criterion</b>	<b>Risk Criterion (A)</b>	<b>Value Weight (B)</b>	<b>Total Risk (A×B)</b>
37. Are updated and acceptable standards, policies and guidelines about computer operation security distributed to concerned employees and are they adequate? (a) Yes, fully adequate and up-to-date. (b) Yes, reasonably adequate but needs improvement. (c) No, not available.	 1.0 2.0 3.0	 4.0 4.0 4.0	
38. Are there any special features to effectively control access to the telecommunication programs and data files and are they being used effectively? (a) Yes, used effectively. (d) Yes, but not used effectively. (e) Not in place.	 1.0 2.0 4.0	 6.0 6.0 6.0	
39. Are the access rules and privileges which have been established, in line with the employees' job duties? (a) Yes, always. (b) Mostly. (c) Never.	 1.0 2.0 4.0	 6.0 6.0 6.0	
40. Are terminal IDs part of the user identification and authentication process? (a) Yes always. (f) Yes not always. (g) Never.	 1.0 2.0 3.0	 6.0 6.0 6.0	



## 5.26 Information Systems Control and Audit

41. Are security related controls over program, data and message transmission activities adequate and effective?			
(a) Yes, fully adequate and effective.	1.0	8.0	
(b) Yes, fairly accurate but needs improvement.	2.0	8.0	
(c) Not adequate or effective.	3.0	8.0	
42. Have telecommunications security aspects been audited?			
(a) Yes, less than a year ago.	1.0	5.0	
(b) Yes, more than a year ago.	2.0	5.0	
(c) Never.	4.0	5.0	

**Action Plan :** The risk assessment matrix can be created based on the above parameters and the total risk can be rated as high, medium or low, depending on how likely the activity is to cause harm and how serious that harm might be. Action can be taken upon all the questions, where the answer is high. Action can be immediately implemented based on the cost of implementation and can be categorized as now, this year or longer term.

### Self - Examination Questions

1. Define risk, threat, vulnerability and exposure?
2. Differentiate between threat and vulnerability?
3. Describe the risk analysis framework?
4. What is residual risk? What is its importance in an organisation?
5. Describe various threats in the computerised environment?
6. What are cyber crimes?
7. What is risk assessment? How is it performed?
8. How does one assess insurance coverage?
9. What is systematic risk and unsystematic risk?
10. Describe the process of risk management?
11. How does one identify risk? How is the risk measured?
12. Describe how assessment and evaluation of risks is done?
13. Describe the risk ranking procedure?
14. How is risk mitigated in an organisation?
15. How are physical security risks determined?
16. What are the various areas that an IS auditor looks into while determining risk?

# BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

---

## LEARNING OBJECTIVES :

- To develop business continuity plan

## 6.0 INTRODUCTION

Business continuity focuses on maintaining the operations of an organisation, especially the IT infrastructure in face of a threat that has materialised. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operation using a prioritised resumption list.

## 6.1 BUSINESS CONTINUITY PLANNING

Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

Planning is an activity to be performed before the disaster occurs or it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience. In fact, these consequences may be more severe because of the lost time that results from inadequate planning. After such an event, it is typical for senior management to become concerned with all aspects of the occurrence, including the measures taken to limit losses. Their concerns range from the initiating event and contributing factors, to the response plans, effective contingency planning and disaster recovery coordination. Rather than delegating disaster avoidance to the facilities or building security organisations, it is preferable for a firm's disaster recovery planner(s) to understand fully the risks to operations and the measures that can minimise the probabilities and consequences, and to formulate their disaster recovery plan accordingly.

## 6.2 Information Systems Control and Audit

When a risk manifests itself through disruptive events, the business continuity plan is a guiding document that allows the management team to continue operations. It is a plan for running the business under stressful and time compressed situations. The plan lays out steps to be initiated on occurrence of a disaster, combating it and returning to normal operations including the quantification of the resources needed to support the operational commitments.

Business continuity covers the following areas:

- *Business resumption planning* : The operation's piece of business continuity planning.
- *Disaster recovery planning* : The technological aspect of business continuity planning, the advance planning and preparation necessary to minimise losses and ensure continuity of critical business functions of the organisation in the event of disaster.
- *Crisis management* : The overall co-ordination of an organisation's response to a crisis in an effective timely manner, with the goal of avoiding or minimising damage to the organisation's profitability, reputation or ability to operate.

The business continuity life cycle is broken down into four broad and sequential sections:

- risk assessment,
- determination of recovery alternatives,
- recovery plan implementation, and
- recovery plan validation.

Within each of these lifecycle sections, the applicable resource sets are manipulated to provide the organisation with the best mix or critical resource quantities at optimum costs with minimum tangible and intangible losses. These resource sets can be broken down into the following components: information, technology, telecommunication, process, people, and facilities.

### 6.1.1 Objectives and Goals of Business Continuity Planning

The primary objective of a business continuity plan is to minimize loss by minimizing the cost associated with disruptions and enable an organisation to survive a disaster and to re-establish normal business operations. In order to survive, the organisation must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- (i) Provide for the safety and well-being of people on the premises at the time of disaster;
- (ii) Continue critical business operations;
- (iii) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
- (iv) Minimise immediate damage and losses;
- (v) Establish management succession and emergency powers;

- (vi) Facilitate effective co-ordination of recovery tasks;
- (vii) Reduce the complexity of the recovery effort;
- (viii) Identify critical lines of business and supporting functions;

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;
- (ii) minimise the duration of a serious disruption to business operations;
- (iii) facilitate effective co-ordination of recovery tasks; and
- (iv) reduce the complexity of the recovery effort

## **6.2 DEVELOPING A BUSINESS CONTINUITY PLAN**

The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The **methodology** emphasises on the following:

- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- (ii) Obtaining commitment from appropriate management to support and participate in the effort;
- (iii) Defining recovery requirements from the perspective of business functions;
- (iv) Documenting the impact of an extended loss to operations and key business functions;
- (v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
- (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
- (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
- (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

The **eight phases** are described in detail in the following paragraphs:

- (i) Pre-Planning Activities (Business continuity plan Initiation)
- (ii) Vulnerability Assessment and General Definition of Requirements
- (iii) Business Impact Analysis
- (iv) Detailed Definition of Requirements
- (v) Plan Development
- (vi) Testing Program

## 6.4 Information Systems Control and Audit

(vii) Maintenance Program

(viii) Initial Plan Testing and Plan Implementation

**6.2.1 Pre-Planning Activity :** In phase 1, we obtain an understanding of the existing and projected systems environment of the organisation. This enables us to refine the scope of business continuity planning and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan.

During this phase a Steering Committee should be established that should undertake an overall responsibility for providing direction and guidance to the business continuity planning team. The committee should also make all decisions related to the recovery planning effort. The Business Continuity Manager should work with the Steering Committee in finalising the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis.

Two other key deliverables of this phase are: the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

**6.2.2 Vulnerability Assessment and definition of Requirement :** Security and control within an organisation is a continuing concern. It is preferable, from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimising the impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence. This phase will include the following tasks:

- (i) A thorough Security Assessment of the system and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
- (ii) The Security Assessment will enable the business continuity team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- (iii) Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- (iv) Define the scope of the planning effort.
- (v) Analyse, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
- (vi) Develop a Plan Framework.
- (vii) Assemble business continuity team and conduct awareness sessions.

**6.2.3 Business Impact Analysis :** Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

The business impact analysis is intended to help understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

A number of tasks are to be undertaken in this phase as enumerated under:

- (i) Identify organisational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimise potential threats that may lead to a disaster.
- (ii) Identify critical business processes.
- (iii) Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
- (iv) Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- (v) Determine the maximum allowable downtime for each business process.
- (vi) Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- (vii) Determine the impact to the organisation in the event of a disaster, e.g. financial reputation, etc.

There are a number of ways to obtain this information:

- Questionnaires,
- Workshops,
- Interviews,
- Examination of documents

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframe in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

**6.2.4 Detailed Definition of requirements :** During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analysing alternative recovery strategies. The profile is developed by identifying resources required to support

## 6.6 Information Systems Control and Audit

critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipments, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

**6.2.5 Plan Development :** The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies.

The recovery strategies may be two-tiered:

- Business - Logistics, accounting, human resources, etc.
- Technical - Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks)

In this phase, recovery plans components are defined and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of recovery teams, their roles and responsibilities. Recovery standards are also developed during this phase. The organisation's recovery strategy needs to be developed for the recovery of the core business processes. In the event of a disaster, it is survival and not business as usual.

**6.2.6 Testing the Plan :** The Testing/Exercising program is developed during this phase. Testing/Exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established. Unless the plan is tested on a regular basis, there is no assurance that in the event the plan is activated, the organisation will survive a disaster.

The objectives of performing BCP tests are to ensure that:

- The recovery procedures are complete and workable.
- The competence of personnel in their performance of recovery procedures can be evaluated.
- The resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- The manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- The success or failure of the business continuity training program is monitored.

**6.2.7 Maintenance Program :** Maintenance of the plans is critical to the success of actual recovery. The plans must reflect changes to the environment. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas

where change management does not exist, change management procedures will be recommended and implemented. The tasks undertaken in this phase are:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the organisation
- Identify the BCP maintenance triggers to ensure that any organisational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date.
- Determine the maintenance regime to ensure the plan remains up-to-date.
- Determine the maintenance processes to update the plan.
- Implement version control procedures to ensure that the plan is maintained up-to-date.

**6.2.8 Testing and Implementation** : Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:

- Defining the test purpose/approach;
- Identifying test teams;
- Structuring the test;
- Conducting the test;
- Analysing test results; and
- Modifying the plans as appropriate.

The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organisation. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

### 6.3 TYPES OF PLANS

There are various kinds of plans that need to be designed. They include the following:

**6.3.1 Emergency Plan** : The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked for example, major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an organisation undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated. First, the plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on. Second, the plan



## 6.8 Information Systems Control and Audit

must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

**6.3.2 Back-up Plan :** The backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system. For some resources, the procedures specified in the backup plan might be straightforward. For example, microcomputer users might be admonished to make backup copies of critical files and store them off site. In other cases, the procedures specified in the backup plan could be complex and somewhat uncertain. For example, it might be difficult to specify; exactly how an organisation's mainframe facility will be recovered in the event of a fire.

The backup plan needs continuous updating as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organisation, the plan must be modified accordingly. Indeed, it is prudent to have more than one person knowledgeable in a backup task in case someone is injured when a disaster occurs. Similarly, lists of hardware and software must be updated to reflect acquisitions and disposals.

Perhaps the most difficult part in preparing a backup plan is to ensure that all critical resources are backed up. The following resources must be considered;

- (i) Personnel : Training and rotation of duties among information system staff so enable them to replace others when required. Arrangements with another company for provision of staff.
- (ii) Hardware : Arrangements with another company for provision of hardware.
- (iii) Facilities : Arrangements with another company for provision of facilities.
- (iv) Documentation : Inventory of documentation stored securely on-site and off-site.
- (v) Supplies : Inventory of critical supplies stored securely on-site and off-site with a list of vendors who provide all supplies.
- (vi) Data / information : Inventory of files stored securely on site and off site.
- (vii) Applications software : Inventory of application software stored on site and off site.
- (viii) System software : Inventory of system software stored securely on site and off site.

**6.3.3 Recovery Plan :** The backup plan is intended to restore operations quickly so the information system function can continue to service an organisation, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plans should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and

provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organisation, new members must be appointed immediately and briefed about their responsibilities.

#### **6.4 TEST PLAN**

The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organisation and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, a phased approach can be adopted. First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs. Next, a disaster can be simulated at a convenient time-for example, during a slow period in the day. Anyone who will be affected by the test (e.g., personnel and customers) also might be given prior notice of the test so they are prepared. Finally, disasters could be simulated without warning at any time. These are the acid tests of the organisation's ability to recover from a catastrophe.

#### **6.5 THREATS AND RISK MANAGEMENT**

To minimise threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, it can be useful to evaluate potential threats to computer systems. Discussed hereunder are various threats, risks and exposures to computer systems and suggested control measures.

*Lack of integrity* : Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails , audit of adequacy of data integrity.

*Lack of confidentiality* : Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure

## 6.10 Information Systems Control and Audit

storage of important media and data files, installation of audit trails , audit of confidentiality of data.

*Lack of system availability* : Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programs and training of employees, installation of audit trails , audit of adequacy of availability safeguards.

*Unauthorised users attempt to gain access to the system and system resources* : Control measures to stop unauthorised users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Data transmitted over a public or shared network may be intercepted by an unauthorised user, security breaches may occur due to improper use or bypass of available security features - strong identification and authentication mechanisms such as biometrics, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.

Hostile software e.g. virus, worm, Trojan horses, etc.- Establishment of policies regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.

*Disgruntled employees* : Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of a disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees,, application of motivation theories, job enrichment and job rotation.

*Hackers and computer crimes* – Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorised changes to programs, installation of logging features and audit trails for sensitive information.

*Terrorism and industrial espionage* : Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage,

use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.

**6.5.1 Minimising risks in organisation’s infrastructure :** A key element in minimising the threat of a disaster occurring in an organisation is “hardening” the organisation’s infrastructure from potential sources of risk. Many organisations fail to identify the potential threats from single points of failure or hazards from organisations environment e.g. buildings, plant, equipment and staff.

The organisation’s infrastructure is at risk from a large number of potential threats and hazards as depicted in the table below:

<b>Human Errors</b>	<b>Equipment Failure</b>	<b>Utility Outage</b>	<b>Supply Chain</b>	<b>Fire</b>	<b>Strike</b>
Outsourcing	Technology	Organisational infrastructure	Outage	Third Parties	Vendors
Environmental conditions	Internet	Water Leaks	Viruses	Terrorism	Hackers

**6.5.2 Single Points of Failure Analysis :** The objective is to identify any single point of failure within the organisation’s infrastructure, in particular the information technology infrastructure. Single point’s of failure have increased significantly due to the continued growth in the complexity in the organisation’s IS environment. This growth has occurred due to changes in technology and customer’s demands for new channels in the delivery service and/or products, for example E-Commerce. Organisations have failed to respond to increase in the exposure from single point of failure by not implementing risk mitigation strategies.

One common area of risk from single point of failure is the telecommunication infrastructure. Because of its transparency, this potential risk is often overlooked. While the resiliency of network and the mean average failures of communication devices, e.g. routers, have improved, it is still a single point of failure in an organisation that may lead to disaster being declared. To ensure single point failures are identified within the organisations IS architecture at the earliest possible stage, it is essential, as part of any project, a technology risk assessment be performed.

The objectives of risk assessment are to:

- Identify Information Technology risks
- Determine the level of risk
- Identify the risk factors
- Develop risk mitigation strategies

The benefits of performing a technology risk assessment are:

- A business-driven process to identify, quantify and manage risks while detailing future suggestions for improvement in technical delivery.

## 6.12 Information Systems Control and Audit

- A framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle.
- Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level.
- Implementation of strict disciplines for active risk management during the project lifecycle.

The technology risk assessment needs to be a mandatory requirement for all projects to ensure that proactive management of risks occurs and that no single point of failure are inadvertently built into the overall architecture.

## 6.6 SOFTWARE AND DATA BACK-UP TECHNIQUES

**6.6.1 Types of Back-ups :** When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.

- Full Backup :* A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.
- Incremental Backup :* An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

Normally, incremental backup are very difficult to restore. You will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

- Differential Backup :* A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

- Mirror back-up :* A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

## 6.7 ALTERNATE PROCESSING FACILITY ARRANGEMENTS

Security administrators should consider the following backup options:

- (i) *Cold site* : If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- (ii) *Hot site* : If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.
- (iii) *Warm site* : A warm site provides an intermediate level of backup. It has all cold-site facilities plus hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.
- (iv) *Reciprocal agreement* : Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

- (1) how soon the site will be made available subsequent to a disaster,
- (2) the number of organisations that will be allowed to use the site concurrently in the event of a disaster,
- (3) the priority to be given to concurrent users of the site in the event of a common disaster,
- (4) the period during which the site can be used,
- (5) the conditions under which the site can be used.
- (6) the facilities and services the site provider agrees to make available, and
- (7) what controls will be in place and working at the off-site facility.

These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

## 6.14 Information Systems Control and Audit

### 6.8 BACK-UP REDUNDANCY

*Multiple Backup Media* : For data of high importance it is absolutely unacceptable to have a situation of data loss. Therefore, single point of failure such as failed backup disk that destroys the entire backup history should be eliminated.

*Off-Site Backup* : off-Site backup is done to keep *at least one copy of your redundant backups in an alternative location. In case the size of the backup is considerably big (>10GB), cost of high-speed link, security issues, and backup time will rule out the idea of backing up through high-speed links.* A practical solution would be to take a backup into a removable backup disk, which will be shuttled out of your site into a secure location.

*Where to Keep the Backups* : If removable-media backups are kept next to the computer, a fire or other disaster will probably destroy both. A secure off-site location is best. Consider keeping one backup disk in the office and the other one or two off-site.

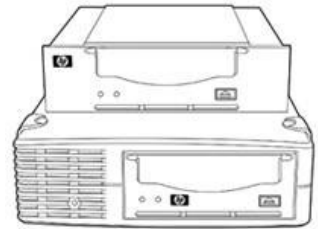
*Media - Rotation – Tactics* : Once in a while, rotate the active backup media with one of the offsite stored media. This will update the offsite media with the latest data changes. To reduce data loss in case of a major disaster, it is recommended to daily switch the active backup media with one of the stored.

**6.8.1 Types of Back-up Media** : The most common types of backup media available on the market today include :

- (i) *Floppy Diskettes* : Floppy diskettes were available with most desktop computers earlier and they were the cheapest back-up solution. However, these drives have been discontinued due to low storage capacity and are slow.
- (ii) *DVD Disks* : DVD (also known as "Digital Versatile Disc" or "Digital Video Disc") is a popular optical disc storage media format. Its main uses are video and data storage. Most DVDs are of the same dimensions as compact discs (CDs) but store more than six times as much data.
- (iii) *Tape Drives* : Tape drives are the most common backup media around due to their low cost. The average capacity of a tape drive is 4 to 10 GB. The drawbacks are that they are relatively slow when compared with other media, and can tend to be unreliable. Magnetic tape cartridges are used to store the data, which leaves it susceptible to loss of information over time or through breaking/stretching the tape.
- (iv) *Disk Drives* : Disk drives are very fast compared to tape drives. The disk drive rotates at a very fast pace and has one or more heads that read and write data. If an organisation is looking for a fast method of backup and recovery then disk drives is the way to go – the difference in speed between a tape drive and a disk drive is hours compared to minutes, respectively.

(v) *Removable Disks* : Using a removable disk such as a ZIP/JAZ drive is becoming increasingly popular for the backup of single systems. They are quite fast, not that expensive and easy to install and carry around.

(vi) *DAT (Digital Audio Tape) drives* : DAT drives are similar to a standard tape drive but they have a larger capacity. They are fast becoming popular and are slowly replacing the tape drive. The tapes come in DLT (Digital Linear Tape), SDLT (Super Digital Linear Tape), LTO (Linear Tape Open) and AIT (Advanced Intelligent Tape) format, offering up to 260GB of compressed data. The image below shows a typical HP DAT drive.



**Fig. 6.8.1 : Digital audio tape drives**

(vii) *Optical Jukeboxes* : Optical Jukeboxes use magnetic optical disks rather than tapes to offer a high capacity backup solution. They are extremely expensive but offer excellent amounts of secure storage space, ranging from 5 to 20 terabytes. A jukebox is a tower that automatically loads internally stored disks when needed for backup and recovery – just add a certain amount of CDs or DVDs when you first set it up, maintenance is relatively low. The image below shows a standard tower optical jukebox:



**Fig. 6.8.2 : Optical Jukebox**

(viii) *Autoloader Tape Systems* : Autoloader tape systems use a magazine of tapes to create extended backup volumes. They have a built-in capability of automatically loading or unloading tapes. Autoloaders use DAT tapes that come in DLT, LTO and AIT format. By implementing a type library system with multiple drives you can improve the speed of a backup to hundreds of Gigabytes per hour. Below is an image showing a typical Autoloader tape system :



**Fig. 6.8.3 : Autoloader tape system**

(ix) *USB Flash Drive* : USB flash Drive Plugs into the USB Port on laptop, PC, or Workstation. The USB flash Drive is available in various sizes. This Drive takes advantage of USB Plug and Play capability Saves and backs-up Documents and any File presentations which provides an excellent solution for mobile and storing data as a reliable Data retention media.

(x) *Zip Drive* : Zip Drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. Zip drives and disks come in various sizes. Zip drive comes with a software utility that provides the facility of copy the entire contents of hard drive to one or more Zip disks. The Zip drive can be purchased in either a Parallel or a Small Computer System Interface (SCSI) version. In the parallel version, a printer can be chained off the Zip drive so that both can be plugged into your computer's parallel port.



## 6.16 Information Systems Control and Audit

In addition to data backup, following are the suggestions for its additional uses :

- Archiving old e-mail or other files that are not in use any more but might be accessed someday.
- Storing unusually large files, such as graphic images that you need infrequently  
Exchanging large files with someone
- Putting your system on another computer, perhaps a portable computer
- Keeping certain files separate from files on your hard disk (for example, personal finance files)

There are a substantial amount of tools and media available for backing up data. When making your selection, there are five fundamental factors that you should base your decision on.

- Speed : How fast can you backup and restore data using this media?
- Reliability : Can you risk purchasing media that's known to have reduced reliability to save on costs?
- Capacity : Is the media big enough for your backup load?
- Extensibility : If the amount of data grows, will the media support this demand?
- Cost : Does the solution you want fit into your budget?

### 6.8.2 Backup Tips

- (i) Draw up a simple (easy to understand) plan of who will do what in the case of an emergency.
- (ii) Be organized! Keep a record of what was backed up, when it was backed up and which backup media contains what data. You can also make a calendar of which type of backup is due on a certain date.
- (iii) Utilize the Volume Shadow Copy (VSS) service in Windows Server 2003. This feature allows you to create point-in-time copies of data so that they can be restored and reverted to at any given time. For instance, if a user created a Word document yesterday and decides that he wants to revert to it today, he can do so using VSS.
- (iv) Select the option to verify backup, the process will take a little longer but it's definitely worth the wait.
- (v) Create a reference point where you know everything is working properly. It will be quicker to restore the changes from tape.
- (vi) Select the option to restrict restoring data to owner or administrator and also set the Domain Group Policy to restrict the Restore privilege to Administrators only. This will help to reduce the risk of someone being able to restore data should the media be stolen.
- (vii) Create a step-by-step guideline (a flowchart for example) clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.

## **6.9 DISASTER RECOVERY PROCEDURAL PLAN**

The disaster recovery and planning document may include the following areas:

- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organisation, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.
- Primary computer centre hardware, software, peripheral equipment and software configuration.

## 6.18 Information Systems Control and Audit

- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

## 6.10 INSURANCE

The purpose of insurance is to spread the economic cost and the risk of loss from an individual or business to a large number of people. This is accomplished through the use of an insurance policy. Policies are contracts that obligate the insurer to indemnify the policyholder or some third party from specific risks in return for the payment of a premium.

Adequate insurance coverage is a key consideration when developing a business recovery plan and performing a risk analysis. Most insurance agencies specialising in business interruption coverage can provide the organisation with an estimate of anticipated business interruption costs. Most business interruption coverage includes lost revenues following a disaster. Extra expense coverage includes all additional expenses until normal operations can be resumed. Policies usually can be obtained to cover the following resources:

- *Equipment* : Covers repair or acquisition of hardware. It varies depending on whether the equipment is purchased or leased.
- *Facilities* : Covers items such as reconstruction of a computer room, raised floors, special furniture.
- *Storage media* : Covers the replacement of the storage media plus their contents – data files, programs, documentation.
- *Business interruption* : Covers loss in business income because an organisation is unable to trade.
- *Extra expenses* : Covers additional costs incurred because an organisation is not operating from its normal facilities.
- *Valuable papers* : Covers source documents, pre-printed reports, and records documentation, and other valuable papers.
- *Accounts receivable* : Covers cash-flow problems that arise because an organisation cannot collect its accounts receivable promptly.
- *Media transportation* : Covers damage to media in transit.
- *Malpractice, errors*: Covers claims against an organisation by its customers, and omission e.g., claims and omission made by the clients of an outsourcing vendor or service bureau.

**6.10.1 Kinds of Insurance :** To understand the role insurance might play in establishing information security standards, it is useful to review the types of insurance that might be utilized. Insurance is generally divided into two general classes based upon whether the insured is the injured party. Lawyers call these two divisions first-party and third-party insurance. First-party insurance identifies claims by the policyholder against their own insurance. Third-party insurance is designed to protect against claims made against the policyholder and his insurer for wrongs committed by the policyholder. The most common form of first-party insurance is property damage, while the most common form of third-party insurance is liability.

**(a) First-party Insurances - Property Damages :** Perhaps the oldest insurance in the world is that associated with damage to property. It is designed to protect the insured against the loss or destruction of property. It is offered by the majority of all insurance firms in the world and uses time-tested forms, the industry term for a standard insurance contract accepted industry-wide. This form often defines loss as “physical injury to or destruction of tangible property” or the “loss of use of tangible property which has not been physically injured or destroyed.” Such policies are also known as all risks, defined risk, or casualty insurance.

**(b) First-party Insurances - Business Interruption :** If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. One potential cause for the inability to deliver might be the loss of information system, data or communications. Some in business and the insurance industry have attempted to mitigate this by including information technology in business recovery/disaster plans. As a result, there has emerged a robust industry in hot sites for companies to occupy in case of fire, flood, earthquake or other natural disaster. Disaster recovery has become a necessity in the physical world. While the role of disaster recovery is well understood in business, the insurance industry was slow to accept the indemnity role relative to insuring data in a business interruption liability insurance context. Insurers are generally aggressive in limiting their own liability and have, in a number of instances, argued that a complete cessation of business is necessary to claim damage.

**(c) Third-party Insurance – General Liability :** Third party insurance is designed to protect the insured from claims of wrongs committed upon others. It is in parts based on the legal theory of torts. Torts are civil wrongs which generally fit into three categories – intentional, negligent and strict liability. Intentional torts are generally excluded from liability insurance policies because they are foreseeable and avoidable by the insured. Strict liability torts, such as product liability issues, are generally covered under specialised liability insurance. Generally liability policies include comprehensive, umbrella and excess liability policies. Insured parties are exposed to the risk of liability whenever they violate some duty imposed on, or expected of, parties’ relative to each other or society in general. In the cyber environment this can take many forms. If the insured’s computer damages another party’s computer, data connectivity, then the insured may be held liable. A company might be held liable if the computer system was used in connection with a denial-of-service attack. The insured may be also held liable for failing to protect adequately the privacy interests of parties who have been entrusted information to the care of the insured.

## 6.20 Information Systems Control and Audit

(iv) **Third-party Insurance - Directors and Officers** : Errors and Omissions (E&O) insurance is protection from liability arising from a failure to meet the appropriate standard of care for a given profession. Two common forms of E & O insurance are directors and officers, and professional liability. Directors and officers insurance is designed to protect officers of companies, as individuals, from liability arising from any wrongful acts committed in the course of their duties as officers. These policies usually are written to compensate the officer's company for any losses payable by the company for the acts of its officer's.

## 6.11 TESTING METHODOLOGY AND CHECKLIST

With good planning a great deal of disaster recovery testing can be accomplished with moderate expenditure. There are four types of tests:

- (i) *Hypothetical* : The hypothetical test is an exercise to verify the existence of all necessary procedures and actions specified within the recovery plan and to prove the theory of those procedures. It is a theoretical check and must be conducted regularly. This exercise is generally a brief one designed to look at the worst case for equipment, ensuring that the entire plan process is reviewed.
- (ii) *Component* : A component is the smallest set of instructions within the recovery plan which enables specific processes to be performed. For example the process "System Load/IPL" involves a series of commands to load the system. However, in the recovery situation this may be different from normal operational requirements. Certain functions need to be enabled or disabled to suit the new environment. If this is not fully tested incompatibility problems with other components are likely. Component testing is designed to verify the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods. Examples of component tests include back-up procedures, offsite tape storage recovery, technology and network infrastructure assembly, recovery and restoration procedures and security package start-up procedures.
- (iii) *Module* : A module is a combination of components. The ideal method of testing is that each component be individually tested before being included in a module. The aim of module testing is to verify the validity and functionality of the recovery procedures when multiple components are combined. If one is able to test all modules, even if unable to perform a full test, then one can be confident that the business will survive a major disaster. It is when a series of components are combined without individual tests that difficulties occur. Examples of module testing include alternate site activation, system recovery, network recovery, application recovery, database recovery and run production processing.
- (iv) *Full* : The full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective detailed in the recovery plan. The test also verifies the interdependencies of various modules to ensure that progression from one module to another can be effected without problem or loss of data. The two main objectives associated with full test are:

- ◆ To confirm that the total time elapsed meets the recovery time objective.
- ◆ To prove the efficiency of the recovery plan to ensure a smooth flow from module to module.

**6.11.1 Setting objectives** : Each test is designed around a worst-case scenario for equipment as this will ensure the entire plan is examined for all possible disastrous situations. Only when every requirement associated with each component has been documented and verified can the recovery plan be said to be complete and functional.

Test objectives should include :

- Recovery of systems at the standby site, and establishment of an environment to enable full accommodation of the nominated applications.
- A fully documented set of procedures to obtain and utilise offsite tapes to restore the system and critical applications to the agreed recovery point, as set out in the recovery plan.
- Recovery of system/application/network/database data from the offsite/backup tapes.
- Detailed documentation on how to restore the production data as stipulated in the recovery plan, to the agreed recovery point.
- Fully documented procedures for establishing communication lines/ equipment to enable full availability and usage by appropriate areas e.g. business units, data entry, users, etc.
- Established communication lines/equipment as set out in the plan.
- Examination of the designated alternative sites and confirmation of all components are also noted in the plan.

**6.11.2 Defining the Boundaries** : Test boundaries are needed to satisfy the disaster recovery strategy, methodology and processes. The management team also must consider future test criteria to ensure a realistic and obtainable progression to meet the end objectives. Opportunities to test actual recovery procedures should be taken wherever possible e.g. purchase of new additional equipment, vendor agreements. Management must also decide whether or not to include internal (auditors/management) or external (data security services) observers or a combination of both.

**6.11.3 Scenario** : The scenario is the description of the disaster and explains the various criteria associated with such a disaster. For example the scenario must outline what caused the disaster and the level of damage sustained to the equipment and facilities, and whether or not anything can be salvaged from the wreckage. The purpose is not to get bogged down in great details but to explain to all the participants what is, or is not available, what tools can, or cannot be used, the objective of the exercise, the time of the disaster, and the planned recovery points.

