

**FINAL 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.

Edition : January, 2015

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

Department/  
Committee : Board of Studies

E-mail : [bosnoida@icai.in](mailto:bosnoida@icai.in)

ISBN No. :

Price :

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 :

# SYLLABUS

---

## PAPER 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

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

**Level of Knowledge:** Advanced Knowledge

**Objective:**

“To develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant”.

**Contents:**

- 1. Concepts of Governance and Management of Information Systems:** Governance, Risk and compliance and relationship between governance and management.  
Role of information technology and IS Strategy in business strategy, operations and control , business value from use of IT, business impact of IS risks different types of Information Systems Risks, IS Risk management overview, IT Compliance overview – Role and responsibilities of top management as regards IT-GRC. Role of Information Systems Assurance. Overview of Governance of Enterprise IT and COBIT.
- 2. Information Systems Concepts:** Overview of information systems in IT environment and practical aspects of application of information systems in enterprise processes. Information as a key business asset and its relation to business objectives, business processes and relative importance of information systems from strategic and operational perspectives. Various types of business applications, overview of underlying IT technologies.
- 3. Protection of Information Systems:** Need for protection of Information systems, types of controls, IT general controls, logical access controls & application controls. Technologies and security management features, IS Security Policies, procedures, practices, standards and guidelines, IT controls and control objectives, Role of technology systems in control monitoring, segregation of duties. Impact of IT controls on Internal controls over financial reporting, cyber frauds and control failures.
- 4. Business Continuity Planning and Disaster recovery planning:** Assessing Business Continuity Management, Business Impact Analysis and Business Continuity Plans, Disaster recovery from perspective of going concern, Recovery Strategies.
- 5. Acquisition, Development and Implementation of Information Systems (SDLC):** Business process design (integrated systems, automated, and manual interfaces), Software procurement, RFP process, evaluation of IT proposals, computing ROI,

Computing Cost of IT implementation and cost benefit analysis, systematic approach to SDLC and review of SDLC controls at different stages.

6. **Auditing of Information Systems:** Different types of IS audit and assurance engagements. Evaluating IT dependencies for audit planning. Overview of continuous auditing. Auditing Information Systems- Approach methodology, and standards for auditing information systems. IS Audit planning, performing an IS audit, rules of digital evidence, best practices and standards for IS audit. Reviewing General Controls, Application Controls, Application control reviews: Review of controls at various levels/layers such as: Parameters, user creation, granting of access rights, input, processing and output controls.
7. **Information Technology Regulatory Issues:** Overview of Specific section of IT Act 2008 & Rules as relevant for assurance: Electronic Contracting, digital signatures, cyber offences, etc. Need for systems audit as per various regulations such as: SEBI Clause 49 listing requirements and internal controls, systems control & audit requirements as per RBI, SEBI, IRDA. Concepts of Cyber forensics/Cyber Fraud investigation, Overview of Information Security Standards ISO 27001, ISAE 3402/SA 402, ITIL.
8. **Emerging Technologies:** Overview of Cloud Computing, Software as a Service, Mobile Computing & BYOD, Web 2.0 & social media, Green IT and related security and audit issues.

## A WORD ABOUT STUDY MATERIAL

---

In today's business world, accounting professionals have to interact with computer-based Information systems on a regular basis. As primary users of information systems in organizations, accountants participate in their design and understand their operations. 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.

Recognizing the importance of Information Technology (IT), the Chartered Accountancy course has also included it as a part of the course curriculum both at Intermediate (IPC) and Final levels. A paper on Information Systems Control and Audit forming a part of the final course helps the students to develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant. The basic knowledge about IT gained at Intermediate (IPC) level is sought to be built up further through this paper.

In this fast changing world of Information and Communication Technologies, the Institute felt an urgent need to relook the syllabus of IT related papers separately and hence, the syllabus of 'Information Systems Control and Audit' has been revised with a view to rationalize the same in the light of recent technological developments by making necessary additions/deletions and modifications therein.

The Study Material of this paper covering the theoretical framework in detail has also been revised, accordingly. However, it is also noteworthy to mention here that in addition to the Study Material, students may also refer the recommended reading books available on this paper to enrich their knowledge levels. In addition, they are also advised to update themselves with the latest changes in the IT sector. For this, they may refer the monthly journal 'The Chartered Accountant' and the Students' Journal published by the Institute and also other IT Journals/Magazines. Chapter-wise coverage of this Study material is given as follows:

Chapter 1 of the study material is devoted to the discussion on concept of Governance and management of Information Systems. In addition, the role of IT in businesses, operations and controls, business impact of IS risks, role and responsibilities of top management as regards IT-GRC etc. have also been covered.

Chapter 2 deals with the basic concepts of Information System and its various types like MIS, DSS, TPS, EIS etc.

Chapter 3 discusses the protection of Information Systems. It highlights the importance of Information Security in today's vulnerable IT world, its policies, related standards/guidelines and also provides a detailed discussion on IS Controls, their objectives and functions with reference to Information Systems. Understanding of these controls is essential to the Chartered Accountants to strengthen their ability for conducting IS Audit in any organization.

Chapter 4 outlines Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) along with its related concepts.

Chapter 5 deals with systems development process for an information system. Various stages of systems development life cycle are also discussed. In this chapter, students will also get an idea 'how computerized 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 6 is devoted to the auditing of Information Systems. It highlights the IS Audit planning, performing an IS audit, rules of digital evidence, best practices and standards for IS audit etc. In addition, the chapter also emphasizes on the reviewing of General and Application Controls.

Chapter 7 extensively deals with IT Regulatory issues. Along with a wide coverage of the relevant sections of IT Act 2000, other related regulatory issues e.g. need for system audit as per Clause 49 of SEBI listing requirements and audit requirements as per RBI, IRDA have also been discussed in the chapter.

Chapter 8 is devoted to the emerging technologies. Major evolving technologies/concepts like Cloud Computing, Mobile Computing, BYOD, Web 2.0 & Social Media and Green IT etc. have been covered in this chapter to make the students familiar with such technological developments.

The significant additions in the revised edition are highlighted in bold and Italics and have also been consolidated in the form of table "Significant additions in the Edition" in subsequent page.

In case you need any further clarification/guidance, please send your queries at [bosnoida@icai.in/](mailto:bosnoida@icai.in)  
[sukriti.arora@icai.in](mailto:sukriti.arora@icai.in).

*Happy Reading and Best Wishes!*

## SIGNIFICANT ADDITIONS/AMENDMENTS IN THIS EDITION

Chapter No.	Chapter Name	Sections/Sub Sections wherein major additions/updates have been done	Page Numbers
1.	Concepts of Governance and Management of Information Systems	Fig. 1.2.1: Enterprise Governance Framework	1.3
		1.10.3 Components in COBIT	1.27
		1.10.4 Benefits of COBIT 5	1.28
		1.10.7 COBIT 5 Process Reference Model	1.31 -1.32
2.	Information Systems Concept	Fig. 2.2.4: Types of Information Systems and the Groups Served	2.10
		2.2.5 Types of Information Systems	2.15 - 2.17
		2.2.6 Specialized Systems	2.31 – 2.33
3.	Protection of Information Systems	3.5.4 Impact of Technology on Internal Controls	3.11 – 3.12
		3.6.4 Classification on the basis of " Audit Functions"	3.36 – 3.37
		3.7 Managerial Controls and their Categories	3.38 – 3.41
		3.8.3 Communication Controls	3.47 – 3.50
		3.8.4 Processing Controls	3.50 – 3.51
6.	Auditing of Information Systems	6.7 Application Controls and their Audit Trails	6.27 – 6.30
7.	Information Technology Regulatory Issues	7.13.1 ISO 27001	7.39 – 7.41
		Fig. 7.13.1: PDCA Cycle	7.40
		7.13.3 Information Technology Infrastructure Library (ITIL)	7.43 – 7.46
		Fig. 7.13.2: ITIL V3	7.47

# STUDY PLAN – KEY TO EFFECTIVE LEARNING

---

## Introduction

The primary objective for the inclusion of the 'Information Systems Control and Audit' paper at the Final Level of the Chartered Accountancy course is to provide conceptual understanding of different aspects of IT risks, security, controls and auditing various aspects of IT processes. This paper enables to understand the enterprise level aspects of governance, risk, compliance, assurance as applicable to enterprises. While updating this paper, the primary rationale has been to ensure the coverage of the latest concepts of Governance, Risk and Compliance (GRC), which has been a regulatory requirement not only for listed enterprises but also for all types of enterprises. Further, implementing GRC in an IT environment requires updated knowledge and skills based on the latest developments and best practices and this is sought to be provided through this paper. Students are advised to read these topics not only from examination point of view but keeping in mind the fact that these topics are highly relevant to their work as articles and in their careers whether they seek to be employed in enterprises or self-employed.

The topics have been given so as to link all the topics together from the macro perspective of Governance, risk, compliance and assurance to the micro perspective and implementation level so that a blend of both concepts as well as the practical aspects could be provided. This knowledge will equip CA students with holistic approach to IT assurance rather than function oriented IS control and audit perspective. This will provide the required competency to meet the challenges of IT environment, which they face in their work area.