**6.11.4 Test Criteria** : Not all tests require all personnel to attend. The test criteria advise all participants including observers as appropriate, where they are to be located and the time/day

## 6.22 Information Systems Control and Audit

the exercise will take place. The role of the observer is to give an unbiased view and to comment on the area of success or concern to assist in future testing.

**6.11.5 Assumption :** Assumptions will need to be made. They allow a test to achieve the results without being bound by other elements of the recovery plan, which may not yet have been verified. Assumptions allow prerequisites of a particular component/module to be established outside the test boundaries. Examples include:

- All technical information documented in the plan, including appendices, are complete and accurate.
- All purchases (equipment, furniture, etc.) can be made in the recovery time required.
- Tapes and other equipment recalled from offsite are valid and useable.

**6.11.6 Test Prerequisites :** Before any test is attempted, the recovery plan must be verified as being fully documented in all sections, including all appendices and attachments that have been referenced to in each process. Each of the participating teams in the test must be aware of how their role relates to other teams, when and how they are expected to perform their tasks, and what tools are permissible. It is the responsibility of each team leader to keep a log of proceedings for later discussion and action to prepare better for future tests.

**6.11.7 Briefing session :** No matter whether it is hypothetical, component, module or full test, a briefing session for the teams is necessary. The boundaries of the test are explained and the opportunities to discuss any technical uncertainties are provided.

Depending on the complexity of the test, additional briefing sessions may be required to outline the general boundaries, discuss technical queries, and brief the senior management on the test objectives. The size of the exercise and the number of staff involved will determine the time between the briefing sessions and the test. However, this time period must provide sufficient opportunity for personnel to prepare adequately particularly the technical staff. It is recommended that the final briefing be held not more than two days prior to a test date to ensure all activities are fresh in the minds of the participants and the test is not impacted through misunderstandings or tardiness. An agenda could be:

- (i) Team objectives
- (ii) Scenario of disaster
- (iii) Time of the test
- (iv) Location of each team
- (v) Restrictions on specific teams
- (vi) Assumptions of the test
- (vii) Prerequisites for each team

**6.11.8 Checklists :** Checklists provide the minimum preparation for all test types. Checklists are directly related to specific modules of the recovery plan and all sections relevant to particular test must be verified as complete before a test date is set.

As these checklists follow various modules associated with the recovery plan, only those parts applicable to the forthcoming test are compulsory prerequisites for that test. However, it is recommended that all sections of the checklist be completed as soon as possible.

Checklists showing the details required are provided in the following section.

**6.11.9 Analysing the test :** While testing is beneficial, the effective recovery plan can be achieved only by constructive analysis of each test and its result through a post-mortem. This also maintains the momentum gained from the test, which is critical to the process of building a workable plan. Many staff perceives disaster recovery as an additional workload. However, over time through constructive and regular involvement, staffs develop a greater commitment.

**6.11.10 Debriefing session :** If the company has a dedicated Disaster Recovery Plan (DRP) team or co-ordinator assigned permanently, the team or co-ordinator would have the responsibility of conducting the briefing and debriefing sessions. If not, then the responsibility lies with the command team leader.

The format is to discuss the results of the findings of the test with a view of improving the recovery plan for future exercises. From these discussions, a set of objectives is developed for later inclusion into the report. An agenda could be:

- (i) Overall performance
- (ii) Team performance
- (iii) Observations
- (iv) Areas of concern
- (v) Next test ( type and time)
- (vi) Test report

Each team leader has the responsibility of maintaining a log of events during each test. The information gathered from these logs, in addition to the post-mortem report by the test manager is used to produce the test report. Any areas for improvement are noted for action, assigned to the appropriate team member and given a realistic completion date. A typical format could be:

- (i) Executive summary
- (ii) Objective results
- (iii) Performance
- (iv) Overall teams and list of actions
- (v) Conclusion

## **6.12 AUDIT TOOLS AND TECHNIQUES**

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorised as under:



## 6.24 Information Systems Control and Audit

- i. **Automated Tools** : Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.
- ii. **Internal Control Auditing** : This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- iii. **Disaster and Security Checklists** : A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- iv. **Penetration Testing** : Penetration testing can be used to locate vulnerabilities.

## 6.13 AUDIT OF THE DISASTER RECOVERY/BUSINESS RESUMPTION PLAN

- (i) Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:
  - Identification and prioritisation of the activities which are essential to continue functioning.
  - The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
  - Operations managers and key employees participated in the development of the plan.
  - The plan identifies the resources that will likely be needed for recovery and the location of their availability.
  - The plan is simple and easily understood so that it will be effective when it is needed.
  - The plan is realistic in its assumptions.
- (ii) Determine if information backup procedures are sufficient to allow for recovery of critical data.
- (iii) Determine if a test plan exists and to what extent the disaster recovery/business resumption plan has been tested.
- (iv) Determine if resources have been made available to maintain the disaster recovery/business resumption plan and keep it current.
- (v) Obtain and review the existing disaster recovery/ business resumption plan.
- (vi) Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests
- (vii) Obtain and review the existing business impact analysis.

## Business Continuity Planning and Disaster Recovery Planning 6.25

- (viii) Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.
- (ix) Determine if copies of the plan are safeguarded by off-site storage.
- (x) Gain an understanding of the methodology used to develop the existing disaster recovery/ business resumption plan. Who participated in the development effort?
- (xi) Gain an understanding of the methodology used to develop the existing business impact analysis.
- (xii) Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.
- (xiii) Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?
- (xiv) Determine if the plan is dated each time that it is revised so that the most current version will be used if needed.
- (xv) Determine if the plan has been updated within past 12 months.
- (xvi) Determine all the locations where the disaster recovery/ business resumption plan is stored. Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?
- (xvii) Review information backup procedures in general. The availability of backup data could be critical in minimising the time needed for recovery.
- (xviii) Interview functional area managers or key employees to determine their understanding of the disaster recovery/ business resumption plan. Do they have a clear understanding of their role in working towards the resumption of normal operations?
- (xix) Does the disaster recovery/ business resumption plan include provisions for Personnel
  - Have key employees seen the plan and are all employees aware that there is such a plan? ii) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?
  - Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?
  - Does the disaster recovery/ business resumption plan include provisions for people with special needs?
  - Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?
- (xx) Building, Utilities and Transportation
  - Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?

## 6.26 Information Systems Control and Audit

- Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
- Review any agreements for use of backup facilities.
- Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
- Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested?
- Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

### (xxi) Information Technology

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritisation of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
- Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications?
- Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.

### (xxii) Administrative Procedures

- Does the disaster recovery/ business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time?
- Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
- Determine if the disaster recovery/ business resumption plan covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.
- Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?

- To facilitate retrieval, are essential records separated from those that will not be needed immediately?
- (xxiii) Does the disaster recovery/ business resumption plan include the names and numbers of suppliers of essential equipment and other material?
- (xxiv) Does the disaster recovery/ business resumption plan include provisions for the approval to expend funds that were not budgeted for the period? Recovery may be costly.
- (xxv) Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorise activation of the plan should the need arise.

### **Self - Examination Questions**

1. Why is a business continuity plan important in an organisation?
2. What are the components of a business Continuity Plan?
3. Describe the methodology of developing a business continuity plan?
4. What are the various phases of developing a business continuity plan?
5. What is business impact analysis?
6. There are different kinds of business continuity plans. Comment?
7. Back-up Plan is one of the most important for an organisation. Comment?
8. As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?
9. What are the benefits of performing a technology risk assessment?
10. Describe various types of back-up techniques?
11. What is the importance of back-up redundancy?
12. What are the various alternate processing arrangements an organisation may consider?
13. Describe various back-up devices?
14. Describe various contents of a disaster recovery procedural plan?
15. What is the importance of taking insurance as a back-up measure? Describe various kinds of insurance?
16. Describe the various disaster recovery testing? Describe the testing procedure?
17. What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.
18. Give an overview of a disaster recovery plan?

# AN OVERVIEW OF ENTERPRISE RESOURCE PLANNING: (ERP)

---

## 7.0 INTRODUCTION

In today's fiercely competitive business environment, there has to be much greater interaction between the customers and manufacturers. This means, in order to produce goods tailored to customer requirements and provide faster deliveries, the enterprise must be closely linked to both suppliers and customers. In order to achieve this improved delivery performance, decreased lead times within the enterprise and improved efficiency and effectiveness, manufacturers need to have efficient planning and control systems that enable very good synchronization and planning in all the processes of the organization.

Also, it requires a strong integration across the value chain. Hence, there is a need for a standard software package, which equips the enterprise with the necessary capabilities to integrate and synchronize the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Most organisations across the world have realised that in a rapidly changing environment, it is impossible to create and maintain a custom-designed software package, which will cater to all their requirements, and be up-to-date. Realising the requirement of user organisations, some of the leading software companies have designed Enterprise Resource Planning software, which offers an integrated software solution to all the functions of an organisation.

Enterprise Resource Planning (ERP) is the latest high-end solution, information technology has lent to business applications. The ERP solutions seek to streamline and integrate operation processes and information flows in the company to synergise the resources of an organisation namely men, material, money and machine through information. Initially implementation of an ERP package was possible only for large multi nationals and infrastructure companies due to high cost. Today, many companies in India have gone in for implementation of ERP. It is expected that in the near future, 60 per cent of the companies will be implementing one or the other ERP packages since this will become a must for gaining competitive advantage.

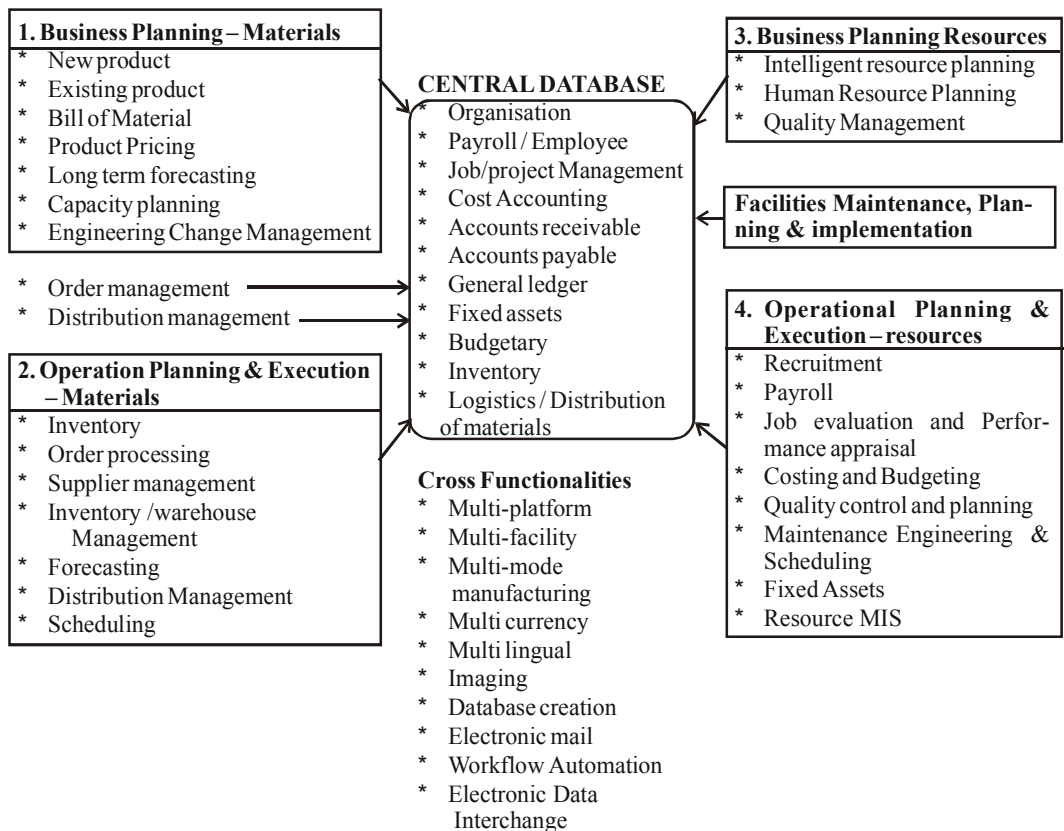
## 7.2 Information Systems Control and Audit

### 7.1 ERP- DEFINITION

An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like Logistics, Production, Finance, Accounting and Human Resources. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine. ERP is a global, tightly integrated closed loop business solution package and is multifaceted.

In simple words, Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales. Taking information from every function it is a tool that assists employees and managers plan, monitor and control the entire business. A modern ERP system enhances a manufacturer ability to accurately schedule production, fully utilize capacity, reduce inventory, and meet promised shipping dates.

A general model of ERP is shown in Fig. 1.



**Fig 7.1.1 : General Model of ERP**

**7.1.1 Evolution of ERP:** In the ever-growing business environment, the following demands are placed on the industry:

- Aggressive cost control initiatives

- Need to analyse costs/revenues on a product or customer basis
- Flexibility to respond to changing business requirements
- More informed management decision making
- Changes in ways of doing business.

The difficulty in getting accurate data, timely information and proper interface of complex business functions have been identified as the hurdles in the growth of any business. Time and again, depending on the velocity of the growing business needs, one or the other applications and planning systems have been introduced into the business world for crossing these hurdles and achieving growth. They are:

- Management Information Systems (MIS)
- Integrated Information Systems (IIS)
- Executive Information Systems (EIS)
- Corporate Information Systems (CIS)
- Enterprise Wide Systems (EWS)
- Material Resource Planning (MRP)
- Manufacturing Resource Planning (MRP II)
- Money Resource Planning (MRP III)

ERP has evolved from the system known as MRPII (Manufacturing Requirement planning) system with the integration of information between Vendor, Customer and Manufacturer using networks such as LAN, WAN and INTERNET etc.

MRPII system again evolved from MRP (Material Requirement Planning) system. MRP is a technique that explodes the end product demands obtained from Master Production Schedule (MPS) for the given product structure which is taken from Bill of Material (BOM) into a schedule of planned orders considering the inventory in hand. MRP system processes this data and provides valuable guidelines to the scheduler in the form of work orders to plan the Production Schedule. The net requirements for each item are computed and replenishment orders are created and planned for release.

MRP system provides reports such as MRP reports, Planned Order releases for Purchase orders, Work Orders, Reschedule open orders report, Firm planned reports, Shortages report etc. MRP is considered as an important planning and manufacturing control activity for materials.

MRPII is a method for planning of all the resources of the manufacturing company. It involves all operational and financial planning and has simulation capabilities to answer 'WHAT IF' questions. It links different functional areas like Business Planning, Production Planning, MPS, MRP, Capacity Requirement Planning and Execution system for capacity and priority. Output from these systems is integrated with Financial Reports such as Business Plan, Purchase, Shipping, Budget, and Inventory for production etc.

## 7.4 Information Systems Control and Audit

MRPII has a number of drawbacks. The main problem is that it has not been able to effectively integrate the different functional areas to share the resources effectively.

ERP as the name indicates is the integration of Enterprise Resources.

The ERP package works on the fundamental premise that the whole being greater than the sum of its parts. It provides an integrated information storehouse where information needs to be stored only once and can be further processed and reported to anyone in the value chain. The traditional application systems, which the organizations generally employ, treat each transaction separately. They are built around the strong boundaries of specific functions that a specific application is meant to cater. For an ERP, it stops treating these transactions separately as stand-alone activities and considers them to be the part of the inter-linked processes that make up the business.

Almost all the typical application systems are nothing but the data manipulation tools. They store data, process them and present them in the appropriate form whenever requested by the user. In this process, the only problem is that there is no link between the application systems being used by different departments. An ERP system also does the same thing, but in a different manner.

There are hundreds of such data tables, which store data generated as a result of diverse transactions, but they are not confined to any departmental or functional boundaries, but rather integrated to be used by multiple users, for multiple purposes and at multiple places.

**7.1.2 Enabling Technologies :** It is not possible to think of an ERP system without sophisticated information technology infrastructure. It is said that, the earlier ERP systems were built only to work with huge mainframe computers. The new era of PC, advent of client server technology and scalable Relational Database Management Systems (RDBMS), all have contributed for the ease of deployment of ERP systems. Most of the ERP systems exploit the power of Three Tier Client Server Architecture. In a client server environment, the server stores the data, maintaining its integrity and consistency and processes the requests of the user from the client desktops. The load of data processing and application logic is divided between the server and the client. The three-tier architecture adds a middle stratum, embodying all application logic and the business rules that are not part of the application, enforcing appropriate validation checks.

It is assumed that the companies implementing ERP solutions have multiple locations of operation and control. Hence, the online data transfer has to be done across locations. To facilitate these transactions, the other important enabling technologies for ERP systems are Workflow, Work group, Group Ware, Electronic Data Interchange (EDI), Internet, Intranet, Data warehousing, etc.

**7.1.3 ERP Characteristics :** An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. These features are:

**Flexibility :** An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).



**Modular & Open :** ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.

**Comprehensive :** It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

**Beyond The Company :** It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.

**Best Business Practices :** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organisation.

**7.1.4 Features of ERP :** Some of the major features of ERP and what ERP can do for the business system are :

- ERP provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities, creation of Materials and Resources. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
- Has end to end Supply Chain Management to optimize the overall Demand and Supply Data.
- ERP facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.
- ERP performs core activities and increases customer service, thereby augmenting the corporate image.
- ERP bridges the information gap across organisations.
- ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ERP is the solution for better project management.
- ERP allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video conferencing, E-Commerce etc.
- ERP eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- ERP provides intelligent business tools like decision support system, Executive information system, Data mining and easy working systems to enable better decisions.

## 7.6 Information Systems Control and Audit

### 7.1.5 Why Companies Undertake ERP

- **Integrate financial information** : As the CEO tries to understand the company's overall performance, he may find many different versions of the truth. Finance has its own set of revenue numbers, sales has another version, and the different business units may each have their own version of how much they contributed to revenue. ERP creates a single version of the truth that cannot be questioned because everyone is using the same system.
- **Integrate customer order information** : ERP systems can become the place where the customer order lives from the time a customer service representative receives it until the loading dock ships the merchandise and finance sends an invoice. By having this information in one software system, rather than scattered among many different systems that can't communicate with one another, companies can keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.
- **Standardise and speed up manufacturing processes** : Manufacturing companies - especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/ recording/ report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of a manufacturing process. Standardising those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.
- **Reduce inventory** : ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfilment process inside the company. That can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users better plan deliveries to customers, reducing the finished good inventory at the warehouses and shipping docks. To really improve the flow of your supply chain, you need supply chain software, but ERP helps too.
- **Standardise HR information** : Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees' time and communicating with them about benefits and services. ERP can fix that.

**7.1.6 Benefits of ERP** : The benefits accruing to any business enterprise by implementing an ERP package are unlimited. According to companies like Nike, DHL, Tektronix, Fujitsu, Millipore, and Sun Microsystems, the following are some of the benefits they achieved by implementing the ERP packages :

- Gives Accounts Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.
- Reduce paper documents by providing on-line formats for quickly entering and retrieving information.

- Improves timeliness of information by permitting posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
- Improved cost control.
- Faster response and follow-up on customers.
- More efficient cash collection, say, material reduction in delay in payments by customers.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change in business operations and market conditions.
- Helps to achieve competitive advantage by improving its business process.
- Improves supply-demand linkage with remote locations and branches in different countries.
- Provides a unified customer database usable by all applications.
- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.
- Provides solution for problems like Y2K and Single Monetary Unit (SMU) or Euro Currency.

**7.2 BUSINESS PROCESS REENGINEERING (BPR)**

ERP is a result of a modern Enterprise’s concept of how the Information System is to be configured to the challenging environments of new business opportunities. However merely putting in place an information system is not enough. Every company that intends to implement ERP has to reengineer its processes in one form or the other. This process is known as Business Process Reengineering (BPR).

**Table 1 : Some Typical processes with descriptions**

<b>Process</b>	<b>Description</b>
Forecasting	Shows sales, Fund Flows etc over a long period of time say next two years
Fund management	The necessity of funds and the way to raise these funds. Uncertainty and Risk factors to be considered. Simulation with ‘What if’ type analysis
Price Planning	Determines the price at which products are offered. Involves application of technology to pricing support such as commercial database services. Also feedback and sensitivity analysis

## 7.8 Information Systems Control and Audit

Budget Allocation	Using computerised algorithms to estimate desirable mix of funds allocated to various functions.
Material requirement planning	Process of making new products from raw materials and include production scheduling, requirement planning. Also activities for monitoring and planning of actual production.
Quality control	Takes care of activities to ensure that the products are of desired quality.

### 7.2.1 What is BPR?

The most accepted and formal definition for BPR, given by Hammer and Champy is reproduced here: “ BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement, in critical, contemporary measures of performance such as cost, quality, service and speed,” This has a few important key words, which need clear understanding. Here, dramatic achievement means to achieve 80% or 90% reduction (in say, delivery time, work in progress or rejection rate) and not just 5%, 10% reduction. This is possible only by making major improvements and breakthroughs, and not small incremental changes (like those in Total Quality Management (TQM) or suggestion schemes).

Radical redesign means BPR is reinventing and not enhancing or improving. In a nutshell, a “cleanslate approach” of BPR says that “Whatever you were doing in the past is all wrong”, do not get biased by it or reassemble you new system to redesign it afresh. Fundamental rethinking means asking the question “why do you do what you do”, thereby eliminating business process altogether if it does not add any value to the customer. There is no point in simplifying or automating a business process which does not add any value to the customer. A class example is that of asking for an invoice from the supplier for payment when the company has already received and accepted a particular quantity of materials physically and at an agreed price. Receiving, processing, and filing of invoices add no value to customer and makes only the supplier unhappy for delayed payments. Thus, BPR aims at major transformation of the business processes to achieve Dramatic improvement. Here, the business objectives of the Enterprise (e.g., profits, customer-satisfaction through optimal cost, quality, deliveries etc.) are achieved by “transformation” of the business processes which may, or may not, require the use of Information Technology (IT).

**7.2.2 Business Engineering** : Business Engineering has come out of merging of two concepts namely Information Technology and Business Process Reengineering.

Business Engineering is the rethinking of Business Processes to improve speed, quality and output of materials or services. The emphasis of business engineering is the concept of Process Oriented Business Solutions enhanced by the Client-Server computing in Information Technology. The main point in business engineering is the efficient redesigning of company's value added chains. Value added chains are a series of connected steps running through a business which when efficiently completed add value to enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes.

Business Engineering is the method of development of business processes according to changing requirements.

**7.2.3 Business Management :** ERP merges very well with common business management issues like Business Process Reengineering, total quality management, mass customisation, service orientation, and virtual corporation etc. The basic objective of implementing an ERP program is to put in place the applications and infrastructure architecture that effectively and completely support the Enterprise’s business plan and business processes. When an enterprise does not have optimized business processes, the ERP implementation needs a process reengineering which enable to capture knowledge of the experts into the system thus gaining considerable benefits in productivity.

The first step in implementation of ERP is the development of a Business process model showing business process as one large system and the interconnection and sequence of business subsystems or processes that drive it.

**7.2.4 Business Modelling :** The approach of ERP implementation is carried out using MIS planning. First of all, a model consisting of core business processes or activities of the business is to be developed. This is the diagrammatic representation of Business as a large system with interconnection of subsystems or processes that it comprises of. A typical layout is shown in Figure 2. The planning to arrive at the process is from top down whereas the MIS implementation is done from bottom up.

We can model Business as a system making the processes managing their facilities and material as their resources. Information is treated as a vital resource managing other resources.

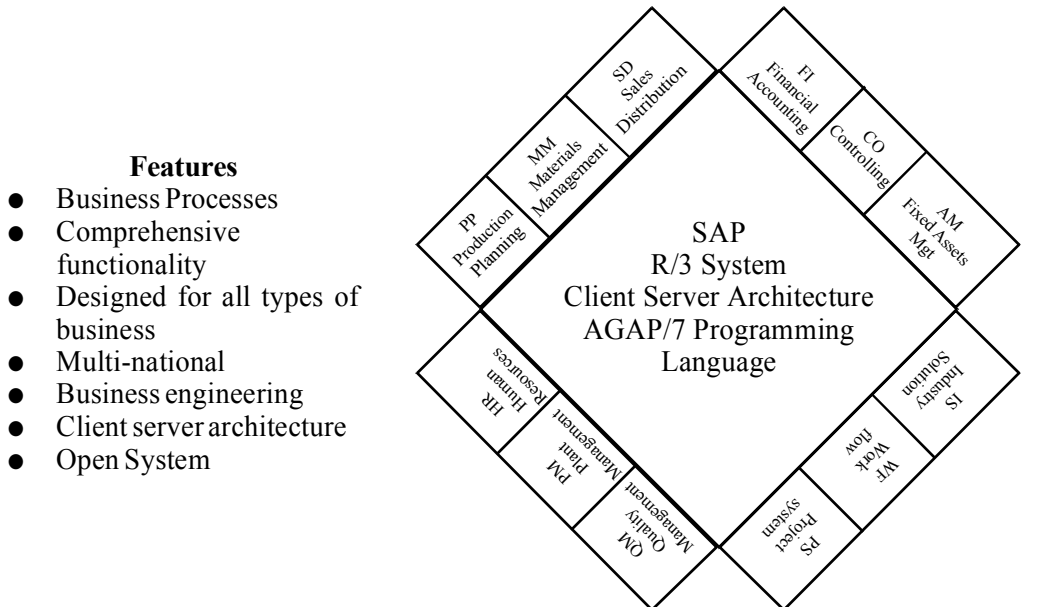


Fig 7.2 : SAP Modules

## 7.10 Information Systems Control and Audit

The Data model consists of two elements.

1. A diagram describing various Business processes and their interactions.
2. An underlying Data Model.

The Reference model can be used by various companies to list their processes and data entities and if required can be subsequently modified to suit specific nature of requirements. Some typical examples are shown in table 2.

**Table 2 : List of some of the entities forming a data model**

Entity	Description
External Data	Entities outside the firm that interact with it such as customers, suppliers, competitors and distributors. Also includes predictive data regarding economy and future events in external environment.
Internal Data	Data generated from the firm's transaction processing system, internal forecasts or parameters monitored .
Funding Data	Includes information on specific sources of funds as well as availability terms and conditions etc.
Marketing Research Data	Mainly consumer related data that can be used to support marketing decisions and result of surveys.
Production Data	Shop floor data on production processes including standards and actual of time and material resources concerned.
Inventory data	Includes inventories of raw materials goods in progress and finished goods.
Personnel data	Mostly includes profiles of employees, their skill levels, experience and past performance on various assignments.
Sales forecast	Product-wise and period-wise forecast for various products sold by the company.
Payroll data	Data about salaries, tax deductions, statutory forms and other deductions
General Ledger	Integrated transaction data from pay roll and account receivable. It is the basis for budgeting and planning data.

The general principles of Business Process Analysis and classification and methodology of looking at a Business Information system to support a series of interlocking subsystems are universally applicable.

**7.2.5 Business modeling in practice :** Most of the ERP packages available today enable flow charting business processes using standard flow chart symbols. By connecting symbols used for users, events, tasks/functions, and other organizational information, complex business information can be analysed .For example SAP which is a popular ERP package

uses event driven process chain (EPC) methodology to model Business Process. All ERP packages provide standard template for each of the processes so that actual processes can be compared and deviations analysed. With the help of the business model, it is possible to check as to how well the model fits into the application so that the degree of suitability of the ERP package can be assessed. Business Modeling is the basis by which one can select and implement a suitable ERP package.

### 7.3 ERP IMPLEMENTATION

ERP implementation is a special event in an organisation. It brings together in one platform, different business functions, different personalities, procedures, ideologies and philosophies with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Implementation of ERP is a risky effort since it involves considerable amount of time, efforts and valuable resources. Even with all these, the success of an implementation is not guaranteed.

The success of an implementation mainly depends on how closely the implementation consultants, users and vendors work together to achieve the overall objectives of the organisation. The implementation consultants have to understand the needs of the users, understand the prevailing business realities and design the business solutions keeping in mind all these factors. It is the users who will be driving the implementation and therefore their active involvement at all stages of implementation is vital for the overall success of implementation.

An ERP package after implementation is expected to improve the flow of information and formalize and standardize all the business processes and workflow that exist in an enterprise. However the workload of users may not decrease. It is worthwhile to remember that ERP is an enabling tool, which makes one do his work better, which naturally need additional efforts.

During the course of implementation the standard package may undergo changes which may be a simple one or a major 'functionality' change. Implementing such changes is known as Customization. The contents of the package are known as *modules* and the modules are further divided into Components. However, it is always better to satisfy user requirements and overall objectives within the available framework of the existing package because any change in any functional module will have an adverse impact on the functioning of the other modules of the package. Maximum benefit will be available only when the standard package is implemented in totality with an aim for optimised use.

The roles and responsibilities of the employees have to be clearly identified, understood and configured in the system. The employees will have to accept new processes and procedures laid down in the ERP system. At the same time these processes and procedures have to be simple and user friendly.

The ability of the ERP package to manage and support dynamically changing business processes is a critical requirement for the organisation and therefore the package should be expandable and adaptable to meet these changes.

## 7.12 Information Systems Control and Audit

A well managed and implemented ERP package can give a 200 percent return on investment where as a poorly implemented one can yield a return on investment as low as 25 percent.

### 7.3.1 Key Planning and Implementation decisions

This discussion looks at a number of the key decisions that need to be made when considering an enterprise integration effort.

#### ➤ ERP or Not to ERP?

The decision to implement an ERP should be based on a business case rational. Possible business cases involve technology, process improvements, productivity improvements and strategic consideration.

Technology justifications include the need to address the Y2K problem (in most cases, this is no longer applicable), integrate the functions of disparate systems, replace poor-quality existing systems and merge acquisitions with new capabilities such as web accessibility into the business environment. Process improvements address actions that result in personal and IT cost reductions. Productivity improvements include the need to close the financial cycle and increase the overall production from an enterprise standpoint. Strategic considerations address the ability to implement new strategies not supported by the current software, improve customer service and satisfaction, respond to competitive pressures and enhance customer responsiveness.

#### ➤ Follow Software's Processes or Customize?

This key decision may determine the success or failure of the ERP effort. If the organization decides to follow the process of the software, this will result in the organization following best practices within its sector, thereby giving it a chance to improve and standardize their processes. This approach will also facilitate future change to the ERP software. However, this approach can create significant turmoil by requiring employees to change their ways of doing business.

If the organization decides to stick with its current processes and customize the software to fit these processes, the organization obviously will not have to experience the pain and stress associated with changing its process. However, it will be very costly to customize and maintained the software over time. Interfaces modular compatibility needs to be sustained.

#### ➤ Inhouse or Outsource?

Outsourcing has the advantage of allowing the organization to continue to focus on its core mission, avoid a relative substantial financial commitment (in some cases) and minimize the impact on the MIS department. On the downside, providing opportunities to those external to the organization may poorly impact employee morale and may give rise to security issues.

The upsides to an in-house implementation include: a better match between the software and the business, applications optimized for the organization and better maintained security. However, an in-house approach cannot be accomplished if there is a lack of internal expertise and personnel to support such an effort.



➤ **“Big Bang” or Phased Implementation?**

A “big bang” implementation involves having all modules at all locations implemented at the same time. Characteristics of this approach include no need for temporary interfaces, limited requirement to maintain legacy software, cross-module functionality and overall cost if no contingencies arise.

Phased implementation one or a group at a time, often a single location at a time. Benefits of this approach include: a smoothing of resource requirements, an ability to focus on a particular module, avail-ability of existing legacy systems as a fall-back, reduced risk, the knowledge gained with each phase and the usefulness of demonstrable working system.

**Other implementation approaches** include:

*The wave approach* : This approach involves the application of different waves of change to different business units or regions.

*Parallel implementation* : This approach involves both ERP and an existing system running together for a period of time. Its attributes include: having a basis of comparison; existing system serves as backup; rewires more computing and human resources ---- more costly; existing system may not be properly maintained during the period; and reengineering not supported by existing systems.

*Instant cutovers (flip-the-switch)* : This approach is lower in cost motivates users to seriously convert to the new system and reduces the need for redundant systems. However, it tends to be risky, stressful to users and requires a high level of contingency planning.

### 7.3.2 ERP Implementation Methodology

Several steps are involved in the implementation of a typical ERP package. These are:

1. Identifying the needs for implementing an ERP package.
2. Evaluating the ‘As Is’ situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.
3. Deciding the ‘Would be’ situation for the business i.e., the changes expected after the implementation of ERP.
4. Reengineering the Business Process to achieve the desired results in the existing processes.
5. Evaluating the various available ERP packages to assess suitability.
6. Finalising of the most suitable ERP package for implementation.
7. Installing the required hardware and networks for the selected ERP package.
8. Finalising the Implementation consultants who will assist in implementation.
9. Implementing the ERP package.

## 7.14 Information Systems Control and Audit

Let us examine these steps in detail:

1. **Identifying the Needs:** Some of the basic questions, which are to be answered, are
  - ◆ Why should an ERP package be implemented?
  - ◆ Will it improve profitability?
  - ◆ Can the delivery times of products be reduced?
  - ◆ How does it improve customer satisfaction in terms of quality, cost, delivery time and service?
  - ◆ Will it help to reduce cost of products?
  - ◆ How can it help to increase business turnover and at the same time reduce manpower?
  - ◆ Will it be possible to reengineer the business processes?

Other requirements to satisfy the information management are:

- ◆ Need for quick flow of information between Business partners.
  - ◆ Effective MIS for quick decision making
  - ◆ Elimination of manual working.
  - ◆ High level of integration between various business functions.
2. **Evaluating the “AS IS” situation of the business :** To understand the present situation of the business, the various functions should first be listed. The processes used to achieve business transactions should be listed in detail. The details of business process can be obtained by mapping the processes to the functions:
    - ◆ Total time taken by the business processes.
    - ◆ Number of decision points existing in the present scenario.
    - ◆ Number of Departments/Locations of business processes.
    - ◆ The flow of information and its routing.
    - ◆ The number of reporting points currently available.
  3. **Deciding the desired ‘Would Be’ situation :** The concept of ‘Benchmarking’ is used to see that processes achieved are the best in industry. Benchmarking is done on various factors like cost, quality, service etc. This concept enables to optimise the processes to gain overall benefits.
  4. **Reengineering the business process :** Reengineering of business processes is done to
    - ◆ Reduce the business process cycle time.
    - ◆ To reduce the number of decision points to a minimum.

- ◆ Streamlining the flow of information and eliminating the unwanted flow of information.

5. **Evaluation of various ERP packages** : Evaluation of ERP packages are done based on the following criteria:-

*Flexibility*: It should enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding to address new products and markets.

*Comprehensive* : It should be applicable across all sizes, functions and industries. It should have in-depth features in accounting and controlling, production and materials management, quality management and plant maintenance, sales and distribution, human resources management and plant maintenance, sales and distribution, human resources management, and project management. It should also have information and early warning systems for each function and enterprise-wide business intelligence system for informed decision making at all levels. It should be open and modular.

It should embrace an architecture that supports components or modules, which can be used individually, expandable in stages to meet the specific requirements of the business, including industry specific functionality. It should be technology independent and mesh smoothly with in-house/third-party applications, solutions and services including the Web.

*Integrated* : It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, warehouse management, financial accounting, and human resources management should be integrated into a workflow of business events and processes across departments and functional areas, enabling knowledge workers to receive the right information and documents at the right time at their desktops across organisational and geographical boundaries.

*Beyond the company* : It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners and create complete logistical chains covering the entire route from supply to delivery, across multiple geographies, currencies and country specific business rules.

*Best business practices* : The software should enable integration of all business operation in an overall system for planning, controlling and monitoring and offer a choice of multiple ready-made business processes including best business practices that reflect the experiences, suggestions and requirements of leading companies across industries. In other words, it should intrinsically have a rich wealth of business and organisational knowledge base.

*New technologies* : It should incorporate cutting-edge and future-proof technologies such as object orientation into product development and ensure inter-operability with the Internet and other emerging technologies.

It should be Y2K and Euro compliant, group up.

## 7.16 Information Systems Control and Audit

Other factors to be considered are :

- ◆ Global presence of package.
  - ◆ Local presence.
  - ◆ Market Targeted by the package.
  - ◆ Price of the package.
  - ◆ Obsolescence of package.
  - ◆ Ease of implementation of package.
  - ◆ Cost of implementation.
  - ◆ Post-implementation support availability.
6. **Finalisation of the ERP package** : Finalisation of the ERP package can be done by making a comparison of critical factors through a matrix analysis.
7. **Installation of Hardware and Networks** : This work is carried out in a phased manner depending on the schedule of implementation and need of the hardware components.
8. **Finalising the Implementation Consultants** : The factors of selection for consultants are:
- ◆ Skill set
  - ◆ Industry specific experience.
  - ◆ Cost of hiring the consultant.
9. **Implementation of ERP package** : The general steps involved in the implementation are
- ◆ Formation of team.
  - ◆ Preparation of plan.
  - ◆ Mapping of Business Processes to package.
  - ◆ Gap Analysis i.e., deviation of existing processes from standard processes.
  - ◆ Customisation.
  - ◆ Development of user-specific reports and transactions.
  - ◆ Uploading of Data from existing system.
  - ◆ Test runs.
  - ◆ User Training.
  - ◆ Parallel run.
  - ◆ Concurrence from user.
  - ◆ Migration to the new system

- ◆ User documentation.
- ◆ Post-implementation support.
- ◆ System monitoring and fine tuning.

**7.3.3 Implementation Guidelines For ERP :** There are certain general guidelines, which are to be followed before starting the implementation of an ERP package.

1. Understanding the corporate needs and culture of the organisation and then adopt the implementation technique to match these factors.
2. Doing a business process redesign exercise prior to starting the implementation.
3. Establishing a good communication network across the organisation.
4. Providing a strong and effective leadership so that people down the line are well motivated.
5. Finding an efficient and capable project manager.
6. Creating a balanced team of implementation consultants who can work together as a team.
7. Selecting a good implementation methodology with minimum customisation.
8. Training end users.
9. Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

## **7.4 POST- IMPLEMENTATION**

To start at the beginning, many post-implementation problems can be traced to wrong expectations and fears. The expectations and fears that corporate management have from an ERP have been greatly published. Of course, some of the blame for this is on the ERP vendors and their pre-implementation sales hype.

A few of the popular expectations are:

- An improvement in processes
- Increased productivity on all fronts.
- Total automation and disbanding of all manual processes.
- Improvement of all key performance indicators.
- Elimination of all manual record keeping.
- Real time information systems available to concerned people on a need basis.
- Total integration of all operations.

## 7.18 Information Systems Control and Audit

ERP implementation also engenders a host of fears. Some of them are:

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile.
- An organizational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Balancing the expectations and fears is a very necessary part of the implementation process.

## 7.5 RISK AND GOVERNANCE ISSUES IN AN ERP

Organizations face several new business risks when they migrate to real-time, integrated ERP systems. Those risks include:

- *Single point of failure* : Since all the organization's data and transaction processing is within one application system and transaction processing is within one application system.
- *Structural changes* : Significant personnel and organizational structures changes associates with reengineering or redesigning business processes.
- *Job role changes* : Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation.
- *Online, real-time* : An online, real-time system environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring of re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
- *Change management* : It is challenging to embrace a tightly integrated environment when different business processes have existed among business units for so long. The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and efficient in the performance of their day-to-day duties. Considerable training is therefore required for what is typically a large number of users.
- *Distributed computing experience* : Inexperience with implementing and managing distributed computing technology may pose significant challenges.
- *Broad system access* : Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.

- *Dependency on external assistance* : Organization accustomed to in-house legacy systems may find they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.
- *Program interfaces and data conversions* : Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposures of data integrity, security and capacity requirements for ERP are therefore often much higher.
- *Audit expertise* : Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialisation such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organisation's business processes, have to maintain a good grasp of all the core modules to function effectively.

More recently, some of the additional risks and good governance issues introduced by the e-enabled ERP environments concern:

- *Single sign on* : It reduces the security administration effort associated with administrating web-based access to multiple systems, but simultaneously introduces additional risk in that an incorrect assignment of access may result in inappropriate access to multiple systems.
- *Data content quality* : As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.
- *Privacy and confidentiality* : Regularity and governance issues surrounding the increased capture and visibility of personal information, i.e. spending habits.

### 7.5.1 Why do ERP projects fail so often?

At its simplest level, ERP is a set of best practices for performing the various duties in the departments of your company, including in finance, manufacturing and the warehouse. To get the most from the software, you have to get people inside your company to adopt the work methods outlined in the software. If the people in the different departments that will use ERP don't agree that the work methods embedded in the software are better than the ones they currently use, they will resist using the software or will want IT to change the software to match the ways they currently do things. This is where ERP projects break down.

Political fights erupt over how or even whether the software will be installed. IT gets bogged down in long, expensive customisation efforts to modify the ERP software to fit with powerful business barons' wishes. Customisations make the software more unstable and harder to maintain when it finally does come to life. Because ERP covers so much of what a business does, a failure in the software can bring a company to a halt, literally.

## **7.20 Information Systems Control and Audit**

The mistake companies make is assuming that changing people's habits will be easier than customising the software. It's not. Getting people inside your company to use the software to improve the ways they do their jobs is by far the harder challenge. If people are resistant to change, then the ERP project is more likely to fail.

### **7.6 HOW DOES ERP FIT WITH E-COMMERCE?**

ERP vendors were not prepared for the onslaught of e-commerce. ERP is complex and not intended for public consumption. It assumes that the only people handling order information will be your employees, who are highly trained and comfortable with the tech jargon embedded in the software. But now customers and suppliers are demanding access to the same information your employees get through the ERP system - things such as order status, inventory levels and invoice reconciliation, except they want to get all this information simply, without all the ERP software jargon, through your website.

E-commerce means IT departments need to build two new channels of access into ERP systems, one for customers (otherwise known as business-to-consumer) and one for suppliers and partners (business-to-business). These two audiences want two different types of information from your ERP system. Consumers want order status and billing information, and suppliers and partners want just about everything else.

The bottom line, however, is those companies with e-commerce ambitions face a lot of hard integration work to make their ERP systems available over the Web. No matter what the details are, solving the difficult problem of integrating ERP and e-commerce requires careful planning, which is the key to getting integration off on the right track.

### **7.7 LIFE AFTER IMPLEMENTATION**

Effective use of ERP is a direct result of steps taken at the time of implementation toward preparing the organization. Change integration has to be necessarily embedded in the task list for any ERP implementation. The main tool for this is the process of communication in all forms-written, oral, workshops, meetings, etc. The process should start quite early, by educating all layers of the management on the particular ERP product, its relevant functionality, limitations and benefits.

Also, at the start of the project, the critical success factors (CSFs) for the company as a whole should be listed. These should be drilled down to CSFs for respective functionalities or departments. From these CSFs, performance measures required to address these CSFs should be culled out. The numeric figures against these performance measures can be classified as the Key performance Indicators (KPIs). The process of firming up the above is usually done through workshops. This has to be completed before the processes to be configured on the ERP are drawn up.

Envisioning the processes to be configured on an ERP is the critical portion to ensure user buy-in during the post-implementation phase. There are various ways this could be done, but what is important is the following should be born in mind. The important end-users should be



involved in evolving the process. This should be done keeping the ERP functionality in mind. The KPIs derived from the organizational goals and CSFs should be kept in mind too.

Having evolved the processes while the configuration, construction and implementation are in progress, the organization needs to ready itself for the post-implementation period. Some of the tasks that are to be performed are:

- Develop the new job descriptions and organization structure to suit the post ERP scenario.
- Determine the skill gap between existing jobs and envisioned jobs.
- Assess training requirements, and create and implement a training plan.
- Develop and amend HR, financial and operational policies to suit the future ERP environment
- Develop a plan for workforce logistics adjustment.

**7.7.1 Post-implementation blues :** While the above checks would take care of most post-implementation blues, certain problems are bound to be encountered. The major task is to monitor the KPIs and take the correct business decisions to improve them. In most Indian organizations, however, these indicators may be non-existent before the implementation. So the immediate task is to set attainable goals. However, this may be unrealistic to be achieved in the first go. The more realistic path would be to have a stretched target to be achieved in phases. Similarly, certain KPIs, though existing in the system, are better monitored and controlled after the ERP system attains maturity.

The other major problem faced is that, more often, for reasons of data transfer or just to be safe, it is decided that the legacy systems run for a period of time. Many a time, the users, having a choice, display resistance to change. The only panacea to this is a strong management resolve to insist on implementation of the system. Even with all the preparations during the implementation, during post-implementation there will be need for course correction many times. It may be because of the following reasons :

- A change in the business environment requires a change in the CSFs, resulting in a new or changed set of KPIs necessitating reconfiguration.
- A review indicates a need for change in some process.
- Vision changes in the ERP and improvements in hardware and communication technology necessitate changes.
- New additions to the business require extra functionality.

The international trend is to outsource the activity of maintenance and upgradation to enable the company to concentrate on its core business activity. Correcting its course can be done by going in for an ERP audit, which is an emerging trend. This audit could be general in nature or very specific. One of the specialized areas is to evaluate the security, authorization and controls. An audit could be triggered either by a perceived inadequacy in terms of return on investment or by a simple desire to improve existing systems.

## 7.22 Information Systems Control and Audit

To conclude, investment in an ERP system is substantial for any organization. While implementation itself is a challenge, the ultimate test is in proper usage. This can be ensured by integrating the business objectives with the ERP functionality during the implementation stage. The limitations of an ERP must also be recognized to get the right expectation. A periodic independent audit would be a proper mechanism for an organization to ensure that it gets the best return on investment.

### 7.8 SAMPLE LIST OF ERP VENDORS

This is only a sample listing of ERP Vendors. It may not be comprehensive.

**Baan (The Baan Company)** : In 1994, a Boeing order catapulted Baan into the global ERP vendor league. Baan has held and built on this position with other major orders and a strategy for simultaneously addressing manufacturers from the largest global player to the smallest ERP user. Baan has a sound technology base and a broad functional scope. It offers credible tools for business process analysis linked to implementation of its software, and is launching workflow capabilities to build on this.

**Business Planning and Control System (BPCS)** : BPCS remains the market-leading manufacturing ERP solution in terms of sites. SSA only targets manufacturing companies. It offers good functionality for process, discrete and Kanban manufacturing, but not for project management. It lags in the areas of process-oriented implementation tools and workflow. Some users are concerned by SSA's stated objective of being the object oriented technology leader. SSA has made mistakes, its developments have not run to schedule and it has incurred enormous losses. However, there are signs that it has turned the corner.

**Mapics XA (Marcam Corporation)** : Mapics has been around for a long time, and many view it as a dated, legacy application. Mapics is a suite of 40 modules with 'good enough' functionality. Many users report that Mapics now offers more functionality than they need. It offers robustness, easy implementation and reasonable value for money.

**MFG/Pro (QAD)** : QAD's strength is in repetitive manufacturing. Originally designed to meet the MRP II criteria published by Oliver Wight, MFG/Pro's reputation includes reliable manufacturing functionality and straightforward implementations.

**Oracle Applications (Oracle)** : Oracle's Manufacturing Applications will tempt IT departments, with its vision of Internet-enabled, network-centric computing. As a one-stop shop, it offers the database, tools, implementation, applications and Unix operating systems running on a wide choice of hardware. Oracle has invested heavily to enhance functionality but production managers should still check that it delivers all the functionality they want.

**Prism (Marcam Corporation)** : Prism is a specialist process manufacturing solution for the AS/400. Its production model, which is akin to a flowchart, handles process industry problems elegantly. Although out dated, it does the job.

**R/3 (SAP)**: In five years, R/3 is the market leader in new sales. Its philosophy of matching business processes to modules is excellent. It offers a wide range of functions and its major shortcomings are yet to be identified. However, it remains complex, because it offers much;

few people know how to get the best from it. R/3 will be around for a long time; few people get fired for buying it.

**System 21 (JBA)** : JBA develops and implements System 21. Its software license revenues are small compared to those of other major ERP vendors. Nevertheless, it is a world player. It does not offer leading-edge technology, but does offer a rugged, reliable manufacturing solution.

## 7.9 ERP SOFTWARE PACKAGE (SAP)

SAP AG has developed an ERP package called SAP. It will be worthwhile to look into this package in detail because SAP looked at the entire business as a single entity when developing this software. Therefore, it is a unique system that supports nearly all areas of business on a global scale.

SAP has a number of Application Modules in the package. Some of these modules are shown in figure 2 given earlier.

1. Financials.
2. Controlling
3. Investment Management
4. Treasury
5. Integrated Enterprise Management
6. Sales and Distribution.
7. Production Planning and Control.
8. Materials Management
9. Human Resources Management.
10. Internet and Intranet.

Each of these modules has a number of components, each taking care of specific functionalities of any normal business. Let us examine these modules and the components within them in detail.

**7.9.1 Financials** : The financial application components cover all aspects of financial accounting.

**Financial Accounting** : Company-wide control and integration of financial information is essential for strategic decision making. SAP financial accounting covers an international framework of multiple companies, languages, currencies and charts of accounts. Central tracking of financial accounting data is possible .For example when raw materials move from inventory to manufacturing the system reduces quantity values in inventory and simultaneously subtracts currency values for inventory accounts in the balance sheet.

Financial accounting component complies with international accounting standards such as

## 7.24 Information Systems Control and Audit

GAAP and IAS. It also fulfills the local legal requirements. Though financial transactions are processed individually, they are integrated with all other relevant financial areas.

**General ledger** : General Ledger is essential both for financial accounting system and for strategic decision making. The functions of General Ledger are as follows :

1. Active Integration with business processes in R/3 logistics and in the accounting sub ledgers.
2. Serves as a central pool of financial data for financial reporting as well as for other accounting areas.
3. Supports all the functions needed for financial accounting systems such as :
  - a. Flexible structuring of chart of accounts at group and company level.
  - b. Distributed application scenarios using Application Link Enabling(ALE).
  - c. Real time simultaneous update of sub ledgers and the general ledger.
  - d. Elimination of time consuming reconciliation.
  - e. Parallel views of data in both general ledger and managerial accounting applications.
  - f. Provides summary information from other components at a user-defined level of detail by creating a special ledger.
  - g. Create data summaries that can be used in planning, allocation, distribution and reporting.
  - h. Can take advantages of more functions in GL and in Cost Centre Accounting.
  - i. Can create own database tables and define non-standard fields to suit specialised accounting or reporting requirements.

**Accounts receivable and payable** : R/3 offers a financial overview of global business partner relationships in the Accounts Receivable and Payable sub ledger functions. These sub ledgers are integrated both with the G/L and with areas in sales and distribution(SD) and materials management(MM) where financial data originates. Accounts Receivable and Payable transactions are performed automatically when related processes take place in other R/3 SAP components.

This component uses standard business rules for procedures ranging from data entry and reporting to processing payments and bank transactions.

Accounts receivable and payable functions include the following:

Integration with Internet.

Document Management.

Support for EDI processing.

Integration with cash management.

Flexible reporting using Customer and Vendor Information System.

Flexible dunning.

Enterprise-wide credit management with workflow integration.

Payment automation with EFT and cheque processing, and document parking with various approval procedures.

**Fixed asset accounting** : Asset Accounting manages the company's fixed assets. With the financial Accounting, fixed asset accounting serves as a sub ledger to the General Ledger, providing detailed information on asset related transactions.

Main features of asset accounting are:

Country specific charts of depreciation complying with local legal requirements.

Full support throughout the asset life cycle from acquisition to disposal.

Depreciation simulation and interest calculation.

Integration with Project Management.

Order accounting for management of Capital Assets.

Integration with plant maintenance for management of machinery and equipment.

Management of leased assets and assets under construction.

Mass processing with Workflow integration.

Interactive Reporting.

### 7.9.2. Controlling Cost

**Overhead Cost Control** : This component focuses on monitoring and allocation of overheads. This cost cannot be directly assigned to the products manufactured or services given. Over head cost allocation needs a transparent method of allocation.

**Cost centre accounting** : Cost centre accounting analyses where overhead occurs within an organisation. Costs are assigned to the sub areas of the organisation where they are originated. A number of methods are available for allocating posted amounts and quantities.

Activity accounting permits allocation of costs to products based on cost resources enabling assignments which were not possible.

**Overhead orders** : Overhead order collects and analyzes costs based on individual internal measures. It can monitor and automatically check budgets assigned to each measure.

**Activity based Costing** : Activity based Costing is developed as the response to the need for monitoring and controlling cross departmental business processes in addition to functions and products.

The system automatically determines the utilisation of business processes by products, customers and other cost objects based on the cost drivers taken from the integrated accounting environment.

**Product cost control** : Product cost control determines the costs arising from the manufacture of a product or providing a service. A control plan and standard values serve in

## 7.26 Information Systems Control and Audit

evaluating warehouse stock and for comparing revenues received with costs. In addition, the values in product cost controlling are crucial for determining the lowest price limit for which a product is profitable. It is possible to study the cost patterns by simulating the effects of changes in different production methods for a particular product and arriving at the lowest cost method.

**Cost Object Controlling** : This helps in monitoring manufacturing orders.

Integration with R/3 Logistics component results in a logistical quantity flow that provides instant information on actual cost, object costs, allowing ongoing cost calculations at any time. Follow up calculations determine and analyze the variances between the actual manufacturing costs and plan costs resulting from Product cost planning.

The system can evaluate work in process and post results to Financial Accounting.

**Profitability analysis** : Profitability Analysis examines sources of returns.

As part of sales control, Profitability Analysis is the last step in cost based settlement, where revenues are assigned to costs according to market segment.

The Market segment can be defined between products, customers, orders, sales organisations, distribution channels, and business areas and evaluate it according to contribution and revenue margins. Information from Profitability analysis can be used for determining prices, selecting customers, choosing distribution channels etc.

### 7.9.3. Investment Management

**Corporate wide budgeting** : Investment management facilitates investment planning and budgeting at a level higher than specific orders and projects.

Specific investment measures are assigned to different levels of hierarchy and therefore available funds, planned costs, and actual costs already incurred from internal and external activities can be made up to date at the appropriate levels.

The investment program allows to distribute budgets which are used during the capital spending process. The system helps to monitor and prevents budget overruns.

**Appropriation requests** : Investment management provides tools to plan and manage projects at the earliest stages. For this, first an appropriation for spending for the project is to be made. It is also necessary to define an evaluation and approval process during which the system keeps a detailed history of the status of the appropriation request. When the request is approved for implementation, the data from the appropriation request is transferred to the investment. It is also necessary to enter the planned values with its different variants in the appropriation requests.

**Investment measures** : Investment measures that are to be monitored individually can be represented either as internal orders or as projects.

These orders or projects provide the means for actually carrying out the capital investment.

They serve as the objects for collecting primary and secondary costs, for calculating overhead and interest, for managing down payments and commitments, and for handling other related tasks. As a result of having an asset under construction assigned to it, the investment

measures also benefits from all of the required asset accounting functions. Settlement is both flexible and almost fully automatic.

This kind of settlement ensures complete integration with business planning and control and provides consistently up-to-date values.

**Automatic settlement to fixed assets** : In this module, the system automatically separates costs requiring capitalisation from costs that are not capitalized, debiting the correct costs to the assets under construction. For different accounting needs, the system can use different capitalisation rules for making this split.

At completion, the investment measure can be settled to various receivers by line item.

Asset accounting provides precise proof of origin for all transactions affecting acquisition and production costs.

**Depreciation Forecast** : Balance sheets and cost planning are always based on current values. Planned depreciation values for investment measures and appropriation requests can be transferred directly to ongoing overhead cost planning. The system recalculates expected depreciation amounts whenever planning data is updated.

#### 7.9.4. Treasury

**Cash Management** : The Cash Management component allows the analysis of financial transactions for a given period. Cash management also identifies and records future developments for the purpose of financial budgeting.

In Treasury cash management, the company's payment transactions are grouped into cash holdings, cash inflows and cash outflows. Cash Management provides

- a. Information on the sources and uses of funds to secure liquidity to meet payment obligations when they become due.
- b. Monitors and Controls incoming and outgoing payment flows.
- c. Supplies data required for managing short-term money market investment and borrowing.
- d. Enables to know current cash position, short term cash management and medium and long term financial budgeting.
- e. Enables analysis of liquidity.
- f. Helps in cash management decisions.
- g. In bank accounting, helps in electronic banking and control functions for managing and monitoring of bank accounts.
- h. The liquidity forecast function integrates anticipated payment flows from financial accounting, purchasing and sales to create a liquidity outlook from medium to long term.
- i. Covers foreign currency holdings and foreign currency items.

## 7.28 Information Systems Control and Audit

**Treasury Management** : Before making any concrete financial decisions, it is necessary to consider current liquidity, currency and risk positions and consider the prevailing conditions on the money and capital markets. The treasury management component offers functions for managing financial deals and positions from trading through to transferring data to Financial Accounting.

Treasury management also supports flexible supporting and evaluation structures for analysing financial deals, positions, and portfolios.

For short term liquidity and risk management, one can use money market or foreign exchange transactions to smooth out liquidity squeezes and gluts or to eliminate currency risks. Securities and loans come in the medium and long term.

Active management of interest rate and currency risks is facilitated by derivative financial instruments. The trading area contains functions for recording financial deals, exercising rights, performing evaluations and calculating prices.

In back office processing, the additional data required for processing deal confirmations is entered. These deals can be account assignment and payment details and generate automatic confirmations. Position management functions such as securities account transfers or corporate actions relating to securities are supported in the back office area.

The General Ledger is updated in the accounting area, which also offers flexible payment processing functions in addition to valuation and accrual/deferral methods.

By using common organisational elements throughout, various organisational structures can be represented in the system such as central enterprise-wide treasury department or 'in-house banks'.

This also ensures full integration of treasury with other SAP components.

**Market risk Management** : Market risk management is a process which involves a complex feedback loop encompassing data collection, risk measurement, analysis, and simulation as well as active planning of financial instruments.

This process fits closely into other treasury and corporate functions.

Market risk management acts as an integrated, central risk control station with monitoring and management functions. Access to information on current and future cash flows and on financial deals already processed is an absolute necessity. Cash management which pools all cash flows from the business sectors such as sales and distribution or purchasing forms the basis.

Consequently all cash flows from the company's operating business can be accessed for the purpose of risk management. Furthermore, all financial transactions managed in Treasury Management can be evaluated together with the cash flows generated by various operating divisions.

The component provides various measurements for analysing and assessing interest rate and currency risks. Market to market, effective rate and effective yield calculations are based on up-to-the minute market data, uploaded via data feed, and financial transactions or positions.



By simulating the market data, one can determine the risk structure of 'What If' analysis (such as crash scenarios or worst case scenarios). It is also possible to measure and compare the impact of alternate strategies using simulated transactions.

**Funds Management** : Funds Management supports the funds management process from budgeting all the way through to payments, including monitoring expenditures, activities, resources and revenues.

Budgeting function serves many useful functions such as:

- a. Original Budget approval and release.
- b. Budget supplements, returns, transfers.
- c. Can cover as much management levels as required.
- d. Fund centres and their hierarchical structures provide a base for top down budgeting and represent responsibility areas within the budget control.
- e. Commitment management system enables to control various funds commitments and determine how much of the budget has already been utilized via availability checking.

The information system can supply information at any time depending on when, where and how the funds commitment arose.

- f. Analyses by responsibility area and commitment items allow identification of any budget bottlenecks.

### 7.9.5. Enterprise Controlling

Enterprise can be managed by using an Integrated Enterprise Management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called Enterprise Controlling (EC).

It is easy to transfer the data to the EC module to automatically set up consolidated financial statements including elimination of inter-company transactions, currency translation etc.

Enterprise Controlling consists of 3 modules.

1. EC-CS.
2. EC-PCA
3. EC-EIS.

**1. EC-CS** : This component is used for financial statutory and management consolidation which also allows fully automated consolidation of investments-even for many companies and complex investment structures.

**2. EC-PCA** : Allows to work with internal transfer prices and at the same time to have the right values from company, profit centre, and enterprise perspectives in parallel. Any transaction that touches an object such as customer order, plant or cost centre allocated to a profit centre will be automatically posted to EC-PCA.

### 7.30 Information Systems Control and Audit

It is also possible to take data directly from EC-PCA to EC-CS consolidation to prepare complete financial statutory statements and management reports in parallel. This provides the management with a consistent view of external and internal financial management reports.

**3. EC-EIS (Executive Information System) :** Executive Information System allows to take financial data from EC-PCA ,EC-CS or any other application and combine with any external data such as market data, industry benchmarks and /or data from non-SAP applications to build a company specific comprehensive enterprise information system .

**Enterprise Controlling :** It allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure . It helps to speed up provision of business control information by fully automated corporate reporting from operative accounting via financial consolidation to management reporting.

From EC-EIS top-level reports, end users can drill down to more detailed information within EC or any other R/3 application.

EC can work with data from SAP and non-SAP sources.

#### 7.9.6. Product Data Management (PDM)

PDM supports in creating and managing product data throughout product lifecycle. SAP supports two basic scenarios in PDM environment.

1. To support a third party PDM system supported by SAP's complementary program to the R/3 system.
2. To implement the single source PDM solution provided within the R/3 system.
3. PDM keeps track of all master data.
4. The Document management system allows managing a wide range of technical, commercial and administrative documents consistently. Original documents can be linked to all types of objects in the R/3 system (for example material master records, BOMS, or change master records).External optical archiving system can be accessed from this system.
5. PDM organises the design and change processes. This feature is known as Engineering Change Management and is fully integrated in the logistics process chain of company.
6. Engineering Change Management ensures that planned changes to master data are automatically available in the productive functions of sales and distribution , demand management and MRP, production control, product costing, quality management, materials management at any given time.
7. PDM gives product structure information at a glance.
8. BOM management solves the problem of distinguishing between engineering BOMS and production BOMS in the company.
9. To maintain the distinction between different uses of a BOM, separate BOMS can be created or different views on the same BOM can be developed.
10. PDM are supported for large product development projects in the R/3 project system.