Before going to the chapter-wise specific tips, it is important to understand the detailed learning objectives that are given below:

- To understand the key concepts of Governance, Risk and Compliance aspects in enterprises as relevant to IT;
- To identify and review IT risks, security, controls and risk management approach;
- To assess impact on controls and organisation structure on account of integration of technological applications and resources into operational processes;
- To assess Business Continuity Plans of enterprises for adequacy from perspective of going concern;
- To assess information systems acquisition, development and implementation strategy including review of Systems Development Life Cycle (SDLC) process;
- To understand how to perform auditing including collecting and evaluating evidence in an IT environment;
- To understand the relevant regulatory procedures, guidelines and standards; and



- To have an overview of IT best practices and impact of emerging technologies on enterprises.

### **Chapter-wise Tips for Preparation**

While studying ISCA paper, students should try to understand the linkages between the chapters at macro-level. This will help them in recollecting the concepts during examination. Chapter-wise suggestions are given as follows:

1. First of all, students should understand the key points covered in the first chapter. The usage of IT is rapidly increasing in most of the large enterprises and also to a great extent even in small and medium enterprises. There is no doubt to say that IT is at the core of most of the key business operations. Further, there is an increasing thrust on corporate governance by regulators encompassing governance, risk management and controls. The use of IT covering all key aspects of business processes of an enterprise impacts not only 'how information is processed' but also 'how computerized information systems are used for strategic and competitive advantage'. Internal controls are integral part of information systems of an enterprise. Hence, it is important to understand 'how information systems are organized' and 'how controls are integrated'. In this chapter, students should understand the relevance of IT in Governance and other related concepts. Further, they should cover the topic IT Governance and Governance on Enterprise IT (GEIT).

Afterwards, students should also understand that successful design and deployment of information systems using IT, determines the success of an enterprise. Hence, it is critical to ensure that the required controls are implemented not only from IT perspective but also from management and regulatory perspective. This requires that the controls are implemented from Governance perspective using a holistic approach and has involvement of the senior management as required. Implementing IT Governance as subset of enterprise governance ensures that implementation of IT meets all the stakeholder requirements including regulators and management. Regulatory requirements mandate not only implementation of governance but also its independent evaluation. Hence, auditors are required to evaluate these aspects in their roles as internal or external auditors. As IT proliferates, there is increasing demands for pro-active objective assessments of governance, risk, compliance and controls of information systems. Accordingly, students should understand the Enterprise Risk Management, internal controls and related concepts. They should also cover various concepts relating to risk namely, vulnerabilities, attacks, threats etc. Once conceptual clarity has been acquired, students should have an idea about Risk assessment/management process. Finally, students should thoroughly study COBIT 5, which is a well-known GEIT Framework used by the enterprises worldwide.

2. As the name of the paper is 'Information Systems Control and Audit'; it is essential that students should understand about the information systems and its related concepts. Accordingly, second chapter of ISCA is on "Information Systems Concepts", which provides an overview of different information systems. In this chapter, students should clearly understand the general concepts of the systems, and their types. In addition, they should also understand the practical aspects of application of information systems in various processes of an enterprise. Further, they should realize that information is a key business asset and

accordingly, they should thoroughly study the topic 'information' and its various attributes. Afterwards, students should understand the relative importance of information systems from strategic and operational perspective along with different types of information systems such as MIS, DSS, EIS, and ES etc. For each type of information systems, its features, attributes, advantages, and limitations must be clearly understood. Students should thoroughly understand the key points given in the material; however, they may write the description of these points in their own language with full coverage of related concepts. Finally, they should also have an overview of underlying IT technologies.

3. Information security plays a vital role in today's highly connected world. Any information system must have three fundamental aspects: resist, tolerate and recover. Hence, the third chapter is dedicated to protection of Information Systems and its related concepts. Students should clearly understand the need for information security and its importance to enterprises, its detailed concepts, various information security policies and their hierarchy. In addition, they should also focus on different categories of information that may be considered sensitive and how the same needs to be protected.

A control is a system that prevents, detects, or corrects unlawful events. In an information system, necessary controls must be incorporated at the appropriate places starting from the development itself. Keeping in mind the aforementioned fact, the chapter provides a detailed discussion on the controls. Accordingly, students should understand the need for the controls and related topics. They should also understand responsibility for controls from the perspective of Management, IT, Personnel, Auditors, and cost effectiveness of control procedures. Then, they should try to understand various IS Control Techniques and particularly User Controls. Afterwards, they should clearly understand the controls over data integrity and security, which are very essential towards protection of information systems. In addition, they should also cover Logical & Physical Access Controls and Environmental Controls along with their related concepts. Understanding of these controls is essential to the Chartered Accountants to strengthen their ability for conducting IS Audit in any organization. Students should also have an in-depth knowledge of Cyber Frauds following by major cyber-attacks as reported by different monitoring agencies like CERT-IN in India. They should also have an overview of the techniques to commit cyber frauds and finally, the students should assess the impact of these cyber frauds on business enterprises.