### 7.9.7. Sales and Distribution

The system's Sales and Distribution application offers access to real-time, online information from sales support to the billing process.

The sales support component has easy to use tools to manage information on sales leads, sales calls, inquiries, quotations, marketing campaigns, competitors, and their products.

Sales and marketing personnel can access this data at any time to perform sales activities or carry out direct mailings. Sales support not only makes existing sales process more efficient but it can identify new sources of business as well.

Order entry in the system is automatic. By referring the information in the simple user interface, the system assembles information such as terms of payment and identity of delivering plant. It then programs this information in the sales order. It deals with materials very easily. The materials can be entered manually and then customer based product proposals can be chosen.

It is also possible to configure a product to meet customer requirements.

Pricing is carried out automatically in the sales order. To determine relevant predefined prices, surcharges and discounts, the system works from price lists and customer agreements or it determines an amount according to the product, product group, or product cost. The pricing function is very flexible and can manage even the most complicated price structures. The pricing information can be maintained with data from sales promotion.

The system carries out a dynamic credit limit check checking against credit, financial and sales data to verify the customer's credit limit. The system can be set automatically to alert credit or sales personnel when a sales order fails to realize.

The system can perform availability check. It is run using materials management module (MM) and Production Planning Applications. It verifies that sufficient quantities of items are available to satisfy a sales order. If the requested delivery date cannot be met, the system determines when the desired quantities will become available so that a new date can be quoted to the customer. It is possible to ensure delivery in multiple locations. In the case of customers requiring specific quantities of products, the make-to-order production features can be used.

Sales and Distribution supports a wide range of contracts from general to more specific contracts.

The features of this module are :

- a. Can specify delivery quantities, delivery dates, and prices.
- b. Scheduling agreements and more complex requirements such as just in time delivery schedules are supported.
- c. The products can be followed up with the service management components with functions such as call management, warranty management, service and maintenance contract processing.

## 7.32 Information Systems Control and Audit

**Shipping Management System** : This offers easy to use functions for managing picking, packing and loading tasks and monitoring delivery dead lines. The system provides a list of all sales orders due for delivery and gives the option of delivering the order completely or partially, individually or collectively. It is also integrated with Warehouse Management System.

**The Transport Module** : The transport module offers functions for transportation planning and processing as well as monitoring and control functions. The items can be sent by land, air and sea .The transportation chain are for individual shipments or stop off shipments involving several deliveries and several destinations. It is possible to select forwarding agents and track shipments.

**Foreign Trade Processing** : SD offers support for foreign trade processing offering automated export control to determine whether specific products can be exported to a particular country, to a specific customer, and at a specific time. The system handles all the custom forms automatically. To declare shipment of goods to the government authorities, the system collects all the data required for the declarations and create the necessary forms. Preference agreement is another feature. It helps to manage the shipments of products that are eligible for custom tariff preferences, track the origin of component parts and assign a tariff classification to materials.

**Billing** : On the basis of orders and deliveries, the system automatically carries out billing for all due items. The system then creates an invoice, debit memo, or credit memo for each item or collectively for several transactions. The billing document can be send directly by mail, fax or EDI.

Revenues and Receivables are immediately visible in the Financial Accounting and Controlling components. It can also process rebates based on a customers purchase volume.

**Sales Information System** : The information in the Sales Information is always up to date. The information is displayed by customer, material, or region in an easy to use interpret list or informative graphic.

This information also enables to address market trends and changes.

### 7.9.8. Production Planning and Control

This module is used for planning ,executing and controlling production. This covers the complete production process starting from creation of master data, production planning, MRP, capacity planning, production control and costing.

#### **Production planning modules :**

**Sales and operation planning (SOP)** : Using Sales and operations planning, it is possible to create realistic and consistent planning figures and data on the basis of expected sales or other key figures .

In Demand management, these planning figures are split down to product level and a demand program is created.

In Materials Requirement Planning (MRP), the system calculates the quantities and procurement dates for the necessary materials, right down to the raw materials.

It is also possible to do capacity planning ahead of the planning phase.

**Production control modules** : Depending on the method of production, various choices are available like Production Order Processing, Repetitive Manufacturing or KANBAN production control is available.

Production order is primarily a tool for discrete job-shop production. It provides extensive status management functions, controlling per order as well as various operation-related functions. Repetitive manufacturing is designed for manufacture of products that are typically produced repetitively on a particular production line over a longer period. Here production planning and control as well as controlling are usually carried out based on periods and quantities.

Capacity planning is integrated with production order processing as well as with repetitive manufacturing.

**Quality Management** : This interfaces with PDC systems , distributed control systems, laboratory information systems as well as extensive data analysis functions in the Open Information Warehouse are all integrated with Production Control.

Production Planning covers the complete production process from the creation of master data to production planning, MRP, and capacity planning right down to production control and costing. It can be used in all sectors of industry and provides a whole range of production methods from make to order production / variant processing to repetitive manufacturing /mass production.

Production Planning also provides an easy to use Information System that one can adjust to suit particular needs.

**Project System** : Project objects and business areas involved form a multifaceted network of which Project Management is one part. This is called WBS (Work Breakdown Structure).

R/3 project system matches this network of relationships by permitting any link between project management and commercial information processing.

Work breakdown structures can use the project system in many different areas such as Investment Management, Marketing, Software and consultancy services, Research and Development, Maintenance tasks, Plant engineering and construction, make to order production etc

The central structures in the Project system are work breakdown structure and networks with their activities and milestones. These structures can be used for sales and distribution and with BOMS for production and procurement to model complex projects in the system.

Project systems graphical interface can be used to create structures quickly and easily. The following additional functions are also available.

- Cost and Schedule planning.
- Integration with other modules i.e., planning of resources in cooperation with Purchasing, Inventory Management and Materials Requirement Planning.
- Assigning human resources in individual employee or group terms.

## 7.34 Information Systems Control and Audit

- Checking and monitoring availability of funds, capacities, and materials.
- Controlling project expenditures using tools for approving and releasing projects.

SAP business workflow is available to improve communications within large projects.

**Project Information System** : Project information system contains Listings and Graphical Analysis to supply all the information needed on the planned budget cost and actual costs, revenues, commitments, schedules of payments received and made and resources.

### 7.9.9. Materials Management

The system's materials management module contains all functions required to simplify business processes in Requirements planning, Purchasing, Inventory Management, Warehouse management and Invoice Verification. It also introduces a high degree of automation into standard procedures.

**Purchasing** : Consumption based planning provides one with up-to-the minute order proposals for purchase requisitions, based either on reorder levels or on forecast data. Logistics applications such as Sales and Distribution, Plant Maintenance, Production Planning or the Project system can also require materials or services to be procured externally.

Individual departments enter purchase requisitions manually. The system passes these purchase requisitions directly to purchasing application where they are converted into purchase orders. Buyers use tools from special purchasing master data, requests for quotations and outline agreements. The prices can be compared during the procurement process or automate vendor selection or order creation processes. Purchase documents can be part of a release and approval procedure before they can be further processed. The purchase orders can be send to vendors on paper or electronically (by EDI for example).The Purchase order allows to monitor status of order and track deliveries or invoices already received.

**Inventory Management** : The stock of materials is managed on a value and quantity basis in Inventory Management.

This application component supports all the most common types of receipts, issues, and stock transfers and allows managing special stocks (such as batches, consignment stocks, project stock, returnable transport packaging, or components with a subcontractor).

Goods movement postings automatically result in an update of values in Financial Accounting, Asset Accounting, and Controlling. The system also supports a number of convenient aids for entering the data and with a variety of inventory valuation such as LIFO (Last in First out) or FIFO (First in First out) for balance sheet valuation.

**Warehouse Management** : The Warehouse Management (WM) module provides flexible automated support that enable to process goods movements and maintains current records of all materials stored in highly complex warehousing structures. Using advanced put-away and picking techniques, WM optimizes material flow and capacity in the warehouse storing goods in the most favourable locations so that they are readily available when needed. WM can be

interfaced with hand held terminals, bar code terminals and many other automatic processes that are available in WM component.

**Invoice Verification** : Invoices received on paper or EDI are checked automatically by the system. If an invoice is entered referring a purchase order, the system can automatically generate the invoice it expects to receive. An invoice is automatically blocked for payments if variances occur that are not allowed such as in the delivery date, the quantity delivered and agreed price.

The Evaluated Receipt Settlement (ERS) functionality allows to do away with vendor invoices altogether. The system automatically creates invoices periodically based on the goods receipt posted in the system for purchase orders.

Invoice verification provides a special method of entering vendor invoices, which is much faster than standard procedures.

MM application comprises countless additional functions that can help shape the materials management system efficiently. For example

1. A pipeline material that flows directly into the production process can be entered in the system for an order, a cost centre or a network and is managed in a manner similar to consignment stock.
2. Stock transfer function can be used to model stock movements among different plants in the system.
3. It is possible to enter a stock transport order with or without a purchase order or delivery.
4. Transport orders are made with a whole suite of functions, such as shipping point determination and route determination.
5. To ensure smooth and efficient foreign trade processing, the necessary data can be prepared for export and import activities.

**Inventory Control using Purchase Information System** : With the purchasing information system, all the facts and figures necessary for negotiating with vendors are at hand. Choosing which data is to be included in reports and how the information is to be presented becomes easy.

It is also possible to determine stock values, to find out inventory turn over rates and carry out analysis.

**Quality Management** : Quality management module is tightly integrated with all modules of an enterprise. Implementing it in a logistics system provides a number of advantages. Some of these advantages are :

1. Verification of the quality of procured goods.
2. Reduction of administrative tasks through company-wide quality planning.
3. Recording of all pertinent quality data during the quality inspection.

## 7.36 Information Systems Control and Audit

4. Using the comprehensive functions for quality control.
5. Managing problems efficiently through quality notifications.
6. Creating a quality management information system.

**Plant Maintenance** : The various components of a plant maintenance module are

1. Structured technical systems.
2. Maintenance planning.
3. Systems for technical and cost accounting data.
4. Creation of a plant maintenance information system.

**Service Management** : R/3 system's service management module provides highly integrated functionality and is suitable for many types of industries.

The following are the main features of Service management module.

1. Installed base management.
2. Service agreements
3. Call management
4. Invoicing and billing
5. Service information system.

### 7.9.10. Human Resource Management (HR)

HR provides comprehensive process driven solutions that can address organisation's human resources needs worldwide. The module consists of various components such as Personnel Management, Personnel administration, Recruitment management, Travel Management, Benefits administration, Salary administration etc. Let us examine these in detail.

**Personnel administration** : Information is not owned by specific departments but is shared by multiple entities across an organisation. The package eliminates duplicate entries across an organization. It offers a global and fully integrated data without compromising the control over the individual segments of the operations.

**Employee master Data** : This is a centralised data-base with integration to multiple components for processing employee information.

SAP R/3 contains "information types" for storing any desired information about employees. One can enter data through the time saving "fast entry" feature processing data in two modes-online or background.

Original documents can be scanned into HR for optical storage with SAP's Archive link.

**Recruitment Management** : SAP has designed the recruitment component, which enables to place people in the right job at the right time and with the right skills and education. This



component contains processes for managing open positions/requisitions, application screening, selection and hiring, correspondence, reporting and cost analysis.

**Open positions :** The R/3 HR recruitment component allows direct access to data stored in other components of HR including personnel administration, payroll and personal planning. These links eliminate duplication of data entry and improve productivity.

Some examples of shared data related to job openings include position open date, location and reporting specifics, job descriptions and skills and education requirements. This information can be used for both internal job postings and external advertisements with newspaper, magazines, or recruitment firms.

**Selection and hiring :** HR recruitment interfaces directly with Microsoft word for windows to generate standard applicant letters. SAP's office communication link is used to send e-mail messages to internal applicants. SAP provides tools to analyse costs during advertising and interviewing for each open position.

With HR recruitment component, one can effectively manage job openings, applications and applicant data, costs and hiring process. Once a selection has been made and an applicant has been hired, the data gathered during the recruitment process becomes new information.

**Travel Management :** HR travel management allows the processing of a business from start to finish – from the initial entry through to posting in Financial accounting and controlling. This includes subsequent corrections and all retroactive accounting requirement. Travel data can be entered by a person travelling or by the relevant department before or after the trip. The entry of a travel request automatically generates a work flow that makes the work of HR department easier.. Business specific, employee specific and country specific trip provisions can be implemented via system settings.

**Benefits Administration:** This component provides capabilities and flexibility to effectively manage benefits programmes for diverse employee populations. It can maintain unlimited number of benefits types and individual plans that are offered to employees. Also, benefits groups based on specific employee demographics can be established.

**Personnel cost planning :** HR organization and planning assists to maintain an accurate picture of organization's structure no matter how fast it changes. A graphical environment makes it easy to review additions or changes in employee positions. Planning features assist in making graphical organization chart, staffing schedules by head counts percentage, working hours, job and work centre descriptions.

R/3 personnel cost-planning enables to perform cost comparisons between target and actual personnel costs and create cost previews. It is possible to forecast wages, salaries and other cost elements for open and filled positions based on simulated, planned or actual payroll figures. The results can be displayed in R/3 business graphics which is linked to Microsoft Excel in a spreadsheet format. The results are transferred to SAP R/3 cost accounting.

## 7.38 Information Systems Control and Audit

### 7.9.11. Payroll accounting

R/3 HR payroll accounting addresses payroll functions from a global point of view. It is possible to centralize or decentralize payroll processing based on country or legal entities. It also enables to establish business rules without modifying existing payroll.

**Payroll processing** : Payroll accounting date reminder feature provides with an online tickler system that notifies when transactions are due for processing. When the process is completed, a built-in audit trail date stamps the record for future reference. The system automatically creates a history record for every payroll transaction. It can create standard reports and user specific reports.

**Integration** : Payroll accounting maintains information on employees in a master file shared with all other HR components. R/3 system writes payroll data into controlling, financial accounting and logistics.

**Global solutions** : SAP R/3 has country-specific versions and therefore payroll accounting can fulfill language, currency and regulatory requirements.

**Time management** : Time management is a powerful tool that helps to administer and evaluate data related to time that the employees spend on working.

**Time data** : Time management manages works schedules efficiently and effectively by automatic schedule generation and allowing flexible definition of time models and schedules for each location and organizational level. It is possible to set flexible working hours and process work notices as times are recorded. Calculation for employee incentive wages is also available.

**Time evaluation** : The time evaluation component allows daily processing of employee time data. It is a flexible tool designed to handle complicated evaluation rules to fulfill regulatory requirements and determine overtime and other time related data. The time evaluation component stores organisation's business rules and automatically validates hours worked and wage types. The results of time evaluation can be shown on a time sheet.

**Time Management review** : With HR time management, special transaction capabilities designed to support time clerks in their daily tasks are available. Error handling feature makes necessary corrections.

**Integration and Interfaces** : Time Management is integrated with Payroll Accounting, Production planning, Plant maintenance, Project system, External services and Shift planning.

SAP has standardized communication channels and protocols for many external data entry systems. Plant Data Collection (PDC) serves as an integration tool linking plant system to all business applications. As employee, machine and work order details are received, PDC automatically assigns it to the appropriate system.

**Shift planning** : HR shift planning enables to arrange a target plan that can be drafted for any given period. Shifts can be planned taking into consideration all criteria including absence due to leave or sickness and employee requests for time off. A convenient planning board is provided for guidance when entering and copying shifts for any designated period of time. Temporarily assigning an employee to another organisational unit is also possible.

**Other additional components**, which are available with HR module, are

1. Profiling of qualifications of employees and matching with available positions.
2. Career and Succession planning of employees
3. Additional education and training programmes
4. Training and event management.
5. Training programs and business events
6. Registration and booking for training
7. Charge determination and invoicing.

Other SAP Components:-

1. Internal and external communications
2. SAP business workflow helps to distribute tasks automatically at the right time to the right employee
3. Employee self-service increases efficiency and service.

**7.9.12 Internet and Intranet** : The R/3 system offers a special Internet functionality for large number of business processes. It also gives an opportunity to advertise vacancies to potential applicants all over the world. The application itself could be carried out online by calling up an application form filling it out and returning it by e-mail. The application would be processed automatically in R/3 HR

An internal search activity to find the required employee information is also possible in R/3 HR.

**SAP Business workflow** : This component enables to create work routines. Business workflow coordinates and monitors business processes step by step. All users automatically receive a list of their tasks in their R/3 mail system inbox. Once the work is completed, the workflow starts the next predefined work-step and sends relevant messages. For example, in HR recruitment the following processes are automatic :

1. Submission of application forms
2. Planning and holding of interviews
3. Drawing up contract offers
4. Preparing appointments
5. Monitoring of rejected applications

A range of workflow techniques such as optical archiving mailing and office communication can be used at every stage. It has also included other business processes in R/3 business workflow component. It is also possible to create new processes suited to a particular business.

## 7.40 Information Systems Control and Audit

**Employee self-service** : HR department no longer has to perform time consuming and costly activities such as issuing information and maintaining data. The employees themselves carry out these functions. This enables to increase the quality of information in any organization.

**Conclusion** : The success of any organisation today depends on its ability to look at business in totality without being influenced by strict departmental boundaries. ERP, which is an integration of components such as Business models, Operating Processes, Control Processes, and Changing Strategic Business Processes, enables the Organization to realize its vision and objectives in an optimized way.

## 7.10 CASE STUDY

### 7.10.1 Videocon Group

**Getting into the groove** : Consolidation of information flowing in from a multi-branch factory and multi operation was the main driver behind the Videocon Group's decision to implement an Enterprise Resource Planning (ERP) package.

"For a multi-manufacturing, multi-branch company like ours, the one major essential was centralized and consolidated information that is available in a uniform manner across various levels in the organisation," says Pradip Kumar N Dhoot, President, Videocon International, the flagship company of the group.

"The factories were already working on legacy systems using an Intranet and collating information. But each factory and branch would use different software, varied platforms, which did not speak to each other. This not only resulted in huge inflow of data which could not be consolidated for analysis but also duplication of data," Videocon is a \$ 1-billion company. Even one per cent change in any data entry or analysis translates into millions and can sometimes wipe out the profits of the organisation. So they needed a system that would help them to be responsive and act fast.

Further, at some stage they wanted to share a common platform with their dealers so that they could access the company servers and database, get updates on issues relating specifically to them as well as the company on the whole.

**The mandate** : It was in 1998 that Videocon began evaluating ERP packages and roped in the Pune-based Ygyan Consulting to help select and implement an appropriate package. In August 1998, based on Ygyan's recommendations, SAP's ERP package was finally selected.

The issues that needed to be addressed included:

- Better inventory management and control.
- Improved financial reporting and control.
- Automation of certain tasks that were performed manually to increase productivity.
- Improved production planning.
- Better information on stocks at various locations.

- Using an integrated system as opposed to disparate systems at different locations, thereby eliminating errors of duplicate entries.
- More accurate costing of products.
- Better credit control.
- Improved cash flow planning.
- Automatic quality-control and tracking.
- Better after-sales-service.
- Better information and reporting to top management.

**Going about the implementation :** For the implementation, Ygyan first tied up with Siemens Information systems Ltd. (SISL) for a pilot project at the first site – Videocon Appliances Ltd. The modules implemented were finance and Control, Materials Management, Sales and Distribution, Production Planning and Quality Management.

Videocon International was next in line. The scope of the project included all modules mentioned above in addition to a Plant Maintenance module. The implementation was divided into two phases where the four factories went first, followed by marketing operations across the country. The factories are located in Aurangabad, Bharuch, Gandhinagar and Bhalgaon.

Factories (parent units) went live first, within a year, and have been live for the past two years. They decided to go with the factories first because they are situated close to each other, compared to the branches, which are scattered across the country.

During the implementation, connectivity was a problem. So Ygyan suggested a mix of leased lines, ISDN, VSATs and Internet connectivity to optimise the costs while ensuring enough speed for users connecting from remote locations.

The entire process took eight months, right from drawing up the blue prints, consulting, customising and training core teams. The Group almost invested in excess of Rs.25 crore for the implementation, including the ERP package, hardware, connectivity etc., excluding the maintenance charges.

The biggest question that they had to ask themselves was whether or not they wanted transparency. That's the first thing that comes to light once ERP is in place since ERP involves a top downward approach – from a sales person to the top management, everybody is accountable.

The most important issue in the implementation of any technology is the attitude of the employees, it has to change – from working for oneself to working as a whole for the organisation. Employees too had their own fears and apprehensions about the system. A strong fear was that of retrenchment as a result of the implementation. However, the company held adequate training workshops at central and state level. In the factories, various processes were documented using print and audio / video to facilitate training on new employees.”

## 7.42 Information Systems Control and Audit

On the whole, employee reaction was positive as people were already using computers and an Intranet to send information. The initial apprehension fell through once people started using the system.

**Lessons to learn :** There were a few areas in which they did face problems with the package, as it does not have modules specific to Indian requirements such as taxes, Letter of Credits (LCs), import clearance and product evolution. In fact, a product evolution module is very essential for a consumer durable company, as it is needed to develop products according to market feedback. For a durable company, a new development would cost crores and be spread across 18 months or so. A product evolution module can be of great help in this scenario, the company management feels.

**Looking ahead :** It was reported in October, 2001, that Ygyan is now in the process of rolling out SAP in all other group companies, one at a time. The company managers are also working with them in other IT initiatives, including e-business and Internet-based customer relationship management systems.

The next step will be to see how system can be extended to include the partners and dealers. But that will start only after six-eight months once the employees get completely comfortable with the system. CRM is another area that the company is interested in.

### 7.10.2 CASE STUDY/TELECOM

Company : AirTouch Cellular

Industry : Telecom

Solution Area : Financials

AirTouch Cellular is a subsidiary of AirTouch Communications, a global wireless communications company serving 6.7 million customers worldwide in the areas of cellular, paging, personal communications services (PCS) and Globalstar satellite system markets.

**Problem :** AirTouch's financial analysts, located in different functional groups in five geographic regions, were missing access to the same data, as well as timely access to information. Dated budget and actual numbers for each business unit resided in seven different systems, separating critical components of the Profit and Loss A/c and inhibiting analysts' ability to assess results. To further complicate matters, analysts in the field could not go to one universal place to retrieve the data themselves - they relied on the home office to deliver it.

The company wanted to set some critical financial objectives to help it remain competitive and increase market share.

AirTouch chose Oracle Corporation's online analytical processing (OLAP) tools to better control costs, analyze performance, evaluate opportunities, and formulate future direction. And to improve the basis for making decisions quickly and accurately with real-time, consistent data; to improve cost control, and to simplify and shorten the budgeting process.

**Implementation :** AirTouch Cellular looked at two other vendors before choosing Oracle, but neither could provide users with the hands-on ability to consolidate budgets, include actuals in

the process, or do what-if scenarios online. AirTouch Cellular's parent company also had a proven, successful track record with other Oracle applications and a corporate initiative to make Oracle the vendor of choice.

Oracle provided on-site expertise in the product, the concept, and the business to create a user-friendly system. The project came in on time and within budget, with very few post-implementation issues. Completing the entire implementation in eight months was quite a feat, given the many changes that occurred in that time frame, according to the company. Not only did the company convert to a new system, it completely overhauled the budget process and the P&L reporting format amid departmental and company reorganizations.

**Benefits :** It resulted into more than \$8 million in hard and soft dollar savings. Also, it reduced the length of the budgeting cycle and the number of people involved in the process, keeping the company financially competitive in a growing market. The system now provides online, real-time access to information.

Now, analysts can individually access the same data warehouse for current, real-time information for their analyses. This means the vice presidents from each business unit in the division now have the data they need—budget or actual—on a timely basis. Thus enabling business units to make better, faster business decisions based on more accurate information. Their increased understanding of the data helps them run their slices of the business more effectively, because they can now make real-time, online decisions that help them stay on budget or shift business direction.

### Self - Examination Questions

1. What is ERP? Would you consider ERP as a process in addition to software?
2. What are the major features of ERP?
3. What are the major components of ERP?
4. You have been asked to recommend to your client whether they should go for implementation of ERP system or not. What would be your process of arriving at the opinion?
5. What all would be the major benefits for a company using an ERP software?
6. Is Business Process Reengineering (BPR) a separate process from ERP? Justify your answer while explaining the various steps involving a BPR.
7. How can BPR improve functioning of finance and accounting department?
8. You have been asked to recommend ERP software from a shortlist of vendors. Prepare a checklist showing what all would you compare before arriving at the recommendation.
9. Discuss in brief, various key planning and implementation decisions for an ERP software?
10. What are the steps involved in implementation of an ERP package?

#### **7.44 Information Systems Control and Audit**

11. You have been asked to assess the total cost of implementing an ERP in your organisation. In addition to the direct software cost, what other costs would you include to arrive at the total cost of ownership and implementation of a successful ERP system?
12. Upon implementation of ERP every organisation is stated to migrate to a regime of new risk and governance issues. Identify the major risk and governance issues for an organisation that has implemented ERP.
13. What all safeguard would you take to ensure successful implementation of ERP?



# INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

---

## 8.0 INTRODUCTION

Technology has affected all of us at home as well as at the work place. Articles engineered with cutting edge technology are no longer items of prestige or luxury but essentials. As the business grows, no office can do without computers, networking, video conferencing etc. It is a natural fall out therefore to accept that technology has also impacted auditing. A subject that has evolved over time possessing its own standards, conventions as well as International Practices is not a subject that can be easily subjugated by an upstart like technology. The reality however remains that old practices and definitions no longer remain valid or even practical.

One major area is Internal Control which hitherto was the accepted backbone of good control has evaporated overnight by the desktop computer which has permitted one person to perform the function of many persons who were earlier members of the internal control. Worse, the batch controls of the Mainframe computing have also disappeared. The residual alternative therefore was to develop anew, standards for Information Systems. This chapter delves into some of the recommended and popular standards. Some have impacted domestic industry directly while some like HIPAA has primarily affected in India, Business Process Outsourced (BPOs) companies processing Health Information and other companies in India having interest in health industry and relations with entities of the same industry in USA.

Some modes of controls or standards are discussed in this chapter. Some of the important standards having more presence are discussed in detail while the rest are merely touched upon. The interpretation of the standards is given in this chapter since you need to be abreast with the standards permitting you to access detailed information should assignment related demand surface later. The common features in all of them can be summarized as follows:

1. Every organization that uses IT uses a set of controls, perhaps unconsciously, even if the “controls” are to let everyone have full access.
2. An ideal set of controls for a given organization should depend on the business objectives, budget, personality, and context of that organization.

## 8.2 Information Systems Control and Audit

3. The set of control objectives—as opposed to the set of controls—can and should be constant across organizations.
4. Each organization could use the same control framework to manage their particular controls to meet those constant control objectives.

### 8.1 IS AUDIT STANDARDS

Every profession has a unique repository of knowledge, which lends credence to its specialisation. The knowledge often forms the basis to define commonly accepted practices. Very often the technical competencies and skills of professionals are assessed against these practices. So the first step towards becoming a specialised professional is to gain a thorough understanding of this repository of knowledge. IS audit standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively.

Some of the standards discussed in this chapter by their year of birth are as follows:

Year	Standards
1994	COSO, CoCo
1996	HIPAA
1998	BS 7799
2000	COBIT,

Discussion on these is presented in the order of their current trend of popularity and not year of birth perhaps in recognition of marketing power that all persons and products possess!

As we study various standards we begin to see some relation of one with the other. All of them are not developed in the same time zone nor are they a replacement for each other. Each fulfilled its own pioneering task at the time of its introduction. However, one has to admit that one influenced the others which in turn influenced the next generation. This does remind us of the DNA where the genetic patterns are passed on to the succeeding generations. The various standards therefore do show a trait of earlier standards.

### 8.2 AAS 29 – AUDITING AND ASSURANCE STANDARD ON AUDITING IN A COMPUTER INFORMATION SYSTEMS ENVIRONMENT

AAS 29 issued by the ICAI established standards on procedures to be followed when an audit relating to accounting information is conducted in a computer information systems environment. The pronouncement outlines the procedures that an auditor entrusted with financial, operational and other conventional audit objective relating to accounting information should carry out while auditing in a computerised environment.

AAS29 requires the auditor to consider the effect of a CIS environment on his audit and discuss the risks and caution that an auditor should exercise while carrying out traditional

audit objectives in a computer information system environment and elaborates on the following:

- The auditor's responsibility in gaining sufficient understanding and assurance on the adequacy of accounting and internal controls that protect against the inherent and control risks in a CIS and the resulting considerations to be taken while designing audit procedures.
- The potential impact of auditing in a CIS on the assessment of control and audit risks.
- The auditor is required to determine the following factors to determine the effect of CIS environment on the audit arising from
  - The extent to which the CIS is used for recording, compiling and analysing accounting information.
  - The system of internal controls relating to the authorised, complete, accurate and valid processing and reporting procedures.
  - The impact of CIS accounting system on the audit trail.
- The standard also requires the auditor to have sufficient knowledge of the CIS and possess appropriate specialised skills to enable him to plan, direct, supervise, control and review the work performed.

Text of AAS 29 is found as an Annexure to Paper 2 : " Advanced Auditing and Professional Ethics" Volume-II, Final Course Study material.

### 8.3 BS 7799

BS 7799 is an International Standard setting out the requirements for an Information Security Management System. It helps identify, manage and minimize the range of threats to which information is regularly subjected.

Specification for information security management systems" constitutes what is known as BS 7799 from the British Standards Institute. The "Security Code of Conduct" from the British Government's Department of Trade and Industry was a originator from which grew BS 7799, which has, in turn, subsequently grown into ISO 17799. The Australian/New Zealand standard, AS/NZS 4444 is a very close adaptation of BS 7799.

BS 7799 Part 1 became an international standard (ISO/IEC 17799) in December 2000. It has been revised in line with ISO procedures. BS 7799 Part 2, although still a UK standard, it has been published as a national standard in many countries and is now itself at an advanced stage of international status.

From the outset, BS7799 focused on protecting the **availability, confidentiality and integrity** of organizational information and this remains, today, the driving objective of the standard. Though, it doesn't talk about protection from every single possible threat, but only from those that the organization considers relevant and only to the extent that is justified financially and commercially through a risk assessment. BS7799 was originally just a single standard, and

## 8.4 Information Systems Control and Audit

had the status of a Code of Practice. In other words, it provided guidance for organizations, but hadn't been written as specification that could form the basis of an external third party verification and certification scheme. As more and more organizations began to recognize the scale, severity and interconnectedness of information security threats and with the emergence of a growing range of data protection and privacy-related law and regulation, the demand for a certification option linked to the standard began to develop. This led, eventually, to the emergence of a second part to the standard, in the form of a specification (a specification uses words like 'shall') numbered as BS7799-2 (or, part 2). The Code of Practice (which uses words like 'may' and which deals with controls, not with Information Security Management Systems), is now recognized under the dual numbers of ISO17799 and BS7799-1 (or, part 1).

### 8.3.1 Benefits of Using BS 7799

The benefits of using BS7799 are straightforward. Using it well will result in:

- Reduced operational risk
- Increased business efficiency
- Assurance that information security is being rationally applied

This is achieved by ensuring that:

- Security controls are justified.
- Policies and procedures are appropriate.
- Security awareness is good amongst staff and managers.
- All security relevant information processing and supporting activities are auditable and are being audited.
- Internal audit, incident reporting / management mechanisms are being treated appropriately.
- Management actively focus on information security and its effectiveness.

It is likely that a number of organisations, including Government, will require suppliers and other partners to be certified to BS 7799 before they can be given work. This could make compliance (or certification) more of a necessity than a benefit. Certification can also be used as part of a marketing initiative, providing assurance to business partners and other outsiders.

**8.3.2 Components of BS 7799** : The standard is composed of two parts: BS 7799 (ISO 17799) Part 1 - Code of Practice on Information Security Management and BS 7799 Part 2 – Specification for Information Security Management Systems. The Code of Practice on Information Security provides a comprehensive set of security controls comprising the best information security practices in current use. It is strongly business-orientated, focusing on being a good management tool rather than being concerned with technical details.

### ISO 27001 –(BS7799 : Part II) – Information Security Management Standard

The requirements of information security system as described by standard are stated below. An organisation must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).

**General:** Organisation shall establish and maintain documented ISMS addressing assets to be protected, organisations approach to risk management, control objectives and control, and degree of assurance required.

**Establishing Management Framework :** This would include

- Define information security policy;
- Define scope of ISMS including functional, asset, technical, and locational boundaries;
- Make appropriate risk assessment ;
- Identify areas of risk to be managed and degree of assurance required;
- Select appropriate controls;
- Prepare Statement of Applicability,

**Implementation :** Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.

**Documentation :** The documentation shall consist of evidence of action undertaken under establishment of the following

- Management control
- Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
- Procedure adopted to implement control under Implementation clause
- ISMS management procedure
- Document Control: The issues focused under this clause would be
  - ◆ Ready availability
  - ◆ Periodic review
  - ◆ Maintain version control;
  - ◆ Withdrawal when obsolete
  - ◆ Preservation for legal purpose
- Records : The issues involved in record maintenance are as follows:
  - ◆ Maintain to evidence compliance to Part 2 of BS7799.;
  - ◆ Procedure for identifying, maintaining, retaining, and disposing of such evidence;

## 8.6 Information Systems Control and Audit

- ◆ Records to be legible, identifiable and traceable to activity involved.
- ◆ Storage to augment retrieval, and protection against damage.

**8.3.3 Areas of focus of ISMS :** There are ten areas of focus of ISMS. These are described in the following paragraphs:

(i) **Security Policy :** This activity involves a thorough understanding of the organization business goals and its dependence on information security. This entire exercise begins with creation of the IT Security Policy. This is an extremely important task and should convey total commitment of top management-. The policy cannot be a theoretical exercise. It should reflect the needs of the actual users. It should be implementable, easy to understand and must balance the level of protection with productivity. The policy should cover

- a definition of information security
- a statement of management intention supporting the goals and principles of information security
- allocation of responsibilities for every aspect of implementation
- an explanation of specific applicable proprietary and general, principles, standards and compliance requirements.
- an explanation of the process for reporting of suspected security incidents
- a defined review process for maintaining the policy document
- means for assessing the effectiveness of the policy embracing cost and technological changes
- nomination of the policy owner

The detailed **control and objectives** are as follows:

- *Information Security Policy:* To provide management direction and support for information security
- *Information System Infrastructure:* To manage information security within the organisation
- *Security of third party access:* To maintain the security of organisational information processing facilities and information assets accessed by third parties
- *Outsourcing:* To maintain the security of information when the responsibility for information processing has been outsourced to another organisation

(ii) **Organisational Security :** A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.

The detailed **control and objectives** are as follows :

- *Information System Infrastructure* : To manage information security within the organisation
- *Security of third party access* : To maintain the security of organisational information processing facilities and information assets accessed by third parties
- *Outsourcing* : To maintain the security of information when the responsibility for information processing has been outsourced to another organisation

(iii) **Asset Classification and Control** : One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, transmit or destruction of the information asset.

An Information Asset Register (IAR) should be created. detailing every information asset within the organisation. For example:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licenses
- Publicity material

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses. One major advantage in practice is that in case the password is also registered, it is a good back-up in case the carton/label containing password is accidentally misplaced. Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure appropriate security is in place.

## 8.8 Information Systems Control and Audit

The detailed **control and objectives** thereof are as follows :

- *Accountability for assets* : To maintain appropriate protection of organisational assets
- *Information Classification* : To ensure that information assets receive an appropriate level of protection

(iv) **Personnel Security** : Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training. Alert and well-trained employees who are aware of what to look for can prevent future security breaches.

Appropriate personnel security ensures that :

- Employment contracts and staff handbooks have agreed, clear wording
- Ancillary workers, temporary staff, contractors and third parties are covered
- Anyone else with legitimate access to business information or systems is covered

It must deal with rights as well as responsibilities, for example:

- Access to personal files under the Data Protection Act
- Proper use of equipment as covered by the Computer Misuse Act (In India that would be Information Technology Act 2000)

Staff training is an important feature of personnel security to ensure the Information Security Management System (ISMS) continues to be effective. Periodically, refreshers on less frequently used parts of the Information Security Management System (ISMS), such as its role in disaster recovery plans, can make a major difference when there is a need to put the theory into practice. This aspect deserves all the importance the management can give as most of the staff react by merely phoning the superior or the Information Technology (IT) Department instead of performing their designated task. Disaster management is a team effort and not the responsibility of a single department or person. Such an attitude may prove costly when and if such an event does occur.

The detailed control and objectives thereof are as follows:

- *Security in Job definition and Resourcing* : To reduce the risks of human error, theft, fraud, or misuse of facilities
- *User Training* : To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in course of their normal work
- *Responding to security incidents and malfunctions* : To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents



- (v) **Physical and Environmental Security** : Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is usually the beginning point of any security plan. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipment such as air conditioning plant or mains services should be properly maintained. Physical controls can be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed **control and objectives** thereof are as follows:

- *Secure areas*: To prevent unauthorized access, damage and interference to business premises and information
- *Equipment Security*: To prevent loss, damage or compromise of assets and interruption to business activities
- *General Controls*: To prevent compromise or theft of information and information processing facilities

- (vi) **Communications and Operations Management** : Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures.

Network management requires a range of controls to achieve and maintain security in computer networks. This also includes establishing procedures for remote equipment including equipment in user areas. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks. Special controls may also be required to maintain the availability of the network services.

Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation. There should be proper information and software exchange agreements, the media in transit need to be secure and should not be vulnerable to unauthorized access, misuse or corruption.

Electronic commerce involves electronic data interchange, electronic mail and online transactions across public networks such as Internet. Electronic commerce is vulnerable to a number of network threats that may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats.

## 8.10 Information Systems Control and Audit

The detailed **control and objectives** thereof are as follows :

- *Operational procedures and responsibilities* : To ensure correct and secure operation of information processing facility
- *System planning and acceptance* : To minimise risks of system failure
- *Protection against malicious software* : To protect the integrity of software and info
- *Housekeeping* : To maintain the integrity and availability of information processing and communication services
- *Network Management* : To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
- *Media handling and security* : Prevent damage to assets and interruptions to business activity
- *Exchanges of information and software* : To prevent loss, modification or misuse of information exchanged between organisations

(vii) **Access Control** : Access to information and business processes should be controlled on the business and security requirements. This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks, network connection control, network routing control, operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.

The detailed **control and objectives** thereof are as follows:

- *Business requirement for access control* : To control access to information
- *User access management* : To prevent unauthorised access to info systems
- *User responsibilities* : To prevent unauthorised user access
- *Network access control* : Protection of networked services
- *Operating system access control* : To prevent unauthorised computer access
- *Application Access Control* : To prevent unauthorised access to information held in information systems
- *Monitoring System Access and use* : To detect unauthorised activities
- *Mobile Computing and teleworking* : To ensure information security when using mobile computing & teleworking facilities

(viii) **Systems Development and Maintenance** : Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior

to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography.

A strict change control procedure should be in place to facilitate tracking of changes. Any changes to operating system changes, software packages should be strictly controlled. Special precaution must be taken to ensure that no covert channels, back doors or Trojans are left in the application system for later exploitation.

The detailed **control and objectives** thereof are as follows:

- *Security requirements of system* : To ensure that security is built into information systems
- *Security in application systems* : To prevent loss, modification or misuse of user data in application system
- *Cryptographic Controls* : To protect the confidentiality, authenticity or integrity of information
- *Security of system files* : To ensure that IT projects and support activities are conducted in a secure manner
- *Security in development and support process* : To maintain the security of application system software and information

(ix) **Business Continuity Management** : A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances

There is one control which is described here in below along with its objectives:

- *Aspects of business continuity management* : To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters

(x) **Compliance** : It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence.

Information Technology's use in business has also resulted in enacting of laws that enforce responsibility of compliance. All legal requirements must be complied with to

## 8.12 Information Systems Control and Audit

avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

The detailed **control and objectives** thereof are as follows:

- ◆ *Compliance with legal requirements* : To avoid breaches of any criminal and civil law, and statutory, regulatory, or contractual obligations, and of any security requirements
- ◆ *Review of security policy and technical compliance* : To ensure compliance of systems with organisational security policies and standards
- ◆ *System Audit Consideration* : To maximise the effectiveness, and to minimise interference to/from the system audit process

**BS 7799 (ISO 17799) AND "IT'S" RELEVANCE TO INDIAN COMPANIES** : Although Indian companies and the Government have invested in IT, facts of theft and attacks on Indian sites and companies are alarming. Numerous Indian Government sites have been hacked. Attacks and theft that happen on corporate websites are high and is usually kept under "strict" secrecy to avoid embarrassment from business partners, investors, media and customers.

Huge losses are some times un-audited and the only solution is to involve a model where one can see a long run business led approach to Information Security Management.

BS 7799 (ISO 17799) consists of 127 best security practices (covering 10 Domains which was discussed above) which Indian companies can adopt to build their Security Infrastructure. Even if a company decides not go in for the certification, BS 7799 (ISO 17799) model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Additional benefits of an ISMS are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately leads to increased profitability.

## 8.4 CMM - CAPABILITY MATURITY MODEL

In November 1986, the Software Engineering Institute (SEI), with assistance from the Mitre Corporation, began developing a process maturity framework that would help organizations improve their software process. In September 1987, the SEI released a brief description of the process maturity framework which was later expanded in Humphrey's book, *Managing the Software Process*. Two methods, software process assessment<sup>1</sup> and software capability evaluation and a maturity questionnaire were developed to appraise software process maturity.

After four years of experience with the software process maturity framework and the preliminary version of the maturity questionnaire, the SEI evolved the maturity framework into the Capability Maturity Model for Software (CMM). The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software

process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government.

The Capability Maturity Model for Software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence. The CMM was designed to guide software organizations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, an organization can steadily improve its organization-wide software process to enable continuous and lasting gains in software process capability.

**8.4.1 Fundamental Concepts Underlying Process – Maturity :** A software process can be defined as a set of activities, methods, practices, and transformations that people use to develop and maintain software and the associated products (e.g., project plans, design documents, code, test cases, and user manuals). As an organization matures, the software process becomes better defined and more consistently implemented throughout the organization.

**Software process capability** describes the range of expected results that can be achieved by following a software process. The software process capability of an organization provides one means of predicting the most likely outcomes to be expected from the next software project the organization undertakes.

**Software process performance** represents the actual results achieved by following a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.

**Software process maturity** is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone.

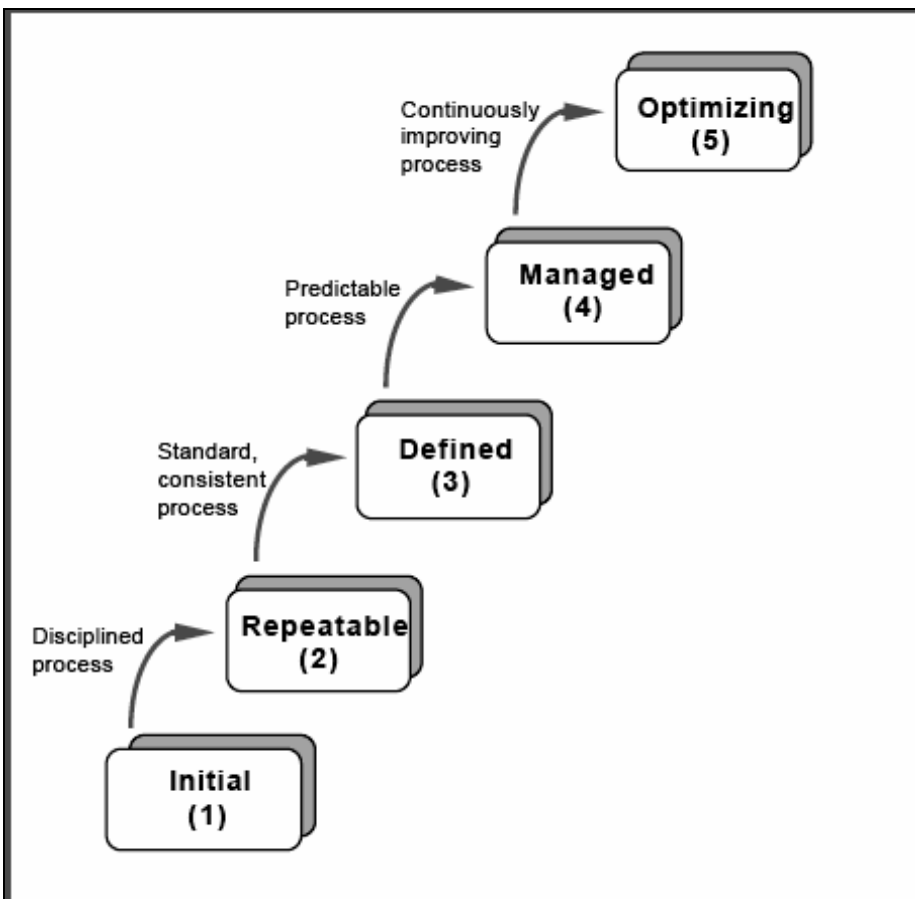
#### **8.4.2 The Five Levels of Software Process Maturity**

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. These five maturity levels define an ordinal scale for measuring the maturity of an organization's software process and for evaluating its software process capability. The levels also help an organization prioritize its improvement efforts.

## 8.14 Information Systems Control and Audit

A **maturity level** is a well-defined evolutionary plateau toward achieving a mature software process. Each maturity level comprises a set of process goals that, when satisfied, stabilize an important component of the software process. Achieving each level of the maturity framework establishes a different component in the software process, resulting in an increase in the process capability of the organization.

Organizing the CMM into the five levels shown in Figure-1 prioritizes improvement actions for increasing software process maturity. The labelled arrows in Figure indicate the type of process capability being institutionalized by the organization at each step of the maturity framework.



**8.4.3 Behavioural Characterization of the Maturity Levels :** Maturity Levels 2 through 5 can be characterized through the activities performed by the organization to establish or improve the software process, by activities performed on each project, and by the resulting process capability across projects. A behavioural characterization of Level 1 is included to establish a base of comparison for process improvements at higher maturity levels.

(i) **Level 1 - The Initial Level :** At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. Such

organizations frequently have difficulty making commitments that the staff can meet with an orderly engineering process, resulting in a series of crises. During a crisis, projects typically abandon planned procedures and revert to coding and testing. Success depends entirely on having an exceptional manager and a seasoned and effective software team. Occasionally, capable and forceful software managers can withstand the pressures to take shortcuts in the software process; but when they leave the project, their stabilizing influence leaves with them. Even a strong engineering process cannot overcome the instability created by the absence of sound management practices. In spite of this ad hoc, even chaotic, process, Level 1 organizations frequently develop products that work, even though they may be over the budget and schedule. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.

- (ii) **Level 2 - The Repeatable Level** : At the Repeatable Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. Process capability is enhanced by establishing basic process management discipline on a project by project basis. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. Projects in Level 2 organizations have installed basic software management controls. Realistic project commitments are based on the results observed on previous projects and on the requirements of the current project. The software managers for a project track software costs, schedules, and functionality; problems in meeting commitments are identified when they arise. Software requirements and the work products developed to satisfy them are baselined, and their integrity is controlled. Software project standards are defined, and the organization ensures they are faithfully followed. The software project works with its subcontractors, if any, to establish a customer-supplier relationship. Processes may differ between projects in a Level 2 organization. The organizational requirement for achieving Level 2 is that there are policies that guide the projects in establishing the appropriate management processes. The software process capability of Level 2 organizations can be summarized as disciplined because planning and tracking of the software project is stable and earlier successes can be repeated. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) **Level 3 - The Defined Level** : At the Defined Level, the standard process for developing and maintaining software across the organization is documented, including both software engineering and management processes, and these processes are integrated into a coherent whole. This standard process is referred to throughout the CMM as the organization's standard software process. Processes established at Level 3 are used (and changed, as appropriate) to help the software managers and technical staff perform more effectively. The organization exploits effective software engineering practices when standardizing its software processes. There is a group that is responsible for the

## 8.16 Information Systems Control and Audit

organization's software process activities, e.g., a software engineering process group, or SEPG. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfil their assigned roles. Projects tailor the organization's standard software process to develop their own defined software process, which accounts for the unique characteristics of the project. This tailored process is referred to in the CMM as the project's defined software process. A defined software process contains a coherent, integrated set of well-defined software engineering and management processes. A well-defined process can be characterized as including readiness criteria, inputs, standards and procedures for performing the work, verification mechanisms (such as peer reviews), outputs, and completion criteria. Because the software process is well defined, management has good insight into technical progress on all projects. The software process capability of Level 3 organizations can be summarized as standard and consistent because both software engineering and management activities are stable and repeatable. Within established product lines, cost, schedule, and functionality are under control, and software quality is tracked. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.

- (iv) **Level 4 - The Managed Level** : At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes. Software processes are instrumented with well-defined and consistent measurements at Level 4. These measurements establish the quantitative foundation for evaluating the projects' software processes and products. Projects achieve control over their products and processes by narrowing the variation in their process performance to fall within acceptable quantitative boundaries. Meaningful variations in process performance can be distinguished from random variation (noise), particularly within established product lines. The risks involved in moving up the learning curve of a new application domain are known and carefully managed. The software process capability of Level 4 organizations can be summarized as being quantifiable and predictable because the process is measured and operates within measurable limits. This level of process capability allows an organization to predict trends in process and product quality within the quantitative bounds of these limits. Because the process is both stable and measured, when some exceptional circumstance occurs, the "special cause" of the variation can be identified and addressed. When the known limits of the process are exceeded, action is taken to correct the situation. Software products are of predictably high quality.
- (v) **Level 5 - The Optimizing Level** : At the Optimizing Level, the entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the



organization's software process. Innovations that exploit the best software engineering practices are identified and transferred throughout the organization. Software project teams in Level 5 organizations analyze defects to determine their causes. Software processes are evaluated to prevent known types of defects from recurring, and lessons learned are disseminated to other projects. There is chronic waste, in the form of rework, in any system simply due to random variation. Waste is unacceptable; organized efforts to remove waste result in changing the system, i.e., improving the process by changing "common causes" of inefficiency to prevent the waste from occurring. While this is true of all the maturity levels, it is the focus of Level 5. The software process capability of Level 5 organizations can be characterized as continuously improving because Level 5 organizations are continuously striving to improve the range of their process capability, thereby improving the process performance of their projects. Improvement occurs both by incremental advancements in the existing process and by innovations using new technologies and methods. Technology and process improvements are planned and managed as ordinary business activities.

## **8.5 COBIT – IT Governance Model**

COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management.

The underpinning concept of the COBIT Framework is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes.

To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models:

- *Quality Requirements*: Quality , Cost, Delivery
- *Fiduciary requirements* : Effectiveness and Efficiency of operations, Reliability of Information, Compliance with laws and regulations
- *Security Requirements* : Confidentiality, Integrity, Availability

**Quality** has been retained primarily for its negative aspect (no faults, reliability, etc.), which is also captured to a large extent by the Integrity criterion. The positive but less tangible aspects of Quality (style, attractiveness, "look and feel," performing beyond expectations, etc.) were, for a time, not being considered from an IT control objectives point of view. The premise is that the first priority should go to properly managing the risks as opposed to the opportunities. The usability aspect of Quality is covered by the Effectiveness criterion. The Delivery aspect of Quality was considered to overlap with the Availability aspect of the Security requirements and also to some extent Effectiveness and Efficiency. Finally, Cost is also considered covered by Efficiency.

For the Fiduciary Requirements, COBIT did not attempt to reinvent the wheel—COSO's definitions for Effectiveness and Efficiency of operations, Reliability of Information and

## 8.18 Information Systems Control and Audit

Compliance with laws and regulations were used. However, Reliability of Information was expanded to include all information—not just financial information.

With respect to the **Security Requirements**, COBIT identified Confidentiality, Integrity, and Availability as the key elements—these same three elements, it was found, are used worldwide in describing IT security requirements.

**8.5.1 COBIT's working definitions** : Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted. COBIT's working definitions are as follows:

- *Effectiveness* : deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- *Efficiency* : concerns the provision of information through the optimal (most productive and economical) use of resources.
- *Confidentiality* : concerns the protection of sensitive information from unauthorized disclosure.
- *Integrity* : relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- *Availability* : relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- *Compliance* : deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.
- *Reliability of Information* : relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

**8.5.2 IT resources** : The IT resources identified in COBIT can be explained/defined as follows:

- *Data* : are objects in their widest sense (i.e. external and internal), structured and non-structured, graphics, sound, etc.
- *Application systems* : are understood to be the sum of manual and programmed procedures.
- *Technology* : covers hardware, operating systems, database management systems, networking, multimedia, etc.
- *Facilities* : are all the resources to house and support information systems.
- *People* : include staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

**8.5.3 The COBIT Framework :** The COBIT Framework consists of high-level control objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources. Starting at the bottom, there are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or life cycle applicable to IT processes.

**Domain of COBIT :** With the preceding as the framework, the domains are identified using wording that management would use in the day-to-day activities of the organisation—not auditor jargon. Thus, four broad domains are identified: planning and organisation, acquisition and implementation, delivery and support, and monitoring. Definitions for the four domains identified for the high-level classification are:

- *Planning and Organisation :* This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.

The following table lists the high level control objectives for the Planning and Organization domain.

Entire top and middle tiers of COBIT:

**Plan and Organize**

PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation 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
PO11	Manager Quality

## 8.20 Information Systems Control and Audit

- *Acquisition and Implementation* : To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

The following table lists the high level control objectives for the Acquisition and Implementation domain.

Entire top and middle tiers of COBIT:

### Acquire and Implement

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 Accredite Solutions and Changes

- *Delivery and Support* : This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.

The following table lists the high level control objectives for the Delivery and Support domain.

Entire top and middle tiers of CobiT:

### 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

- Monitoring* - All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management’s oversight of the organization’s control process and independent assurance provided by internal and external audit or obtained from alternative sources.

The following table lists the high level control objectives for the Monitoring domain.

Entire top and middle tiers of CobiT:

**Monitor and Evaluate**

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

**8.5.4 COBIT and Other Standards**

- COBIT and ISO/IEC 17799:2005 : The two international standards used today are COBIT and ISO/IEC 17799:2005. COBIT (Control Objectives for Information and related Technology) was released and used primarily by the IT community. In 1998, Management Guidelines were added, and COBIT became the internationally accepted framework for IT governance and control. ISO/IEC 17799:2005 (The Code of Practice for Information Security Management) is also an international standard and is best practice for implementing security management. The two standards do not compete with each other and actually complement one another. COBIT typically covers a broader area while ISO/IEC 17799 is deeply focused in the area of security.
- COBIT and Sarbanes Oxley : Public companies that are subject to the U.S. Sarbanes Oxley Act of 2002 are encouraged to adopt the following control frameworks: the Committee of Sponsoring Organizations of the Treadway Commission –COSO Internal Control Integrated Framework and the IT Governance Institute’s Control Objectives for Information and Related Technology –COBIT. In choosing which of the control

## 8.22 Information Systems Control and Audit

frameworks to implement in order to comply with Sarbanes-Oxley, the U.S. Securities and Exchange Commission suggests that companies follow the COSO framework.

- **COSO** Internal Control Integrated Framework states that internal control is a process established by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of stated objectives. COBIT approaches IT control by looking at information not just financial information that is needed to support business requirements and the associated Information Technology (IT) resources and processes. COSO control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. COBIT is extended to cover quality and security requirements in seven overlapping categories, which include effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information. These categories form the foundation for COBIT's control objectives. The two frameworks also have different audiences. COSO is useful for management at large, while COBIT is useful for management, users, and auditors. COBIT is specifically focused on IT controls. Because of these differences, auditors should not expect a one-to-one relationship between the five COSO control components and the four COBIT objective domains.

## 8.6 COCO

The "Guidance on Control" report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants. CoCo does not cover any aspect of information assurance per se. It is concerned with control in general. CoCo is "guidance," meaning that it is not intended as "prescriptive minimum requirements" but rather as "useful in making judgments" about "designing, assessing and reporting on the control systems of organizations." As such, CoCo can be seen as a model of controls for information assurance, rather than a set of controls. CoCo's generality is one of its strengths: if information assurance is just another organizational activity, then the criteria that apply to controls in other areas should apply to this one as well. CoCo "builds on the concepts in the COSO document." CoCo can be said to be a concise superset of COSO. It uses the same three categories of objectives: •effectiveness and efficiency of operations •reliability of financial reporting •compliance with applicable laws and regulations CoCo states that the "essence of control is purpose, capability, commitment, and monitoring and learning," These form a cycle that continues endlessly if an organization is to continue to improve. Four important concepts about "control" are as follows :

- 1 Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
- 2 People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives.
- 3 Organizations are constantly interacting and adapting.
- 4 Control can be expected to provide only reasonable assurance, not absolute assurance.

## 8.7 ITIL (IT INFRASTRUCTURE LIBRARY)

The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books. In order to make ITIL more accessible (and affordable) to those wishing to explore it, one of the aims of the ITIL v2 project was to consolidate the works into a number of logical 'sets' that aimed to group related sets of process guidelines for different aspects of the management of Information Technology systems, applications and services together

The eight ITIL books and their disciplines are:

The **IT Service Management** sets relating to

1. Service Delivery
2. Service Support

**Other operational guidance relating to**

3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management

To assist with the implementation of ITIL practices a further book was published providing guidance on implementation (mainly of Service Management)

8. Planning to Implement Service Management

### 8.7.1 Details of the ITIL Framework

- (a) The **Service Support** ITIL discipline is focused on the User of the ICT services and is primarily concerned with ensuring that they have access to the appropriate services to support the business functions. The service desk will try to resolve it, if there is a direct solution or will create an incident. Incidents initiate a chain of processes: Incident Management, Problem Management, Change Management, Release Management and Configuration Management.
- (b) The goal of **Problem Management** is to resolve the root cause of incidents and thus to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A 'problem' is an unknown underlying cause of one or more incidents, and a 'known error' is a problem that is successfully diagnosed and for which a work-around has been identified

## 8.24 Information Systems Control and Audit

(c) **Configuration Management** is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department. Configuration Management includes:

- ◆ Creating a parts list of every CI (hardware or software) in the system.
- ◆ Defining the relationship of CIs in the system
- ◆ Tracking of the status of each CI, both its current status and its history.
- ◆ Tracking all Requests for Change to the system.
- ◆ Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

- ◆ Planning
- ◆ Identification
- ◆ Control
- ◆ Status accounting
- ◆ Verification and Audit

(d) **Release Management** is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper Software and Hardware Control ensure the availability of licensed, tested, and version certified software and hardware, which will function correctly and respectively with the available hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software can be conceptually optimized to meet the demands of the business processes. The goals of release management are:

- ◆ Plan to rollout of software
- ◆ Design and implement procedures for the distribution and installation of changes to IT systems
- ◆ Effectively communicate and manage expectations of the customer during the planning and rollout of new releases
- ◆ Control the distribution and installation of changes to IT systems

(e) **Service Delivery** : The Service Delivery discipline is primarily concerned with the proactive and forward-looking services that the business requires of its ICT provider in order to provide adequate support to the business users. It is focused on the business as the Customer of the ICT services (compare with: Service Support). The discipline consists of the following processes, explained in subsections below:

- ◆ Service Level Management
- ◆ Capacity Management



- ◆ IT Service Continuity Management
  - ◆ Availability Management
  - ◆ Financial Management
- (f) **Service Level Management** : Service Level Management provides for continual identification, monitoring and review of the levels of IT services specified in the Service Level Agreements (SLAs). Service Level Management ensures that arrangements are in place with internal IT support providers and external suppliers in the form of Operational Level Agreements (OLAs) and Underpinning Contracts (UpCs). The process involves assessing the impact of change upon service quality and SLAs.
- (g) **Capacity Management** : Capacity Management supports the optimum and cost effective provision of IT services by helping organizations match their IT resources to the business demands. The high-level activities are Application Sizing, Workload Management, Demand Management, Modelling, Capacity Planning, Resource Management, and Performance Management
- (h) **Security Management** : The ITIL-process Security Management describes the structured fitting of information security in the management organization. ITIL Security Management is based on the code of practice for information security management also known as ISO/IEC 17799. A basic concept of the Security Management is the information security. The primary goal of information security is to guarantee safety of the information. Safety is to be protected against risks. Security is the means to be safe against risks. When protecting information it is the value of the information that has to be protected. These values are stipulated by the confidentiality, integrity and availability. Inferred aspects are privacy, anonymity and verifiability.
- (i) **ICT Infrastructure Management** : ICT Infrastructure Management processes recommend best practice for requirements analysis, planning, design, deployment and ongoing operations management and technical support of an ICT Infrastructure. The Infrastructure Management processes describe those processes within ITIL that directly relate to the ICT equipment and software that is involved in providing ICT services to customers.
- ◆ ICT Design and Planning
  - ◆ ICT Deployment
  - ◆ ICT Operations
  - ◆ ICT Technical Support
- (j) **The Business Perspective** : The Business Perspective is the name given to the collection of best practices that is suggested to address some of the issues often encountered in understanding and improving IT service provision, as a part of the entire business requirement for high IS quality management. These issues are:

## 8.26 Information Systems Control and Audit

- ◆ Business Continuity Management describes the responsibilities and opportunities available to the business manager to improve what is, in most organizations one of the key contributing services to business efficiency and effectiveness.
  - ◆ Surviving Change. IT infrastructure changes can impact the manner in which business is conducted or the continuity of business operations. It is important that business managers take notice of these changes and ensure that steps are taken to safeguard the business from adverse side effects.
  - ◆ Transformation of business practice through radical change helps to control IT and to integrate it with the business.
  - ◆ Partnerships and outsourcing
- (k) **Application Management** : ITIL Application Management set encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.
- (l) **Software Asset Management** : Organisations rely increasingly on technology in order to operate profitably and software as such should be treated as a valuable asset. Good Software Asset Management achieved through Best Practice enables organisations to save money through effective policies and procedures which are continuously reviewed and improved. Software Asset Management is a part of overall IT Service Management best illustrated by the IT Infrastructure Library (ITIL) guides, which is the mostly widely accepted approach to providing a comprehensive and consistent set of best practices.

## 8.8 SYSTRUST AND WEBTRUST

SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce. Only certified public accountants (CPAs) may provide the assurance services of Trust Services that result in the expression of a Trust Services, WebTrust, or SysTrust opinion, and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust Services engagements such as SysTrust and WebTrust.

- *Security*. The system is protected against unauthorized access (both physical and logical).
- *Availability*. The system is available for operation and use as committed or agreed.
- *Processing integrity*. System processing is complete, accurate, timely, and authorized.

- *Online privacy.* Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
- *Confidentiality.* Information designated as confidential is protected as committed or agreed.

Each of these Principles and Criteria are organized and presented in four broad areas:

- *Policies.* The entity has defined and documented its policies relevant to the particular principle.
- *Communications.* The entity has communicated its defined policies to authorized users.
- *Procedures.* The entity uses procedures to achieve its objectives in accordance with its defined policies.
- *Monitoring.* The entity monitors the system and takes action to maintain compliance with its defined policies.

At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion that effective controls have been maintained. The practitioner can report on all the SysTrust principles together or on each separately.

## **8.9 HIPAA**

The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996.

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. What is of interest here is the Security Rule issued under the Act

**8.9.1 The Security Rule :** The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans". The Security lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The standards and specifications are as follows:

## 8.28 Information Systems Control and Audit

(a). **Administrative Safeguards** : policies and procedures designed to clearly show how the entity will comply with the act

- ◆ Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
- ◆ The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
- ◆ Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.
- ◆ The procedures must address access authorization, establishment, modification, and termination.
- ◆ Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.
- ◆ Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
- ◆ A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- ◆ Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- ◆ Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

(b) **Physical Safeguards** : controlling physical access to protect against inappropriate access to protected data

- ◆ Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)

- ◆ Access to equipment containing health information should be carefully controlled and monitored.
- ◆ Access to hardware and software must be limited to properly authorized individuals.
- ◆ Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- ◆ Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- ◆ If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

(c) **Technical Safeguards** : controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

- ◆ Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- ◆ Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- ◆ Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
- ◆ Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone call-back, and token systems.
- ◆ Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
- ◆ In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- ◆ Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

## 8.30 Information Systems Control and Audit

### 8.10 SAS 70–STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report. SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

SAS No. 70 is generally applicable when an auditor ("user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres, or other data processing service bureaus.

In an audit of a user organization's financial statements, the user auditor obtains an understanding of the entity's internal control sufficient to plan the audit. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing or other data processing services to the user organization, the user auditor may be required to gain an understanding of the controls at the service organization.

**8.10.1 Service Auditor's Reports :** One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003). A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003).

The contents of each type of report is described in the following table:

<b>Report Contents</b>	<b>Type I Report</b>	<b>Type II Report</b>
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

**8.10.2. Benefits to the Service Organization :** Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

**8.10.3. Benefits to the User Organization :** User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization

### 8.32 Information Systems Control and Audit

receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

#### Self - Examination Questions

1. What are the auditing standard for IS Audit? Is AAS29 such a standard?
2. What are the major documentation requirement under BS7799
3. What are the areas of focus under BS7799 cover?
4. Under BS7799 (Part II) what is the importance of documentation?
5. What do you mean by Software Process Maturity?
6. What is the process of graduating from a Level 1 maturity to a Level 5 maturity under CMM Framework?
7. As an auditor, what all areas would you expect to evidence an organisation's migration from one level of maturity to a higher level under CMM framework?
8. What are the four domains identified under COBIT for high level classification? Can you establish their inter-relationship?
9. What are the eight ITIL series of documents?
10. What is the importance of configuration management under ITIL framework?
11. Who can sign SysTrust and WebTrust certifications? What are the principles under which such certifications take place?
12. What is the role of HIPAA in ensuring privacy and security of health data?
13. What are the various safeguards that HIPAA has suggested to ensure safeguarding of health data?
14. Why do you think a separate standard (SAS70) is useful for auditing a service organisation esp. with respect to examination of general controls over information technology and related controls?
15. What are the Type I and Type II reports under SAS70?



## **DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING- A PRACTICAL PERSPECTIVE**

---

### **LEARNING OBJECTIVES :**

- To understand the importance of IS Security,
- To discuss about Information Security Policies, and their hierarchy,
- To learn about Audit Policy, and
- To discuss about Audit Working Papers and documentations.

### **9.0 INTRODUCTION**

In the computerized information systems, most of the business processes are automated. Organizations are increasingly relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The information technology innovations such as hardware, software, networking technology, communication technology and ever-increasing bandwidth lead to completely new business models.

All these new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis (24 hours, 7 days a week). However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before. The denial of service attacks on the web sites of yahoo.com, amazon.com and lot of other web sites in February 2000 is a case in point. Those web sites were down for several hours to a few days jeopardizing the business of those organizations. The virus threat is real. The horror stories of 'Melissa' and 'I love you' are fresh in the minds of those organizations, who were affected by them. Further, the hacking and cracking on the Internet is real threat to virtual organizations, which are vulnerable to information theft and manipulations.

## **9.2 Information Systems Control and Audit**

### **9.1 IMPORTANCE OF INFORMATION SYSTEM SECURITY**

In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, information systems and communications that deliver the information are truly pervasive throughout organizations—from the user's platform to local and wide area networks to servers to mainframe computers. Organizations depend on timely, accurate, complete, valid, consistent, relevant, and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.

It is clear from the instances cited above that there are not only many direct and indirect benefits from the use of information systems, there are also many direct and indirect risks relating to the information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by:

- Widespread use of technology;
- Interconnectivity of systems;
- Elimination of distance, time, and space as constraints;
- Unevenness of technological changes;
- Devolution of management and control;
- Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
- External factors such as legislative, legal, and regulatory requirements or technological developments.

Security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information.

Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. The threats may emanate from, among others, technical conditions (program bugs, disk crashes), natural disasters (fires, floods), environmental conditions (electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) that can potentially result in a loss of management control and oversight are increasing in significance.

Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failures.

## **9.2 INFORMATION SYSTEM SECURITY**

Security relates to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood and implemented by most organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc. which are not understood nearly as well by organizations as physical safeguards. In organizations where a security breach has been experienced, the effectiveness of security policies and procedures has had to be reassessed.

This concept of security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

**Security Objective** : The objective of information system security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability”.

For any organization, the security objective comprises three universally accepted attributes:

- **Confidentiality** : Prevention of the unauthorized disclosure of information.
- **Integrity** : Prevention of the unauthorized modification of information.
- **Availability** : Prevention of the unauthorized withholding of information.

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

**9.2.1 What Information is Sensitive?** : The following examples highlight some of the factors, necessary for a company to succeed. The common thing thread in each case is the critical information that each generates.

- **Strategic Plans** : Most organizations readily acknowledge that strategic plans are crucial to the success of a company. But most of the companies fail to really make an effort to protect these plans.

For example: a competitor learns that a company is testing a new product line in a specific geographic location. The competitor removes its product from that location, creating an illusionary demand for the product. When the positive results of the marketing test are provided to the company's executives, they decide to roll the product out nationwide. Only then did the company discover that in all other geographic regions the competition for their product was intense. The result: the company lost several million, dollars as its product sales faltered.

## 9.4 Information Systems Control and Audit

Although it might have been impossible for the company to completely prevent its intentions from being discovered, this situation does illustrate the real value of keeping strategic plans confidential. In today's global environment, the search for competitive advantage has never been greater. The advantages of achieving insight into a competitor's intentions can be substantial. Industry studies bear witness to this fact.

- **Business Operations** : Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary. As such, they may provide a market advantage to the organization. This is the case when one company can provide a service profitably at a lower price than the competition. A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor.

While most organizations prohibit the sharing of such data, carelessness often results in its compromise. Such activity includes inadvertent storage of data on unauthorized systems, unprotected laptops, and failure to secure magnetic media.

- **Finances** : Financial information, such as salaries and wages, are very sensitive and should not be made public. While general salary ranges are known within industry sectors, precise salary information can provide a competitive edge. As salaries and wage-related charges normally comprise the majority of fixed costs, lower costs in this area contribute directly to an organization's profitability. When a competitor knows specific information about a company's wages, the competitor may be able to price its products accordingly. When competitors' costs are lower, they can either under-price the market or increase profits. In either case, the damage to an organization may be significant.

**9.2.2 Establishing better Information Protection** : The examples given in the above section highlight only three of the various types of sensitive information every business holds. Protecting this information is crucial to the overall success or failure of a company. Businesses hold such a vast array of data, what steps do they need to take to keep all of their critical information protected?

These points may be considered:

- **Not all data has the same value.** And, as such, the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they can plan for the appropriate levels of protection.
- **Know where the critical data resides.** In today's business environment, this is normally the company's information systems infrastructure. Because each piece of information may require different levels of protection, identifying where each is located enables an organization to establish an integrated security solution. This approach also provides significant cost benefits, as the company does not need to spend more on protecting data than the data itself is worth. Protection solutions must be based on the most valuable

information assets. The network environment also presents additional challenges for protecting information.

- **Develop an access control methodology.** Information does not have to be removed to cause damage or to have financial impact. Information that is inadvertently damaged disclosed or copied without the knowledge of the owner may render the data useless. To guard against this, organizations must establish some type of access control methodology. For important data, this access control (and the associated auditing) should extend to the file level. Such access control extends from the host to the network. There are many types of solutions designed to provide this protected access.
- **Protect information stored on media.** Employees can cause considerable damage by walking out the door with information on 3 ½-inch floppy disks or CD-ROMS. In addition, companies should control magnetic media to reduce the loss of software (both application and operating system). And finally, when migrating from one platform to another, the status of all hard drives, and the associated data, should be controlled.
- **Review hardcopy output.** The hardcopy output of employees' daily work should also be reviewed. Although strategic plans in their final forms may be adequately protected, what measures are used to safeguard all drafts and working papers? What information is regularly placed in the recycle or trash containers without thought to its value?

Based on this limited discussion, it is clear that much of the information that is so essential to successful business operations could be destructive if it is misused by employees, or should fall into the wrong hands. The exposure of the information systems to unauthorized individuals is greatly increased when companies connect their computers to other networks and the Internet. Computer systems and networks are inherently prone to data theft, loss, damage or destruction. Protecting such information systems must be done holistically, providing the organization with the appropriate level of security at a cost that is acceptable to the business.

### **9.3    PROTECTING COMPUTER-HELD INFORMATION SYSTEMS**

In section 9.2.1, we discussed that not all information is equal and that some information requires greater protection than other information. Making the very broad assumption that all of an organization's valuable information systems are held electronically on a computer, we can now consider how these should be protected.

Prior to discussing the details of 'how to protect the information systems', we need to define a few basic ground rules that must be addressed sequentially:

- **Rule #1 :** We need to know that 'what the information systems are' and 'where these are located'.
- **Rule #2 :** We need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
- **Rule #3:** We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.

## 9.6 Information Systems Control and Audit

- **Rule #4** : We need to know that 'how quickly information needs to be made available should and it become unavailable for whatever reason (loss, unauthorized modification, etc.) '

These four rules are deceptively simple. For most organizations, providing answers to permit the design and implementation of any information system protection is very taxing.

There are two basic types of protection that an organization can use: Preventative and Restorative.

**9.3.1 Preventative Information Protection** : This type of protection is based on use of security controls. Information system security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls. The organization's Information Security Policy through the associated Information Security Standards documentation mandates use of these controls.

Here are some examples of each type of control:

- **Physical** : Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
- **Logical (Technical)** : Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems; and
- **Administrative** : Security Awareness, User Account Revocation, Policy

**9.3.2 Restorative Information Protection** : Security events that damage information systems will happen. If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business.

Planning and operating an effective and timely information system backup and recovery program is vital to an operation. Information system backup does not simply involve backing up "just the valuable information," but it frequently also means backing up the system as well, since the information may need services that the system provides to make the information usable.

The key requirement of any restorative information system protection plan is that the information systems can be recovered. This is frequently an issue that many organizations fail to properly address. There is a common belief that if the backup program claimed it wrote the information system to the backup media, it can be recovered from the backup media. However, there are many variables that can prove that belief wrong.

Here are a few questions that any restorative information system protection program must address:

- Has the recovery process been tested recently?
- How long did it take?
- How much productivity was lost?
- Did everything go according to plan?

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

**9.3.3 Holistic Protection :** Protecting corporate information systems from harm or loss is not an easy task. Protection must be done holistically and give the organization the appropriate level of security at a cost that is acceptable to the business. One must plan for the unexpected and unknown, expect the worst events to happen, and recover from these events if and when they occur, as though nothing ever happened. Such events can't be planned, and they always seem to happen at the most inopportune times. Organizations that wait until the last minute to decide on a protection plan and recovery process will suffer.

## **9.4 INFORMATION SECURITY POLICY**

A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets, including sensitive information are managed, protected, and distributed within the user organization.

An information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

**9.4.1 Issues to address :** This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organisation, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

## 9.8 Information Systems Control and Audit

**9.4.2 Members of Security Policy :** Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

- Management members who have budget and policy authority,
- Technical group who know what can and cannot be supported, and
- Legal experts who know the legal ramifications of various policy charges

Information security policies must always take into account business requirements. Business requirements are the principles and objectives adopted by an organization to support its operations and information processing. E-commerce security is an example of such business requirements.

Furthermore, policies must consistently take into account the legal, statutory, regulatory and contractual requirements that the organization and its professional partners, suppliers and service providers must respect. The respect of intellectual property is a good example of such requirements.

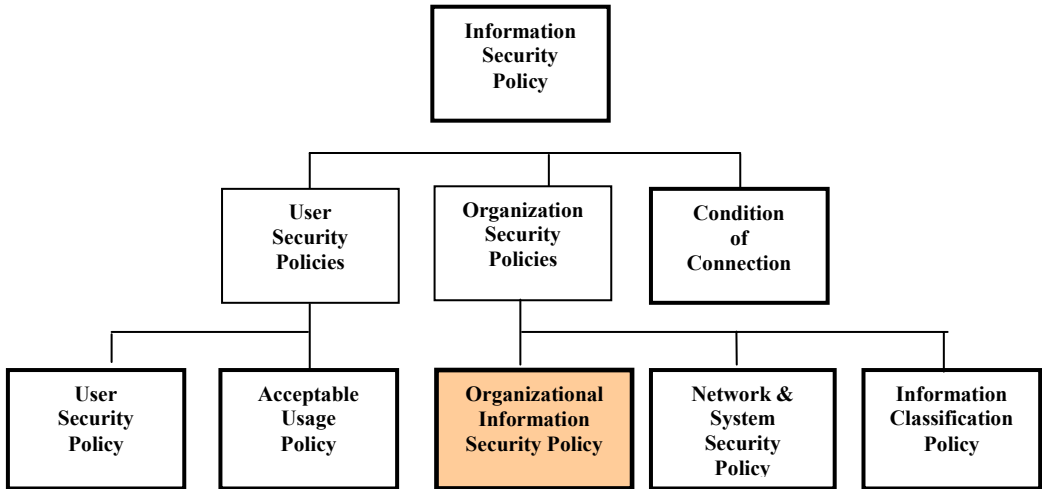
## 9.5 TYPES OF INFORMATION SECURITY POLICIES AND THEIR HIERARCHY

Major Information Security Policies are given as follows:

- **Information Security Policy :** This policy provides a definition of Information Security, its overall objective and the importance applies to all users.
- **User Security Policy :** This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
- **Acceptable Usage Policy :** This sets out the policy for acceptable use of email and Internet services.
- **Organisational Information Security Policy :** This policy (the one you are reading) sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. (Although it is positioned at the bottom of the above hierarchy diagram, it is the main IT security policy document.)
- **Network & System Security Policy :** This policy sets out detailed policy for system and network security and applies to IT department users
- **Information Classification Policy :** This policy sets out the policy for the classification of information
- **Conditions of Connection :** This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.



The hierarchy of these policies is shown in the Fig. 9.5.1.



**Fig 9.5.1 : The hierarchy of Information Security Policies**

**9.5.1 Components of the Security Policy :** A good security policy should clearly state the following :

- Purpose and Scope of the Document and the intended audience,
- The Security Infrastructure,
- Security policy document maintenance and compliance requirements,
- Incident response mechanism and incident reporting,
- Security organization Structure,
- Inventory and Classification of assets,
- Description of technologies and computing structure,
- Physical and Environmental Security,
- Identity Management and access control,
- IT Operations management,
- IT Communications,
- System Development and Maintenance Controls,
- Business Continuity Planning,
- Legal Compliances,
- Monitoring and Auditing Requirements, and
- Underlying Technical Policy.

## 9.10 Information Systems Control and Audit

Described below are the major contents of a typical security policy. The policy is very organization specific and a study of the organizations functions, their criticality and the nature of the information would determine the content of the security policy.

**9.5.2 Purpose and Scope :** It defines what the authorized is trying to accomplish through the policy. The primary objective of the policy would be to ensure confidentiality, integrity and availability of information and related systems. The security policy is designed to:

- (a) Deny authorized access to any IT resources, and Restrict access to data and resources or IT processes.
- (b) Within the operational constraints, the security controls will allow the required services to be available to authorized users only.
- (c) The scope defines how far the policy would be applicable, to whom it would be applicable and the period for which the policy would be applicable.

**9.5.3 Security Organization Structure :** The security responsibility and the line of reporting in the organization should be defined in the policy as stated below:

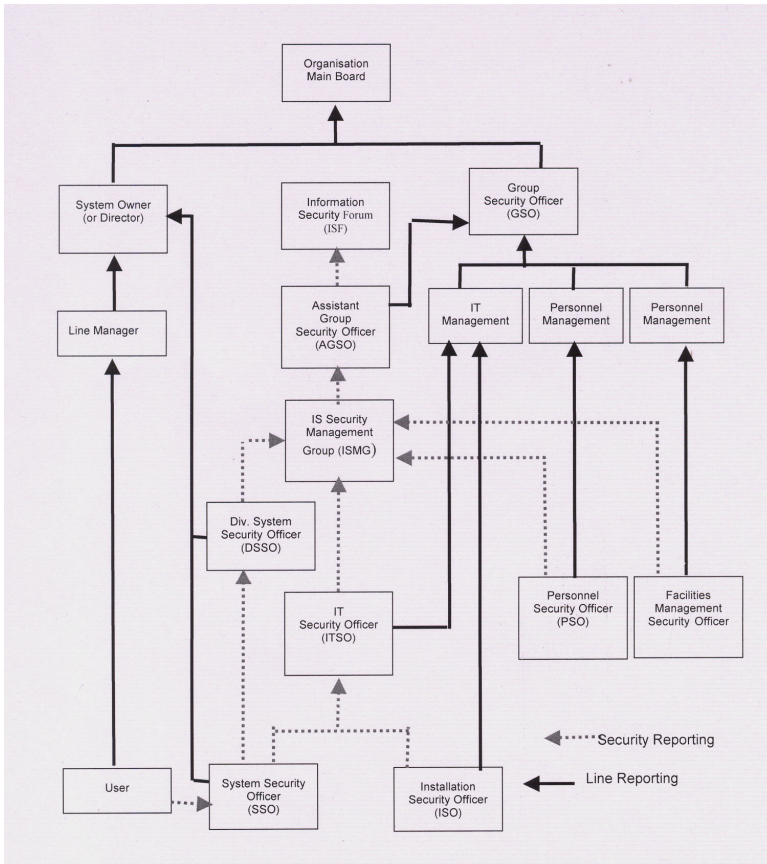
- **Information Security Forum (ISF) :** This forum is chaired by the GSO and includes senior representatives from each of the divisions within the Group, together with the AGSO. The AGSO provides the reporting conduit from the ISMG. It is the role of this forum to ensure that there is clear direction and visible management support of security initiatives within the organization.
- **Information Security Management Group (ISMG) :** This cross functional group is chaired by the AGSO and comprises of a Divisional System Security Officer (DSSO) from each of the divisions within the Group, together with the IT Security Officer (ITSO), and the Personnel and Facilities Management Security Officers. Its role is to co-ordinate the implementation and management of information security controls across all of the divisions and sites.
- **Group Security Officer (GSO) :** The GSO will have overall responsibility for security within the Group. This includes the security of all information assets, the network accreditation scheme and for non-IT security including physical and personnel matters.
- **Assistant Group Security Officer (AGSO) :** The AGSO reports to the GSO and the Information Security Forum and is responsible for the co-ordination of information security implementation and management across the Group. The AGSO chairs the ISMG.
- **IT Management :** IT Management have overall responsibility for security of the IT infrastructure. This is discharged mainly through Installation Security Officers (ISOs) and the IT Security Officer (ITSO) who will report directly to the IS Service Manager.
- **IT Security Officer (ITSO) :** The IT Security Officer reports to the ISMG on IT security matters. The ITSO is responsible for managing IT security programmes and IT security incidents. The ITSO will chair regular meetings of the ISO's.

## Drafting of IS Security Policy, Audit Policy, IS Audit Reporting 9.11 - A Practical Perspective

- **Installation Security Officer (ISO)** : An ISO will be appointed for each IT environment (including Network and Desktop) from the IT Team Leaders. ISOs will be responsible for all security matters related to their system/installation and/or network and will meet regularly with the IT Security Officer.
- **Personnel Security Officer (PSO)** : The Personnel Security Officer (PSO) will report directly to Personnel Management and the ISMG on all security matters relating to personnel. The role involves ensuring the controls set out are implemented, adhered to and reviewed as necessary.
- **Facilities Management Security Officer (FMSO)** : The Facilities Management Security Officer (FMSO) will report directly to Facilities Management on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.
- **Divisional System Security Officer (DSSO)** : A System Security Officer (SSO) from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSOs in their division at the ISMG and for communicating requirements and issues to/from this group.
- **System Security Officer (SSO)** : A senior user will be appointed to fulfill the role of System Security Officer (SSO) for each major application system or group of systems. SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
- **System Owners** : System Owners carry the overall responsibility for the information security of their own systems. Much of the day to day operational aspects of live systems may be delegated across a range of user defined roles and technical roles including their systems accreditation process. System Owners are responsible for allocation of protective markings to their systems and data according to the Information Classification policy, and all staff for treating protectively marked material accordingly.
- **Line Managers** : All Line Managers with any responsibility for live or developing IT systems must take appropriate steps to ensure compliance with the aims and objectives of this policy. As part of this process they will ensure that all required security measures are understood and in force.
- **Users** : All users of live IT systems are required to comply with the security procedures for their system and any applicable general IT security guidance.

## 9.12 Information Systems Control and Audit

A sample structure is given in Fig. 9.5.2 :



**Fig. 9.5.2: The Information Security Organization Structure**

**9.5.4 Responsibility allocation :** The responsibilities for the management of Information Security should be set out in this policy.

- An owner would be appointed for each information asset.
- All staff should be aware of the need for Information Security and should be aware of their responsibilities.
- All the tasks have been completed successfully and the System Owner is satisfied.
- All new network communications links must be approved.
- A contact list of organizations that may be required in the event of a security incident to be maintained.
- Risk assessments for all third party access to the information assets and the IT Network must be carried out.

- Access by third parties to all material related to the IT Network and infrastructure must be strictly limited and controlled. There should be a Conditions of Connection agreement in place for all third party connections.
- All outsourcing contracts must detail All major changes to software and hardware including major updates and new versions must be approved. It is not permissible to make the changes to a live system until tests have security responsibilities

### **9.5.5 Asset Classification and Security Classification**

Following are the major points for these classifications:

- An inventory of assets must be maintained. This must include physical, software and information assets.
- A formal, documented classification scheme (as set out in the Information Classification Policy) should be in place and all staff must comply with it.
- The originator or 'owner' of an item of information (e.g. a document, file, diskette, printed report, screen display, e-mail, etc.) should provide a security classification, where appropriate.
- The handling of information, which is protectively marked CONFIDENTIAL or above must be specifically approved (i.e. above RESTRICTED).
- Exchanges of data and software between organizations must be controlled. Organizations to whom information is to be sent must be informed of the protective marking associated with that information, in order to establish that it will be handled by personnel with a suitable clearance corresponding to the protective marking.
- Appropriate procedures for information labeling and handling must be agreed and put into practice.
- Classified waste must be disposed of appropriately and securely.

### **9.5.6 Access Control**

In Access Control, the following points need to be taken into consideration:

- Access controls must be in place to prevent unauthorized access to information systems and computer applications
- Access must only be granted in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
- System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.

## **9.14 Information Systems Control and Audit**

- Users should be granted access to systems only up to the level required to perform their normal business functions.
- The registration and de-registration of users must be formally managed.
- Access rights must be deleted for individuals who leave or change jobs.
- Each individual user of an information system or computer application will be provided with a unique user identifier (user id)
- It should not be permitted for an individual to use another person's user id or to log-on, to allow another individual to gain access to an information system or computer application.
- PCs and terminals should never be left unattended whilst they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorized changes.
- Passwords Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
- Mobile computing - When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.

### **9.5.7 Incident Handling**

For incident handling, following are the major points:

- Security incident reporting times and approach must be consistent at all times. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analyzed to identify weaknesses or trends.
- Procedures for the collection of evidence relating to security incidents should be standardized. All staff must be made aware of the process. Adequate records must be maintained and inspections facilitated to enable the investigation of security breaches or concerted attempts by third parties to identify security weaknesses.

### **9.5.8 Physical and Environmental Security**

For the proper implementation of Physical and Environment Security, the following points need to be taken into account:

- Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- The IT infrastructure must be physically protected.
- Access to secure areas must remain limited to authorized staff only.

## **Drafting of IS Security Policy, Audit Policy, IS Audit Reporting 9.15 - A Practical Perspective**

- Confidential and sensitive information and valuable assets must always be securely locked away when not in use.
- Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
- Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities
- Equipment, information or software must not be taken off-site without proper authorization.
- Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- The location of the equipment room(s) must not be obvious. It will also where practical be located away from, and protected against threats of, unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures

### **9.5.9 Business Continuity Management**

In Business Continuity planning, following points should be addressed:

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.

### **9.5.10 System Development and Maintenance Controls**

These controls are given as follows:

- System development or enhancements must have appropriate security controls included to safeguard their availability and ensure the integrity and confidentiality of the information they process.
- All security requirements and controls must be identified and agreed prior to the development of information systems.

## **9.6 AUDIT POLICY**

**9.6.1 Purpose of the audit policy :** Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats which includes the following:

- Access to confidential data,
- Unauthorized access of the department computers,

## 9.16 Information Systems Control and Audit

- Password disclosure compromise,
- Virus infections,
- Denial of service attacks,
- Open ports, which may be accessed from outsiders, and
- Unrestricted modems unnecessarily open ports.

Audits may be conducted to ensure integrity, confidentiality and availability of information and resources.

The IS Audit Policy should lay out the objective and the scope of the Policy. An IS audit is conducted to :

- safeguard the Information System Assets/Resources,
- maintain the Data Integrity,
- maintain the System Effectiveness,
- ensure System Efficiency, and
- comply with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

**9.6.2 Scope of IS Audit :** The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system(s) for the use and protection of information and the information system, as under:

- Data
- Application systems
- Technology
- Facilities
- People

The Information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The information system auditor will examine, among others, the following:

- Information system mission statement and agreed goals and objectives for information system activities.



## Drafting of IS Security Policy, Audit Policy, IS Audit Reporting    9.17 - A Practical Perspective

- Assessment of the risks associated with the use of the information systems and approach to managing those risks.
- Information system strategy plans to implement the strategy and monitoring of progress against those plans.
- Information system budgets and monitoring of variances.
- High level policies for information system use and the protection and monitoring of compliance with these policies.
- Major contract approval and monitoring of performance of the supplier.
- Monitoring of performance against service level agreements.
- Acquisition of major systems and decisions on implementation.
- Impact of external influences on information system such as internet, merger of suppliers or liquidation etc.
- Control of self-assessment reports, internal and external audit reports, quality assurance reports or other reports on Information System.
- Business Continuity Planning, Testing thereof and Test results.
- Compliance with legal and regulatory requirements.
- Appointment, performance monitoring and succession planning for senior information system staff including internal information system audit management and business process owners.

**9.6.3 What Audit policy should do ?** : The Audit Policy should lay down the responsibility of audit. The audit may be conducted by internal auditors or external auditors. Information System Auditors should be independent of the activities they audit. Independence permits the auditors to render impartial and unbiased judgment essential to the proper conduct of audits. It is achieved through organizational status and objectivity.

- The Policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made
- A statement of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.
- All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design.
- The policy may lay out the extent of testing to be done under the various phases of the audit
  - ◆ Planning
  - ◆ Compliance Testing
  - ◆ Substantive Testing

## 9.18 Information Systems Control and Audit

- 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.
- The policy should determine when and to whom the audit results would be reported and communicated. It would define the access rights to be given to the auditors. This access may include:
  - ◆ User level and/or system level access to any computing or communications
  - ◆ device
  - ◆ Access to information (electronic, hardcopy, etc.) that may be produced,
  - ◆ transmitted or stored on respective Dept. equipment or premises
  - ◆ 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.
- 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.
- 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.
- The Audit Policy would define the compulsory audit working papers to be maintained and their formats.

## **9.7    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.

In case of recurring audits, some working paper files may be classified as permanent audit files which are updated currently with information of continuing importance to succeeding audits, as distinct from the current audit files which contain information relating primarily to audit of a single period.

The permanent audit file normally includes:

- The organization structure of the entity,
- The IS policies of the organization,
- The historical background of the information system in the organization,
- Extracts of copies of important legal documents relevant to audit,
- A record of the study and evaluation of the internal controls related to the information system,
- Copies of audit reports and observations of earlier years, and
- Copies of management letters issued by the auditor, if any.

The current file normally includes:

- Correspondence relating to the acceptance of appointment and the scope of the work,
- Evidence of the planning process of the audit and audit programme,
- A record of the nature, timing, and extent of auditing procedures performed, and the results of such procedures,
- Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weaknesses in relevant internal controls,
- Letters of representation and confirmation received from the client,
- Conclusions reached by the auditor concerning significant aspects of the audit, including the manner in which the exceptions and unusual matters, if, any, disclosed by the auditor's procedures were resolved and treated, and
- Copies on the data and system being reported on and the related audit reports.

## 9.20 Information Systems Control and Audit

Working papers are the property of the auditor. The auditor may, at his discretion, make portions of, or extracts from his working papers available to the client. The auditor should adopt reasonable procedures for custody and confidentiality of his working papers and should retain them for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal and professional requirements of record retention.

**9.7.1 Planning the Documentation :** It is important to understand why it is important to plan 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:
  - ◆ **Knowing Your Resources:** The three basic resources: time, people, money. One has to check for their availability and affordability.
  - ◆ **Defining the Scope and Audience:** The same report may undergo significant changes depending on the character of report and nature of audience. Presentation on Balance Sheet made to bankers and to investors would be quite different in content and focus.
  - ◆ **Using a Scope Definition Report:** It is critical to know how to complete a Scope Definition Report. This report helps in developing a workable schedule for completing the project.
- (ii) **The Documentation Writer:** The qualities and skills that the documentation writer would need. The requirement may often be legal in nature
- (iii) **Rules to guide documentation writing:** The four steps of writing documentation described in subsequent section

**9.7.2 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.

- **About the Reader:** Finding information about the reader by doing a task analysis. Three parts of the task: viz. input, process, output will have to be identified before one could develop an understanding of a reader.
- **About the Subject:** The three sources of information about a subject are people, paper, and the object of the report.

**9.7.3 Organizing Information:** Organizing information involves deciding what information to include and how to sequence it. This covers five organizational sequences and examines how to divide the documentation into various sections and subsections.

- **Selecting Information:** Selecting 'what the reader needs to know'. Organizing the information into a useful sequence.
- **Organizing the Documentation:** Using the five organizational sequences: subject, difficulty, chronological, importance and analytical.

- Dividing Into Sections: Dividing documentation into chapters or sections.
- Dividing Into Subsections: Dividing sections or chapters into subsections.

**9.7.4 Writing the Documentation** : Writing is governed by the following major rules/principles:

- Writing in Active Voice: Using active voice in documentation.
- Giving the Consequences: Giving the consequences of the reader's action.
- Writing from General to Specific: Designing the documentation from general to specific.
- Consistency: Using style, order and format consistently.
- Writing Online Documentation: Laying down guidelines for writing online documentation. Using appropriate techniques to emphasize text.

**9.7.5 Finalizing Documents** : This section identifies the tasks involved in reviewing and testing the document, generating the glossary and index and formatting the document for final production.

- 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.
- 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.
- Formatting and Production: The idea of creating a good document is incomprehensible 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 also important to select an appropriate binding style that would aid filing and ease of consultation.

## **9.8 IS AUDIT REPORTS**

**Structure:** Audit reports broadly include the following sections: title page, table of contents, summary (including the recommendations), introduction, findings and appendices. These components of an audit report are discussed below:

(i) **Cover and Title Page** : Audit reports should use a standard cover, with a window showing the title: "Information System Audit" or "Data Audit", the department's name and the report's date of issue (month and year). These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.

## 9.22 Information Systems Control and Audit

(ii) **Table of Contents** : The table lists the sections and sub-sections with page numbers including summary and recommendations, introduction, findings (by audit field) and appendices (as required).

(iii) **Summary / Executive Summary** : The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not normally exceed three pages, including the recommendations.

(iv) **Introduction** : Since readers will read the summary, the introduction should not repeat details. It should include the following elements:

- ◆ **Context** : This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.
- ◆ **Purpose** : This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
- ◆ **Scope**: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
- ◆ **Methodology**: This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.

(v) **Findings** : Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives and clients' expectations. If the auditor is using any standard grading standard like InfoSecGrade or others, the arrived value should also be stated.

(vi) **Opinion** : If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.

(vii) **Appendices** : Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

**Level of Detail** : The depth of coverage for issues should normally reflect the significance of the findings. Situations representing a high degree of risk or indicating shortcomings that are serious enough to justify a recommendation should be treated extensively.

Specific initiatives that the auditors wish to mention as examples should be described in detail, while issues where the department meets the expectations and there is nothing specific to mention should be dealt with briefly.

**Commentary** : Where a recommendation and a compliment are made under the same issue, they should be in separate paragraphs, otherwise, they may confuse the reader and reduce the impact of one or the other.

Statistics need to be used consistently throughout the report. Sample size and error rate mean more when they are given in context. The size of the population, the number of transactions and the period of time provide that context.

Percentages should not be used when referring to small samples (less than one hundred).

Graphics should be used when they add to the understanding of the text.

## Sample IS Security Policy

### 1. INFORMATION SECURITY OVERVIEW

#### *a. Information as an Important Asset*

Information is an important asset. Accurate, timely, relevant, and properly protected information is absolutely essential to the organization. To ensure that information is properly handled, all accesses to, uses of, and processing of information must be consistent with information systems related policies and standards.

#### *b. Designation of Software and Systems as Competitive Information*

The information security function must annually prepare a list of software and systems which have been developed in-house and which provide the organization with a competitive advantage.

#### *c. Confidentiality Agreements Required for All Workers*

All employees, consultants, contractors, and temporaries must sign a confidentiality agreement at the time they join the organization.

#### *d. Data Classification Scheme*

Data must be categorized into different sensitivity classifications with separate handling requirements--e.g., restricted, confidential, and unclassified. This standard data sensitivity classification system must be used throughout the organization. These classifications should be defined to ensure understanding and consistency in their application. All restricted and confidential information must be labeled (marked) according to standards. Information that does not fall into one or more of these categories need not be marked. These marks must be maintained regardless of what technology is used to capture, store, or process the information--e.g., all tape reels, floppy disks, and other computer storage media containing restricted or confidential information must be externally labeled (marked).

#### *e. Confidentiality Agreements and Disclosures of Sensitive Information*

All disclosures of restricted or confidential information to third parties must be accomplished via a signed confidentiality agreement, which includes restrictions on the subsequent dissemination and usage of the information.

### 2. INFORMATION OWNERSHIP

#### *a. Information Ownership Must Be Assigned*

Management must clearly specify in writing the assignment of ownership responsibilities for databases, master files, and other shared collections of information. Such statements must also indicate the individuals who have been granted authority to originate, modify, or delete specific types of information found in these collections of information.



*b. Information Security Management Committee*

An information security management committee must be composed of senior managers or their delegates from each of the organization's major functions. This committee will meet periodically to:

- (a) review the current status of information security,
- (b) review and monitor security incidents within the company,
- (c) approve and later review information security projects,
- (d) approve new or modified information security policies, and
- (e) perform other high-level information security management activities.

*c. Information Ownership and Management's Responsibilities*

All production information possessed by or used by a particular organisational unit must have a designated owner. This owner, typically a user department middle-level manager, must determine appropriate sensitivity classifications, criticality ratings, and access controls over the use of this information. This owner must also take steps to ensure that appropriate controls are used in the storage, handling, distribution, and use of the information.

*d. Who Must Comply with Information Security Requirements*

Outside consultants, contractors, and temporaries must be subject to the same information security requirements and have the same information security responsibilities as the organization's employees.

*e. Designated Security Administrator for All Multi-user Systems*

Every multi-user computer system must have a designated security administrator to define user privileges, monitor access control logs, and perform similar activities. For purposes of this policy, local area network (LAN) servers and private branch exchange (PBX) switches are considered to be multi-user systems.

*f. Owners Required for Each Major Type of Information*

Each major type of information must have a designated owner. Each information owner must make decisions about the sensitivity and criticality of information assets consistent with published instructions. Owners must additionally identify user access requirements, determine an acceptable level of risk for both the information and systems that process it, and select appropriate controls for the information.

*g. Criteria for Assigning Information Ownership*

If there are several potential information owners, higher-level management should assign ownership responsibility to the single individual who makes the greatest use of the information.

## 9.26 Information Systems Control and Audit

### *h. Management Information Systems Department Must Not Be Owner of Information*

With the exception of operational computer and network information, the management information systems department must not be the owner of any information.

### *i. Designated Custodian Required for All Major Information Types*

Each major type of information must have a designated custodian. Each custodian must properly protect information in keeping with the designated owner's control sensitivity and criticality instructions.

### *j. Security Responsibilities of Information Custodians*

Information custodians are responsible for defining specific control procedures, administering information access controls, implementing and maintaining cost-effective information control measures, and providing recovery capabilities consistent with the instructions of information owners.

### *k. Security Responsibilities of Information Users*

All users of information must comply with the control requirements specified by the information's owner and/or custodian. Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements have been made.

## 3. INFORMATION SECURITY MANAGEMENT

### *a. Periodic Analysis of Information Security Violations and Problems*

A periodic analysis of reported information security problems and violations must be prepared by the information security function.

### *b. Problem Reporting and Management Process*

Information reflecting the effects of system faults, breakdowns, and computer-related problems must be made available to users on a regular basis. A formal problem management process must be in place to record the problems, reduce their incidence, and prevent their recurrence.

### *c. Risk Assessments Required for Production Information Systems*

All production information systems must be periodically evaluated by the information security function to determine the minimum set of controls required to reduce risk to an acceptable level.

### *d. Agreements with Third Parties Who Handle Information*

All agreements dealing with the handling of information by third parties must include a special clause. This clause must allow the organization to audit the controls used for these information handling activities and to specify the ways in which information will be protected.

*e. Avoid Actual and Apparent Conflict of Interest*

All workers must avoid the actual or apparent conflict of interest in their business-related dealings with the organization. Should there be any doubt as to the existence of a potential conflict of interest, the worker must consult his or her manager.

*f. Disciplinary Measures for Information Security Non-compliance*

Non-compliance with information security policies, standards, or procedures is grounds for disciplinary action, including termination. Management must inform workers that information security is a serious matter deserving their continued attention.

*g. Disciplinary Measures for Various Information Security Violations*

Assuming the action is inadvertent or accidental, first violations of information security policies or procedures must result in a warning. Second violations involving the same matter must result in a letter being placed in the involved worker's personnel file. Third violations involving the same matter must result in a five-day suspension without pay. Fourth violations involving the same matter must result in dismissal. Willful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including dismissal.

*h. Security Violations Requiring Instant Termination*

Unless the special permission of a senior executive is obtained, all workers who have stolen organizational property, acted with insubordination, or been convicted of a felony must be terminated immediately. Such instant terminations must involve both escort of the individual off the premises and assistance in collecting and removing the individual's personal effects.

*i. Agreements Not to Compete Required for Employees*

At the time they join the company; all employees must sign an agreement not to compete for two years after their separation from the organization.

*j. Minimum Password Length*

The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least six characters.

*k Cyclical Passwords Prohibited*

Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor.

*l. Periodic Forced Password Changes*

All users must be automatically forced to change their passwords at least once every thirty days.

*m. Assignment of Expired Passwords*

The initial passwords issued by a security administrator must be valid only for the involved user's first on-line session. At that time, the user must choose another password.

## **9.28 Information Systems Control and Audit**

### *n. Limit on Consecutive Unsuccessful Attempts to Enter a Password*

To prevent password-guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three unsuccessful attempts to enter a password, the involved user ID must be either suspended until reset by a system administrator, temporarily disabled for no less than ten minutes, or disconnected if dial-up or other external network connections are involved.

### *o. Password Sharing Prohibition*

Regardless of the circumstances, passwords must never be shared or revealed to anyone other than the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms.

### *p. User ID and Password Required for Computer-Connected Network Access*

All users must have their identity verified by a user ID and a secret password, or by other means which provide equal or greater security, prior to being permitted to use computers connected to a network.

### *q. Unique User-ID and Password Required*

All users must have a unique user ID and a personal secret password in order to gain access to every multi-user computer and computer network.

## **4. BUSINESS CONTINUITY PLANNING**

### *a. Compliance with Standards Required for Emergency/Disaster Support*

If subsidiaries, divisions, departments, and other organizational units wish to be supported by the management information systems department on a priority basis in the event of an emergency or a disaster, they must implement hardware, software, policies, and related procedures consistent with standards.

### *b. Framework for Segmenting Information Resources by Recovery Priority*

Computer operations management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first. All departments must use this same framework when preparing information systems contingency plans.

### *c. Annual Criticality Rating for Multi-user Applications*

In conjunction with relevant information owners, the management information systems department must periodically prepare or revise an assessment of the degree of criticality of all production multi-user computer applications. This will allow appropriate contingency plans to be prepared.

*d. Application Criticality Classification Scheme*

All production computer applications must be placed into one of these classifications: restricted, confidential, or unclassified. Each has separate handling requirements: critical, required, and deferrable. This criticality classification system must be used throughout the organization and must form an integral part of the system contingency planning process.

*e. Preparation and Maintenance of Computer Emergency Response Plans*

Management must prepare, periodically update, and regularly test emergency response plans that will allow all critical computer systems to continue processing in the event of an interruption or degradation of service.

*f. Preparation and Maintenance of Computer Disaster-Recovery Plans*

Management must prepare, periodically update, and regularly test a disaster-recovery plan that will allow all critical computer and communication systems to be available in the event of a major loss, such as a flood, earthquake, or tornado.

*g. Preparation and Maintenance of Business Contingency Plans*

Management must prepare, periodically update, and regularly test a business recovery plan. This recovery plan must specify how alternative facilities such as offices, furniture, telephones, and copiers will be provided so workers can continue operations in the event of an emergency or disaster.

*h. Business Continuity Planning Process*

A standard organization-wide process for developing and maintaining business and computer contingency plans must exist and be observed.

## **5. CHANGE CONTROL POLICIES**

*a. Separation between Production and Development Environments*

New business application software in development must be kept strictly separate from production application software. If existing facilities permit it, this separation must be achieved via physically separate computer systems. When computing facilities do not allow this, separate directories/libraries with password-based access controls must be employed.

*b. Development Staff Access to Production Application Information*

Business application software development staff must not be permitted to access production information, with the exception of the production information relevant to the particular application software on which they are currently working.

*c. System Developers Must Not Perform Formal Testing*

Workers who have been involved in the development of specific business application software must not be involved in the formal testing or day-to-day operation of such software.

### **9.30 Information Systems Control and Audit**

#### *d. Control over Movement of Software from Development to Production*

Business application development staff must not have the ability to move any software into the production processing environment.

#### *e. Review and Recompilation Required Before Movement into Production*

Executable modules must never be moved directly from test libraries to production libraries. Fully tested modules must be reviewed and then recompiled before being moved to production libraries. Review and recompilation activities must be performed by technical staff not associated with the testing process. This will help to detect and eradicate errors, as well as Trojan horses and other unauthorized codes.

#### *f. Formal Change Control Process Required for Business Applications*

A formal written change control process must be used to ensure that all business application software which is in development moves into production only after receiving proper authorization from the management of both the management information systems department management and user organization.

#### *g. Separation of Duties and Control over Assets*

Whenever a computer-based process involves sensitive, valuable, or critical information, the system must include controls involving a separation of duties or other compensating control measures. These control measures must ensure that no one individual has control over this type of information assets.

## **6. END-USER COMPUTING POLICIES**

#### *a. Approval for End-User Production System Development Efforts*

All software that handles sensitive, critical, or valuable information and that has been developed by end-users must have its controls approved by the information security function prior to being used for production processing.

#### *b. When Making Additional Copies of Software Is Permissible*

Third-party software in the possession of the organization must not be copied unless such copying is consistent with relevant license agreements and unless management has previously approved of the copying or copies are being made for contingency planning purposes.

#### *c. Games May Not Be Stored or Used on Computer Systems*

Games may not be stored or used on any computer systems.

#### *d. Initial Backup Copies of Microcomputer Software*

All microcomputer software must be copied prior to its initial use, and the copies must be stored in a safe place. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard-disk crashes, and other computer problems. These master copies must also be stored in a secure location.

*e. Periodic Review of Software Licensing Agreements*

The agreements for all computer programs licensed from third parties must be periodically reviewed for compliance.

*f. Storage of Sensitive Information on Personal Computers*

If sensitive information is to be stored on the hard-disk drive or other internal components of a personal computer, it must be protected by either a physical lock or encryption. If this information is written to a floppy disk, magnetic tape, smart card, or other storage media, the media must be suitably marked with the highest relevant sensitivity classification. When not in use, these media must be stored in locked furniture.

## **7. INTERNAL AUDIT**

*a. Internal Audit Review of Information System Controls*

The Internal Audit Function must periodically review the adequacy of information system controls, as well as compliance with such controls.

## **8. PHYSICAL SECURITY**

*a. Physical Security Measures for Computers and Communications Systems*

Buildings which house computers or communications systems must be protected with physical security measures that prevent unauthorized persons from gaining access.

### **Self - Examination Questions**

1. What are the objectives of information security? How does an information security policy help in achieving those objectives?
2. What are the various types of Information Security Policy? What is the hierarchical relationship between the policies?
3. What would be the major components of an Information Security Policy?
4. Describe a typical security organization structure for information security.
5. How important would you consider access control component of information security? What all provisions would you wish to incorporate in the same?
6. What role is Information Systems Audit policy expected to play in ensuring information security? What are the objectives of IS Audit?
7. Name some common security threats that the IS Audit is likely to address?
8. In addition to computer system hardware, what else would be included in the scope of an IS Auditor?
9. You are to conduct an IS Audit for an organization. Identify what all you would include in the audit plan?
10. What caution would you exercise while asking for an access right during an IS Audit?
11. Describe the content of a standard IS Audit report.

## **INFORMATION TECHNOLOGY (AMENDED) ACT, 2008**

---

### **LEARNING OBJECTIVES :**

- To know about IT Act 2000 (as Amended by Information Technology (Amendment) Act 2008), and its objectives,
- To understand its scope and definitions, and
- To discuss various chapters of the Act.

### **10.0 BRIEF HISTORY**

New communication systems and digital technology have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware with the advantages which the electronic form of business provides but people are reluctant to conduct business or conclude and transaction in the electronic form due to lack of appropriate legal framework. Electronic commerce eliminates need for paper based transactions. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance, are the requirements of writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate e-commerce, the need for legal changes has become an urgent necessity.

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. The legal recognition to electronic records and digital signatures in turn will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999.

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the



## 10.2 Information Systems Control and Audit

Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India. Therefore, it is important to understand 'what are the various perspectives of the IT Act, 2000 and what it offers?'

The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

This Act was amended by *Information Technology Amendment Bill 2006*, passed in *Lok Sabha* on Dec 22nd and in *Rajyasbha* on Dec 23rd of 2008. The then Hon'ble Minister of Communications & IT, Mr. Dayanidhi Maran discussed the statement of Objects and Reasons for ITAA-2006, which are given as follows:

- The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.
- With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as a protected system so as to restrict its access.
- A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.
- The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of the United Nations by its resolution No. 56/80, dated 12th December, 2001, recommended that all States accord favorable consideration to the said Model Law on Electronic Signatures. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonization with the said Model Law.

- The service providers may be authorized by the Central Government or the State Government to set up, maintain and upgrade the computerized facilities and also collect, retain appropriate service charges for providing such services at such scale as may be specified by the Central Government or the State Government.
- The Bill seeks to achieve the above objects.

### **10.1 THE IT ACT 2000 AND IT'S OBJECTIVES**

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

Objectives of the Act are :

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law.
- To facilitate electronic filing of documents with Government departments
- To facilitate electronic storage of data
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions
- To give legal recognition for keeping of books of accounts by banker's in electronic form.
- 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.

### **10.2 PRELIMINARY [CHAPTER I]**

It contains one section and two subsections. In subsection I, Short Title, Extent, Commencement and Application are given, and in subsection II, various definitions are discussed.

#### **10.2.1 Short Title, Extent, Commencement and Application**

- (1) This Act may be called the Information Technology Act, 2000. [As Amended by Information technology (Amendment) Act 2008]

P.S: Information Technology (Amendment) Bill 2006 was amended by Information Technology Act Amendment Bill 2008 and in the process, the underlying Act was renamed as Information Technology (Amendment) Act 2008 herein after referred to as **ITAA 2008**.

## 10.4 Information Systems Control and Audit

- (2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person.
- (3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.[Act notified with effect from October 17, 2000. Amendments vide ITAA-2008 notified with effect from....]
- (4) (Substituted Vide ITAA-2008)
- Nothing in this Act shall apply to documents or transactions specified in the First Schedule by way of addition or deletion of entries thereto.
- (5) (Inserted vide ITAA-2008)
- Every notification issued under sub-section (4) shall be laid before each House of Parliament

### 10.2.2 Definitions

- (1) In this Act, unless the context otherwise requires,
- (a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
- (b) "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
- (c) "Adjudicating Officer" means adjudicating officer appointed under subsection (1) of section 46;
- (d) "Affixing **Electronic** Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;
- (e) "Appropriate Government" means as respects any matter.
- (i) enumerated in List II of the Seventh Schedule to the Constitution;
- (ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;
- (f) "Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
- (g) "Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

- (h) "Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;
- (ha) "Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)
- (i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
- (j) **(Substituted vide ITAA-2008)**
- "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
- (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
- (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;
- (k) "Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software;
- (l) "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
- (m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;
- (n) "Cyber Appellate Tribunal" means the Cyber Appellate \* Tribunal established under sub-section (1) of section 48 (\* "Regulations" omitted)
- (na) (Inserted vide IT AA-2008)
- "Cyber Café" means 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.
- (nb) (Inserted Vide ITAA 2008)
- "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

## 10.6 Information Systems Control and Audit

- (o) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
- (p) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
- (q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;
- (r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
- (s) "Electronic Gazette" means official Gazette published in the electronic form;
- (t) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
  - (ta) **(Inserted vide ITAA-2006)**  
"electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature
  - (tb) **(Inserted vide ITAA-2006)**  
"Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"
- (u) "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
  - (ua) "Indian Computer Emergency Response Team" means an agency established under sub-section (1) of section 70 B
- (v) "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Amended vide ITAA-2008)
- (w) **(Substituted vide ITAA-2008)**  
"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that 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.

- (x) "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
  - (y) "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made there under
  - (z) "License" means a license granted to a Certifying Authority under section 24;
    - (za) Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
    - (zb) Prescribed" means prescribed by rules made under this Act;
    - (zc) Private Key" means the key of a key pair used to create a digital signature;
    - (zd) Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
    - (ze) Secure System" means computer hardware, software, and procedure that -:
      - (a) are reasonably secure from unauthorized access and misuse;
      - (b) provide a reasonable level of reliability and correct operation;
      - (c) are reasonably suited to performing the intended functions; and
      - (d) adhere to generally accepted security procedures;
    - (zf) "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;
    - (zg) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued;
    - (zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether
      - (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
      - (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.
- (2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

## 10.8 Information Systems Control and Audit

### 10.3 DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (AMENDED VIDE ITAA 2008) CHAPTER-II]

This chapter gives legal recognition to electronic records and digital signatures. It contains only **section 3**. The section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by any body who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message. In ITAA 2008, this section is given as follows:

#### **[Section 3] Authentication of Electronic Records :**

- (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

#### **Explanation -**

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
- (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

#### **[Section 3A] Electronic Signature (Inserted vide ITAA 2006) :**

- (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-
  - (a) is considered reliable ; and
  - (b) may be specified in the Second Schedule

- (2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-
- (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;
  - (b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
  - (c) any alteration to the electronic signature made after affixing such signature is detectable
  - (d) any alteration to the information made after its authentication by electronic signature is detectable; and
  - (e) it fulfills such other conditions which may be prescribed.
- (3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated
- (4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;
- Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable
- (5) Every notification issued under sub-section (4) shall be laid before each House of Parliament

#### 10.4 ELECTRONIC GOVERNANCE [CHAPTER III]

This chapter is one of the most important chapters. It specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt. This chapter contains sections 4 to 10.

Section 4 provides for “*legal recognition of electronic records*”. It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form. This section is as follows:

##### **[Section 4] Legal Recognition of Electronic Records :**

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

- (a) rendered or made available in an electronic form; and
- (b) accessible so as to be usable for a subsequent reference



## 10.10 Information Systems Control and Audit

Section 5 provides for legal recognition of Digital Signatures. Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly. This section is as follows:

### ***[Section 5] Legal recognition of Electronic Signature :***

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

### **Explanation -**

For the purposes of this section, "Signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "Signature" shall be construed accordingly.

**Section 6** lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any licence or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection. This section is given as under as per ITAA 2008:

### ***[Section 6] Use of Electronic Records and Electronic Signature in Government and its agencies :***

- (1) Where any law provides for
  - (a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
  - (b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
  - (c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

- (2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe
  - (a) the manner and format in which such electronic records shall be filed, created or issued;
  - (b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

**[Section 6A] Delivery of Services by Service Provider (Inserted vide ITAA-2008) :**

- (1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

**Explanation :** For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

- (2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.
- (3) Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.
- (4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

Section 7 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

- (i) The information therein remains accessible so as to be usable subsequently.
- (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.
- (iii) The details which will facilitate the identification of the origin, destination, dates and time of despatch or receipt of such electronic record are available therein.

## 10.12 Information Systems Control and Audit

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. ITAA 2008, this section is given as follows:

### ***[Section 7] Retention of Electronic Records :***

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
  - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
  - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
  - (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

### **However,**

this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation, etc.. in Electronic Gazette.

### ***[Section 7A] Audit of Documents etc in Electronic form :***

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form (ITAA 2008, Standing Committee Recommendation)

Section 8 provides for the publication of rules, regulations and notifications in the Electronic Gazette. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

***[Section 8] Publication of rules, regulation, etc, in Electronic Gazette :***

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

**However**

where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

However, **section 9** of the Act provides that the conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central Government or the State Government.

***[Section 9] Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form :***

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

***[Section 10] Power to make rules by Central Government in respect of Electronic Signature (Modified Vide ITAA 2008) :***

The Central Government may, for the purposes of this Act, by rules, prescribe

- (a) the type of Electronic Signature;
- (b) the manner and format in which the Electronic Signature shall be affixed;
- (c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;
- (d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
- (e) any other matter which is necessary to give legal effect to Electronic Signature.

***10A : Validity of contracts formed through electronic means (Inserted by ITAA 2008)***

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

## 10.14 Information Systems Control and Audit

### 10.5 ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS [CHAPTER IV]

Chapter IV of the Act deals with attribution, receipt and dispatch of electronic records. 'Attribution' means 'to consider it to be written or made by someone'. Hence, this section lays down how an electronic record is to be attributed to the person who originated it. This is given in section 11. As per ITAA 2008, Section 11 is as follows:

#### **[Section 11] Attribution of Electronic Records :**

An electronic record shall be attributed to the originator

- (a) if it was sent by the originator himself;
- (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
- (c) by an information system programmed by or on behalf of the originator to operate automatically.

Section 12 provides for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made. As per ITAA 2008, Section 12 is given as under:

#### **[Section 12] Acknowledgement of Receipt (Modified by ITAA 2008) :**

- (1) Where the originator has not stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -
  - (a) any communication by the addressee, automated or otherwise; or
  - (b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
- (2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
- (3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Section 13 provides for *the manner in which the time and place of despatch and receipt of electronic record* sent by the originator shall be identified. It is provided that in general, an

electronic record is deemed to be despatched at the place where the originator has his place of business and received where the addressee has his place of business. As per ITAA 2008, Section 13 is as follows:

***[Section 13] Time and place of despatch and receipt of electronic record :***

- (1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
- (2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely -
  - (a) if the addressee has designated a computer resource for the purpose of receiving electronic records
    - (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 computer resource of the addressee that is not the designated 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 along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
- (3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to "be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
- (4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
- (5) For the purposes of this section -
  - (a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;
  - (b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
  - (c) "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

## 10.16 Information Systems Control and Audit

### 10.6 SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES [CHAPTER V]

Chapter V sets out the conditions that would apply to qualify electronic records and digital signatures as being secure. It contains sections 14 to 16.

Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. In ITAA 2008, Section 14 is given as follows:

***[Section 14] Secure Electronic Record :***

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 15 provides for the security procedure to be applied to Digital Signatures for being treated as a secure digital signature. In ITAA 2008, Section 15 is given as under:

***[Section 15] Secure Electronic Signature (Substituted vide ITAA 2008) :***

An electronic signature shall be deemed to be a secure electronic signature if-

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed

**Explanation-** In case of digital signature, the "signature creation data" means the private key of the subscriber

Section 16 provides for the power of the Central Government to prescribe the *security procedure* in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc. As per ITAA 2008, Section 16 is given as follows:

***[Section 16] Security procedures and Practices (Amended vide ITAA 2008):***

The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

## 10.7 REGULATION OF CERTIFYING AUTHORITIES (CHAPTER VI)

Chapter VI contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities. It contains sections 17 to 34.

Section 17 provides for the *appointment of Controller and other officers* to regulate the Certifying Authorities. As per ITAA 2008, Section 17 is given as follows:

### **[Section 17] Appointment of Controller and other officers (Amended Vide ITAA 2008) :**

- (1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers, other officers and employees (Inserted vide ITAA 2008) as it deems fit.
- (2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
- (3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
- (4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees (Inserted vide ITAA 2008) shall be such as may be prescribed by the Central Government.
- (5) The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
- (6) There shall be a seal of the Office of the Controller.

Section 18 lays down the *functions which the Controller may perform* in respect of activities of Certifying Authorities. As per ITAA 2008, Section 18 is given as under:

### **[Section 18] The Controller may perform all or any of the following functions, namely :**

- (a) exercising supervision over the activities of the Certifying Authorities;
- (b) certifying public keys of the Certifying Authorities
- (c) laying down the standards to be maintained by the Certifying Authorities;
- (d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
- (e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
- (f) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;
- (g) specifying the form and content of a Electronic Signature Certificate and the key;
- (h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;



## **10.18 Information Systems Control and Audit**

- (i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- (j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
- (k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- (l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
- (m) laying down the duties of the Certifying Authorities;
- (n) maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Section 19 provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

### ***[Section 19] Recognition of foreign Certifying Authorities :***

- (1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
- (2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
- (3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

### ***Section 20 : (Omitted vide ITA 2008)***

Section 21 provides that a licence to be issued to a Certifying Authority to issue *Digital Signature Certificates* by the Controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the licence or reject the application after giving reasonable opportunity of being heard. As per ITAA 2008, Section 21 is given as under:

### ***[Section 21] License to issue electronic signature certificates:***

- (1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a license to issue Electronic Signature Certificates.

- (2) No license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature Certificates as may be prescribed by the Central Government.
- (3) A license granted under this section shall -
  - (a) be valid for such period as may be prescribed by the Central Government;
  - (b) not be transferable or heritable;
  - (c) be subject to such terms and conditions as may be specified by the regulations.

Section 22 provides that the *application for licence* shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant. It shall be further accompanied by a fee not exceeding Rs.25,000 and other documents as may be prescribed by the Central Government. In ITAA 2008, section 22 is given as follows:

**[Section 22] Application for license :**

- (1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
- (2) Every application for issue of a license shall be accompanied by-
  - (a) a certification practice statement;
  - (b) a statement including the procedures with respect to identification of the applicant;
  - (c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
  - (d) such other documents, as may be prescribed by the Central Government.

Section 23 provides that the application for *renewal of a licence* shall be in such form and accompanied by such fees not exceeding Rs.5,000 which may be prescribed by the Central Government. In ITAA 2008, Section 23 is given as follows:

**[Section 23] Renewal of license:**

An application for renewal of a license shall be -

- (a) in such form;
- (b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the license:

Section 24 deals with the procedure for grant or rejection of licence by the controller on certain grounds. No application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case. In ITAA 2008, Section 24 is given as follows:

## 10.20 Information Systems Control and Audit

### **[Section 24] Procedure for grant or rejection of license :**

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

#### **However,**

no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Section 25 provides that the Controller may *revoke a licence* on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Thereafter, the Controller shall publish a notice of suspension or revocation of license as the case may be in the database maintained by him.

Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock. It is also provided that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate. As per ITAA 2008, different sections are given as follows:

### **[Section 25] Suspension of License :**

- (1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has -
  - (a) made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;
  - (b) failed to comply with the terms and conditions subject to which the license was granted;
  - (c) failed to maintain the standards specified in Section 30 [Substituted for the words "under clause (b) of sub-section (2) of section 20;" vide amendment dated September 19, 2002]
  - (d) contravened any provisions of this Act, rule, regulation or order made there under, revoke the license:

#### **However,**

no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

- (2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him:

**However,**

no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

- (3) No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

***[Section 26] Notice of suspension or revocation of license :***

- (1) Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data-base maintained by him.
- (2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

**However,**

the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock

**However,**

that the Controller may, if he considers necessary, publicize the contents of the data-base in such electronic or other media, as he may consider appropriate.

***[Section 27] Power to delegate :***

The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

The Controller or any person authorised by him, shall have access to any computer system, data or any other material connected with such system if he has reasonable cause to suspect that contravention of the provisions of the Act or the rules or regulation is being committed.

***[Section 28] Power to investigate contraventions :***

- (1) The Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.
- (2) The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

***[Section 29] Access to computers and data :***

- (1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any

## 10.22 Information Systems Control and Audit

contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(Amended vide ITAA 2008)

- (2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.

### ***[Section 30] Duties of Certifying Authorities :***

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below: Every Certifying Authority shall-

- (a) make use of hardware, software, and procedures that are secure from intrusion and misuse;
- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- (c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (**Amended vide ITAA 2008**)
  - (ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)
  - (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (**Inserted vide ITAA 2008**)
- (d) observe such other standards as may be specified by regulations.

### ***[Section 31] Certifying Authority to ensure compliance of the Act, etc. :***

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

### ***[Section 32] Display of license :***

Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.

### ***[Section 33] Surrender of license :***

- (1) Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.
- (2) Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offense and shall be

punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

**[Section 34] Disclosure :**

- (1) Every Certifying Authority shall disclose in the manner specified by regulations
  - (a) its Electronic Signature Certificate (Amended vide ITAA 2008)
  - (b) any certification practice statement relevant thereto;
  - (c) notice of revocation or suspension of its Certifying Authority certificate, if any; and
  - (d) any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services
- (2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall-
  - (a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
  - (b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

**10.8 ELECTRONIC SIGNATURE CERTIFICATES [CHAPTER VII]**

Chapter VII of the Act contains Sections 35 to 40.

Section 35 lays down the procedure for issuance of a Digital Signature Certificate. It provides that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000. The fee shall be prescribed by the Central Government, and different fees may be prescribed for different classes of applicants.

The section also provides that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that –

- (a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
- (b) the applicant holds a private key, which is capable of creating a digital signature;
- (c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

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

- (1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

## 10.24 Information Systems Control and Audit

- (2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority :

### However,

while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

- (3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
- (4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application

### However,

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

Section 36 required that while issuing a Digital Signature Certificate, the Certifying Authority should certify that it has complied with the provisions of the Act, the rules and regulations made there under and also with other conditions mentioned in the Digital Signature Certificate.

### Representations upon issuance of Digital Signature Certificate

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

- (a) it has complied with the provisions of this Act and the rules and regulations made there under;
- (b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
- (c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
- (ca) the subscriber holds a private key which is capable of creating a digital signature (Inserted vide ITAA 2008)
- (cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber (Inserted vide ITAA 2008)
- (d) the subscriber's public key and private key constitute a functioning key pair;
- (e) the information contained in the Digital Signature Certificate is accurate; and
- (f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

**[Section 37] Suspension of Digital Signature Certificate :**

The Certifying Authority may suspend such certificate if it is of the opinion that such a step needs to be taken in public interest.

Such certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard.

**Suspension of Digital Signature Certificate**

Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate -

- (a) on receipt of a request to that effect from -
  - (i) the subscriber listed in the Digital Signature Certificate; or
  - (ii) any person duly authorized to act on behalf of that subscriber;
- (b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

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

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

Section 38 provides for the *revocation of Digital Signature Certificates* under certain circumstances. Such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. Upon revocation or suspension the certifying Authority shall publish the notice of suspension or revocation of a Digital Signature Certificate.

**Revocation of Digital Signature Certificate**

A Certifying Authority may revoke a Digital Signature Certificate issued by it

- (a) where the subscriber or any other person authorized by him makes a request to that effect; or
- (b) upon the death of the subscriber; or
- (c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

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

- (a) a material fact represented in the Digital Signature Certificate is false or has been concealed;
- (b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
- (c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;



## 10.26 Information Systems Control and Audit

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

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

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

### ***[Section 39] Notice of suspension or revocation :***

- (1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.
- (2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

## 10.9 DUTIES OF SUBSCRIBERS [CHAPTER VIII]

This Chapter contains **sections 40 to 42**. It specifies duties of subscribers. As per ITAA 2008, different Sections are as under:

### ***[Section 40] Generating Key Pair :***

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, (\*) the subscriber shall generate that [substituted for "the" vide amendment dated 19/09/2002] key pair by applying the security procedure. [\* word "then"-deleted vide amendment dated 19/9/2002],

### ***[Section 40A] Duties of subscriber of Electronic Signature Certificate :***

In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed. (Inserted Vide ITAA 2008)

### ***[Section 41] Acceptance of Digital Signature Certificate :***

- (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate -
- (a) to one or more persons;
  - (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
- (2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –
- (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

- (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

**[Section 42] Control of Private key :**

- (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the r public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.[ "to a person not authorized to affix the digital signature of the subscriber".-Omitted vide amendment dated 19/09/2002]
- (2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

**Explanation** - For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate—

- (a) to one or more persons;
- (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
- (c) Certificate in any manner.

By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

- (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
- (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

## 10.28 Information Systems Control and Audit

### 10.10 PENALTIES AND ADJUDICATION [CHAPTER IX]

Chapter IX contains sections 43 to 47. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudication Officer for holding an inquiry in relation to certain computer crimes and for awarding compensation. Sections 43 to 45 deal with different nature of penalties.

Section 43 deals with penalty for damage to computer, computer system, etc by any of the following methods:

***[Section 43] Penalty and Compensation for damage to computer, computer system, etc. (Amended vide ITAA-2008) :***

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

- (a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)
- (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- (e) disrupts or causes disruption of any computer, computer system or computer network;
- (f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
- (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,
- (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,
- (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008)
- (j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation to the person so affected. (change vide ITAA 2008)

**Explanation** - for the purposes of this section -

- (i) "Computer Contaminant" means any set of computer instructions that are designed -
  - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
  - (b) by any means to usurp the normal operation of the computer, computer system, or computer network;
- (ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- (iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- (iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.
- (v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

**Compensation for failure to protect data (Inserted vide ITAA 2006)**

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected. (Change vide ITAA 2008)

**Explanation:** For the purposes of this section

- (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities
- (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

### 10.30 Information Systems Control and Audit

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

#### **[Section 44] Penalty for failure to furnish information, return, etc. :**

If any person who is required under this Act or any rules or regulations made there under to -

- (a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- (b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:
- (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Section 45 provides for residuary penalty. Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees. As per ITAA 2008, Section 45 is given as under:

#### **[Section 45] Residuary Penalty :**

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

Section 46 confers the *power to adjudicate contravention* under the Act to an officer not below than the rank of a Director to the Government of India or an equivalent officer of a State Government. Such appointment shall be made by the Central Government. In order to be eligible for appointment as an adjudicating officer, a person must possess adequate experience in the field of Information Technology and such legal or judicial experience as may be prescribed by the Central Government. The adjudicating officer so appointed shall be responsible for holding an inquiry in the prescribed manner after giving reasonable opportunity of being heard and thereafter, imposing penalty where required. In ITAA 2008, section 46 is given as follows:

#### **[Section 46] Power to Adjudicate:**

- (1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer

not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government. ( **amended vide ITAA 2008**)

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crores.

Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees five crores shall vest with the competent court. (Inserted Vide ITAA 2008).

- (2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.
- (3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.
- (4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
- (5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and -
  - (a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
  - (b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.
  - (c) shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908 (Inserted vide ITAA 2008)

Section 47 provides that while deciding upon the quantum of compensation, the adjudicating officer shall have due regard to the amount of gain of unfair advantage and the amount of loss caused to any person as well as the respective nature of the default. As per ITAA 2008, Section 47 is given as under:

***[Section 47] Factors to be taken into account by the adjudicating officer :***

While adjudging the quantum of compensation under this Chapter the adjudicating officer shall have due regard to the following factors, namely -

- (a) the amount of gain of unfair advantage, wherever quantifiable, 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

## **10.32 Information Systems Control and Audit**

### **10.11 THE CYBER APPELLATE TRIBUNAL (Amended vide ITA-2008) [Chapter X]**

The “Cyber Regulations Appellate Tribunal” has appellate powers in respect of orders passed by any adjudicating officer. Civil courts have been barred from entertaining any suit or proceeding in respect of any matter which an adjudicating officer or Tribunal is empowered to handle.

Section 48 provides for establishment of one or more Appellate Tribunals to be known as Cyber Regulations Appellate Tribunals.

The Cyber Regulations Appellate Tribunal shall consist of one person only (called the Presiding Officer of the Tribunal) who shall be appointed by notification by the Central Government. Such a person must be qualified to be a judge of a High Court or is or has been a member of the Indian Legal Service in the post in Grade I of that service for at least three years.

The Presiding Officer shall hold office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier. As per ITAA 2008 different sections are given as follows:

#### ***[Section 48] Establishment of Cyber Appellate Tribunal :***

- (1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.
- (2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

#### ***[Section 49] Composition of Cyber Appellate Tribunal (Substituted vide ITAA 2008) :***

- (1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint (Inserted vide ITAA-2008).

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted Vide ITAA 2008).

- (2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. (Inserted vide ITAA-2008).
- (3) Subject to the provisions of this Act-
  - (a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof
  - (b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.

Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 (ITAA 2008)

- (c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.
- (d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(Inserted vide ITAA-2008).

- (4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench (Inserted vide ITAA-2008)
- (5) If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. (Inserted vide ITAA-2008)

***[Section 50] Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal (Substituted vide ITAA 2006) :***

- (1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court; (substituted vide ITAA-2008)
- (2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the central Government or State Government for a period of not less than seven years.

(Inserted vide ITAA-2008)

- (3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that service for a period of not less than five years.



## 10.34 Information Systems Control and Audit

### ***[Section 51] Term of office, conditions of service etc of Chairperson and Members (Substituted vide ITAA 2008) :***

- (1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier. (Inserted vide ITAA 2008)
- (2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member. (Inserted vide ITAA 2008)
- (3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member. (Inserted vide ITAA 2008).

Section 52 provides for the salary and allowances and other terms and conditions of service of the presiding Officer.

### ***[Section 52] Salary, allowance and other terms and conditions of service of Chairperson and Member (Substituted vide ITAA 2008) :***

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed: (Inserted vide ITAA 2008)

### ***[Section 52A] Powers of superintendence, direction, etc (Inserted vide ITAA 2008) :***

The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

### ***[Section 52B] Distribution of Business among Benches (Inserted vide ITAA 2008):***

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

### ***[Section 52C] Powers of the Chairperson to transfer cases (Inserted vide ITAA 2008):***

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

### ***[Section 52D] Decision by majority (Inserted vide ITAA 2008) :***

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the

Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

Section 53 provides that in the situation of any vacancy occurring in the office of the Presiding officer of Cyber Regulations Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act.

***[Section 53] Filling up of vacancies (Amended vide ITAA 2008) :***

If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

***[Section 54] Resignation and removal (Amended vide ITAA 2008) :***

(1) The Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

**However,**

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

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

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

***[Section 55] Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings (Inserted vide ITAA 2008) :***

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

***[Section 56] Staff of the Cyber Appellate Tribunal (Error in amendment...item 28) :***

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

### **10.36 Information Systems Control and Audit**

- (2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.
- (3) The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

#### ***[Section 57] Appeal to Cyber Regulations Appellate Tribunal :***

- (1) Save as provided in sub-section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter
- (2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
- (3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

#### **However,**

the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

- (4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against
- (5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.
- (6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

#### ***[Section 58] Procedure and Powers of the Cyber Appellate Tribunal :***

- (1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
- (2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -
  - (a) summoning and enforcing the attendance of any person and examining him on oath;
  - (b) requiring the discovery and production of documents or other electronic records;

- (c) receiving evidence on affidavits;
- (d) issuing commissions for the examination of witnesses or documents;
- (e) reviewing its decisions;
- (f) dismissing an application for default or deciding it ex parte
- (g) any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

***[Section 59]: Right to legal representation :***

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

***[Section 60] Limitation :***

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

***[Section 61] Civil court not to have jurisdiction (Amended vide ITAA 2008) :***

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

Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter. (Inserted vide ITAA 2006).

***[Section 62] Appeal to High court :***

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

**However,**

the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

**Compounding of contravention**

Section 63 provides that any contravention under the Act may be compounded by the Controller or adjudication officer, either before or after the institution of the adjudication proceedings subject to such conditions as he may impose.

## 10.38 Information Systems Control and Audit

It is also provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded. However, these provisions shall not apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention committed by him, was compounded.

### **[Section 63] Compounding of Contravention :**

- (1) Any contravention under this Act [substituted for "Chapter" vide amendment dated 19/09/2002] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

#### **However,**

such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

- (2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

**Explanation** - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

- (3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

### **Recovery of Penalty**

Section 64 provides for recovery of penalty as arrears of land revenue and for suspension of the license or Digital Signature Certificate till the penalty is paid.

### **[Section 64] Recovery of Penalty or compensation (Amended vide ITAA 2006) :**

A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

## 10.12 OFFENCES [CHAPTER XI]

Chapter XI deals with some computer crimes and provides for penalties for these offences. It contains sections 65 to 78.

Section 65 provides for punishment up to three years or with a fine which may extend to Rs. 2 lakhs or with both whoever knowingly or intentionally tampers with the computer code source documents.

“Computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. As per ITAA 2008, Section 65 is given as follows:

**[Section 65] Tampering with Computer Source Documents :**

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

**Explanation -**

For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

**Hacking with computer system**

‘Hacking’ is a term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the public or that person. Section 66 provides that a person who commits hacking shall be punished with a fine upto Rs.2 lakhs or with imprisonment upto 3 years, or with both. As per ITAA 2008, Section 66 is given as follows:

**[Section 66] Computer Related Offences (Substituted vide ITAA 2008) :**

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

**Explanation :** For the purpose of this section,-

- (a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
- (b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

**[Section 66 A] Punishment for sending offensive messages through communication service, etc.( Introduced vide ITAA 2008) :**

Any person who sends, by means of a computer resource or a communication device,-

- (a) any **information** that is grossly offensive or has menacing character; or
- (b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently **by making** use of such computer resource or a communication device,

## 10.40 Information Systems Control and Audit

- (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (**Inserted vide ITAA 2008**) shall be punishable with imprisonment for a term which may extend to three years and with fine.

**Explanation :** For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

***[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008) :***

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

***[Section 66C] Punishment for identity theft. (Inserted Vide ITA 2008) :***

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

***[Section 66D] Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008) :***

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

***[Section 66E] Punishment for violation of privacy. (Inserted Vide ITA 2008) :***

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

**Explanation -** For the purposes of this section--

- (a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;
- (b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;
- (c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

- (d) “publishes” means reproduction in the printed or electronic form and making it available for public;
- (e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that--
  - (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
  - (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

**[Section 66F] Punishment for cyber terrorism :**

- (1) Whoever,-
  - (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –
    - (i) denying or cause the denial of access to any person authorized to access computer resource; or
    - (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
    - (iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or
  - (B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.
- (2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life’.

**Publishing of information which is obscene in electronic form**

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a



## 10.42 Information Systems Control and Audit

term which may extend to ten years and fine which may extend to Rs. 2 lakhs. As per ITAA 2008, Section 67 is given as under:

### ***[Section 67] Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008) :***

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

### ***[Section 67 A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008) :***

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

**Exception :** This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

- (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or
- (ii) which is kept or used bona fide for religious purposes.

### ***[Section 67 B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form :***

Whoever,-

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
- (d) facilitates abusing children online or

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

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

- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
- (ii) which is kept or used for bonafide heritage or religious purposes

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

***[Section 67 C] Preservation and Retention of information by intermediaries :***

- (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- (2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Section 68 provides that the controller may give directions to a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, so as to ensure compliance with this law. If any person fails to comply, he shall be liable to imprisonment upto 3 years or fine upto Rs.2 lakhs, or both. As per ITAA 2008, Section 68 is given as under:

***[Section 68] Power of Controller to give directions (Amended Vide ITAA 2008) :***

- (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.
- (2) Any person who **intentionally or knowingly** (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

## 10.44 Information Systems Control and Audit

Section 69 empowers the Controller, if he is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign states or public order, to intercept any information transmitted through any computer system or computer network. As per ITAA 2008, Section 69 is given as follows:

### ***[Section 69] Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008) :***

- (1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
- (2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
- (3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -
  - (a) provide access to **or secure access to** the computer resource generating, transmitting, receiving or storing such information; or
  - (b) intercept or monitor or decrypt the information, **as the case may be**; or
  - (c) provide information stored in computer resource.
- (4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

### ***[Section 69 A] Power to issue directions for blocking for public access of any information through any computer resource :***

- (1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

- (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
- (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

***[Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security :***

- (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
- (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
- (3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
- (4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

**Explanation :** For the purposes of this section,

- (i) "Computer Contaminant" shall have the meaning assigned to it in section 43
- (ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications 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. As per ITAA 2008, Section 70 is given as under:

***[Section 70] Protected system (Amended Vide ITAA-2008) :***

- (1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

## 10.46 Information Systems Control and Audit

**Explanation :** For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. (Substituted vide ITAA- 2008)

- (2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)
- (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
- (4) The Central Government shall prescribe the information security practices and procedures for such protected system. (Inserted vide ITAA 2008)

### ***[Section 70 A] National nodal agency. (Inserted vide ITAA 2008) :***

- (1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
- (2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
- (3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

### ***[Section 70 B] Indian Computer Emergency Response Team to serve as national agency for incident response :***

- (1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.
- (2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.
- (3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.
- (4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-
  - (a) collection, analysis and dissemination of 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, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
  - (f) such other functions relating to cyber security as may be prescribed
- (5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.
- (6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person
- (7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
- (8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1)

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. As per ITAA 2008, Section 71 is given as follows:

***[Section 71] Penalty for misrepresentation :***

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, 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. As per ITAA 2008, Section 72 is given as under:

***[Section 72] Breach of confidentiality and privacy :***

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

## 10.48 Information Systems Control and Audit

### ***[Section 72 A] Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008) :***

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

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. As per ITAA 2008, Section 73 is given as follows:

### ***[Section 73] Penalty for publishing electronic Signature Certificate false in certain particulars :***

- (1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that
  - (a) the Certifying Authority listed in the certificate has not issued it; or
  - (b) the subscriber listed in the certificate has not accepted it; or
  - (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation
- (2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74 provides for punishment with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both to a person whoever knowingly publishes for fraudulent purpose any Digital Signature Certificate. As per ITAA 2008, Section 74 is given as follows:

### ***[Section 74] Publication for fraudulent purpose :***

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, 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. As per ITAA 2008, Section 75 is given as follows:

**[Section 75] Act to apply for offence or contraventions committed outside India :**

- (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
- (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person 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.

It is also provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening the provisions of this Act, rules, orders or regulations made there under as it may think fit. Section 76 is as under:

**[Section 76] Confiscation:**

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

**However,**

where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Section 77 further provides that penalty and confiscation provided under this Act shall not interfere with other punishments provided under any other law for the time being in force. Different parts of Section 77 is as follows:

**[Section 77] Compensation, penalties or confiscation not to interfere with other punishment. (Substituted Vide ITAA-2008) :**

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. Different subsections of the section is given as follows:



## 10.50 Information Systems Control and Audit

### **[Section 77 A] Compounding of Offences :**

- (1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

- (2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

### **[Section 77 B] Offences with three years imprisonment to be cognizable :**

Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Section 78 provides for power to investigate the offences under the Act by a police officer not below the rank of Deputy Superintendent of Police. This is as follows:

### **[Section 78] Power to investigate offences (Amended Vide ITAA 2008) :**

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act. (Amended Vide ITAA 2008)

## **10.13 INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES (SUBSTITUTED VIDE ITA-2006) [CHAPTER XII]**

Chapter XII contains section 79 which provides that the Network Service Providers shall 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.

**Explanation** – For the purposes of this section,-

- (a) “network service provider” means an intermediary;
- (b) “third party information” means any information dealt with by a network service provider in his capacity as an intermediary; Section 79 is as follows:

### **[Section 79] Exemption from liability of intermediary in certain cases :**

- (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. (corrected vide ITAA 2008)
- (2) The provisions of sub-section (1) shall apply if-

- (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
  - (b) the intermediary does not-
    - (i) initiate the transmission,
    - (ii) select the receiver of the transmission, and
    - (iii) select or modify the information contained in the transmission
  - (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)
- (3) The provisions of sub-section (1) shall not apply if
- (a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)
  - (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

**Explanation :** For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

#### **Examiner of Electronic Evidence (Inserted Vide ITA-2006) (CHAPTER XII A)**

##### ***[Section 79A] Central Government to notify Examiner of Electronic Evidence :***

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

**Explanation:-** For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

#### **10.14 MISCELLANEOUS [CHAPTER XIII]**

Some miscellaneous sections are as under:

##### ***[Section 80] Power of Police Officer and Other Officers to Enter, Search, etc. :***

- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a **Inspector** or any other officer of the Central Government

## 10.52 Information Systems Control and Audit

or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

### **Explanation**

For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

- (2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
- (3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section

### ***[Section 81] Act to have Overriding effect :***

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 (Inserted Vide ITAA 2008)

### ***[Section 81-A] : Application of the Act to Electronic cheque and Truncated cheque- (Inserted vide Negotiable Instruments Amendment Act 2002, - Effective from 6th Day of February 2003) :***

- (1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.
- (2) Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

**Explanation :** For the purpose of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act 1881 (26 of 1881).

**[Section 82] : Chairperson, Members, Officers and Employees to be Public Servants (Amended Vide ITA-2008) :**

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be Public Servants within the meaning of section 21 of the Indian Penal Code.

**[Section 83] Power to Give Direction :**

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made there under.

**[Section 84] Protection of Action taken in Good Faith :**

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

**[Section 84 A] Modes or methods for encryption (Inserted Vide ITA-2008) :**

The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption

**[Section 84 B] Punishment for abetment of offences (Inserted Vide ITA-2008) :**

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

**Explanation:** An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

**[Section 84 C] Punishment for attempt to commit offences (Inserted Vide ITA-2008) :**

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

**[Section 85] Offences by Companies :**

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

## 10.54 Information Systems Control and Audit

### However,

Nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

### Explanation-

For the purposes of this section

- (i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
- (ii) "Director", in relation to a firm, means a partner in the firm

### **[Section 86] Removal of Difficulties :**

- (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

### However,

no order shall be made under this section after the expiry of a period of two years from the commencement of this Act. (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

### **[Section 87] Power of Central Government to make rules :**

- (1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely
  - (a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A (Substituted vide ITA-2008)
    - (aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) of section 3A (Inserted Vide ITA-2006) (Inserted vide ITAA-2008)
    - (ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5. (Inserted vide ITAA-2008)

**Information Technology (Amended) Act, 2008 10.55**

- (b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;
- (c) the manner and format in which electronic records shall be filed or issued and the method of payment under sub-section (2) of section 6;
  - (ca) the manner in which the authorized service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A (Inserted vide ITAA-2008)
- (d) the matters relating to the type of Electronic Signature, manner and format in which it may be affixed under section 10;
- (e) the manner of storing and affixing electronic signature creation data under section 15 (substituted vide ITAA-2008)
  - (ea) the security procedures and practices under section 16 (Inserted vide ITAA-2008)
- (f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers, other officers and employees under section 17; (ITAA 2008)
- (g) (omitted vide ITAA-2008)
- (h) the requirements which an applicant must fulfill under sub-section (2) of section 21;
- (i) the period of validity of license granted under clause (a) of sub-section (3) of section 21;
- (j) the form in which an application for license may be made under subsection (1) of section 22;
- (k) the amount of fees payable under clause (c) of sub-section (2) of section 22;
- (l) such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;
- (m) the form and the fee for renewal of a license and the fee payable thereof under section 23;
  - (ma) the form of application and fee for issue of Electronic Signature Certificate under section 35.(Inserted vide ITAA-2008)
- (n) the amount of late fee payable under the proviso to section 23;
- (o) the form in which application for issue of a Electronic Signature Certificate may be made under sub-section (1) of section 35;
- (oa) the duties of subscribers under section 40A (Inserted vide ITAA-2008)
- (ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A (Inserted vide ITAA-2008)

## 10.56 Information Systems Control and Audit

- (p) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;
- (q) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;
- (r) the qualification and experience which the adjudicating officer shall possess under sub-section (2) of section 46; (Ed: error in the act item number (vii). Bill mentions correction not in the original section-"Presiding Officer" to be replaced with "Chairman and Members")
- (s) the salary, allowances and the other terms and conditions of service of the Chairman and Members under section 52; (amended vide ITAA-2008)
- (t) the procedure for investigation of misbehaviour or incapacity of the Chairman and Members under sub-section (3) of section 54; (Ed: Error: bill mentions corrections to (r) and (s) instead of (s) and (t))
- (u) the salary and allowances and other conditions, of service of other officers and employees under sub-section (3) of section 56;
- (v) the form in which appeal may be filed and the fee thereof under subsection (3) of section 57;
- (w) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52 A (substituted vide ITAA-2008)
- (wa) the information, duration, manner and form of such information to be retained and preserved under section 67 C (ITAA 2008)
- (x) The Procedures and safeguards for interception, monitoring or decryption under sub-section (2) of section 69 (ITAA 2008)
  - (xa) the procedure and safeguards for blocking for access by the public under sub-section (2) of section 69 A. (ITAA 2008)
  - (xb) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of section 69 B (ITAA 2008)
- (y) the information security practices and procedures for protected system under section 70 (Inserted vide ITAA-2008)
  - (ya) manner of performing functions and duties of the agency under sub-section (3) of section 70 A (ITAA 2008)
  - (yb) the officers and employees under sub-section (2) of section 70 (B) (ITAA 2008)
  - (yc) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70 B (ITAA 2008)
  - (yd) the manner in which the functions and duties of agency shall be performed under sub-section (5) of section 70 B (ITAA 2008)

- (z) the guidelines to be observed by the intermediaries under sub section ~~(4)~~ (2) of section 79 (Inserted vide ITAA-2008)
  - (za) the modes or methods for encryption under section 84A (Inserted vide ITAA-2008).
- (3) Every notification made by the Central Government under sub-section (1) of section 70 (A) and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation. (ITAA 2008).

***[Section 88] Constitution of Advisory Committee :***

- (1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.
- (2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.
- (3) The Cyber Regulations Advisory Committee shall advise –
  - (a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;
  - (b) the Controller in framing the regulations under this Act
- (4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

***[Section 89] Power of Controller to make Regulations :***

- (1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made there under to carry out the purposes of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely
  - (a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (n) [Substituted for (m) vide amendment dated 19/09/2002] of section 18;



## **10.58 Information Systems Control and Audit**

- (b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority under sub-section (1) of section 19;
  - (c) the terms and conditions subject to which a license may be granted under clause (c) of sub-section (3) of section 21;
  - (d) other standards to be observed by a Certifying Authority under clause (d) of section 30;
  - (e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;
  - (f) the particulars of statement which shall accompany an application under sub-section (3) of section 35
  - (g) the manner by which a subscriber communicates the compromise of private key to the Certifying Authority under sub-section (2) of section 42.
- (3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive- sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall there after have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

### ***[Section 90] Power of State Government to make rules :***

- (1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely :
  - (a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
  - (b) for matters specified in sub-section (2) of section 6;
- (3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

***Sections 91, 92, 93, 94 are omitted vide ITAA, 2006.***

**Self - Examination Questions**

1. What are the major objectives of enacting the Information Technology Act, 2000?
2. What all are included in the definition of computer network, computer system, and data under the Act?
3. What is a secure system under Information Technology Act, 2000? Has the act suggested any technical standards for a system to be recognized as a secured system?
4. What is a digital signature? What are the attributes of a digital signature and explain that how is a document authenticated through a digital signature?
5. Explain, in short, how does enactment of Information Technology Act, 2000 paves the way for electronic governance in India?
6. What are the duties of a subscriber of a digital signature?
7. What are the major penal provisions under Information technology Act, 2000?
8. What are the powers of Cyber Appellate Tribunal? When can one make an appeal to the tribunal?
9. What are the powers of a Police Officer under the Information Technology Act to enter and search a public place?
10. What are the liabilities of companies under section 85 of the Information Technology Act?
11. Discuss the major differences between original IT Act 2000 and ITAA 2008?

**Sources :**

1. [www.legalserviceindia.com/cyber/itact.html](http://www.legalserviceindia.com/cyber/itact.html)
2. [www.nicca.nic.in/pdf/itact2000.pdf](http://www.nicca.nic.in/pdf/itact2000.pdf)
3. [www.eprocurement.gov.in/news/actzeromod.pdf](http://www.eprocurement.gov.in/news/actzeromod.pdf)
4. [www.naavi.org/ita-2006/index.html](http://www.naavi.org/ita-2006/index.html).