4. Information systems should continue without fail at any circumstances. 'What strategies should be followed to achieve this goal' is discussed in the fourth chapter on Business Continuity Planning and Disaster Recovery Planning. First of all, students should realize the need for Business Continuity Management (BCM) in enterprises, and understand BCM Policy, Business Continuity Planning (BCP) and its objectives/goals in depth. Moreover, students should know that how Business Continuity Plan is actually developed, covering all the eight phases. Students should also focus on various backup techniques and disaster recovery plans. Further, various audit tools and techniques must be understood by the students and finally, audit of Disaster Recovery and Business Continuity Plan must be covered in detail, which focuses on various important checkpoints relating to auditing.

5. As the paper is basically dedicated to Information Systems Controls; only the generalized knowledge of information systems is not sufficient rather various concepts of the Software Development Life Cycle (SDLC) are also needed. Accordingly, the fifth chapter is on SDLC in which all the relevant concepts of SDLC for a Chartered Accountant perspective are introduced. In this chapter, students should grasp the key issues for the system development process. They should understand the Request For Proposal (RFP) process and its evaluation along with the concepts of Return on Investment (RoI) in terms of investments made in systems. Afterwards, concepts relating to all the development models namely Waterfall, Spiral etc. used for developing the software should be clearly understood. Normally, the weaknesses of the previous model are addressed by the next model, and these weaknesses become the strengths of the current model. In this way, students may remember the concepts of various models. Further, it also establishes a link between the need for businesses and the method adopted to develop the suitable information system for them.

Further, all the phases of SDLC namely Preliminary Investigation, Requirements Analysis, Designing, Coding, Testing, Implementation, and Maintenance should be studied with the coverage of all the major activities in each of the phases in detail. Here, it is also noteworthy to mention that students must have the knowledge of appropriate controls required for various stages of SDLC starting from Preliminary Investigation till Maintenance. Finally, a checklist relating to SDLC is also included at the end of this chapter, which should be clearly understood by the students.

6. Sixth Chapter is on auditing of information systems. In the chapter, first of all, students should understand Information System Audit and the method of performing the same. Further, they should also know that an organization may face losses; incase, it does not get it audited. Afterwards, students should assess the impact of computers on audit and audit procedures adapted. Then, they should understand the detail steps to perform an Information System Audit. The idea of pre-audit survey and planning of an audit, for effective execution of an audit should also be understood by them in-depth.

Afterwards, students should also gain the knowledge of various auditing standards that an auditor can use for performing a systems audit. In addition, they should understand the auditing and evaluation techniques of general, physical and environmental controls including specialized security arrangements like firewalls. Concept of continuous auditing along with its advantages and disadvantages must be understood by the students. Finally, students should go through application controls covering input, processing and output controls along with their audit in detail. In addition, they must have the knowledge of operational, tactical and strategic layers of Application Security Controls and related audit issues.

7. In the current IT driven environment, there was a tremendous need for introducing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. Realizing this need, Govt. of India introduced Information Technology Act in the year 2000. However, due to various transformations in technology, it was felt necessary to carry out certain amendments to make the Act more relevant and accordingly, Govt. of India passed these amendments through a bill in 2008. Students should understand various definitions covered under this act, and clearly understand the important provisions of this Act.

Afterwards, students should also know the requirements regarding system audit/disclosure by other governing bodies like RBI, SEBI and IRDA etc. Recognizing the importance of Information Security, Government of India has also introduced National Cyber Security Policy 2013 in July, 2013, which should also be understood by the students. In addition, they should also go through other related standards like ISO 27001 and ITIL in detail with emphasis on the key points of each standard in depth. Here, it is noteworthy to mention that Students must keep themselves updated with the latest developments in the standards.

8. Emerging technologies are seen to be having enormous potential to meet the global challenges of enterprises and accordingly, the eighth and last chapter is dedicated to the emerging technologies. In this chapter, students should start from the cloud computing, which simply means the use of computing resources as a service over a network typically the internet. They should study the pertinent issues and goals of cloud computing. Further, they should understand the cloud computing architecture and environment covering public, private and hybrid clouds. In addition, students must have an overview of different cloud computing models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Network as a Service (NaaS) and Communication as a Service (CaaS). Afterwards, they should also learn numerous advantages that can be achieved by implementing cloud architecture in an enterprise. Like any other technology, in spite of its various advantages, cloud computing also has certain major challenges, which requires proper attention from research community. These challenges must be clearly understood by the students.

Afterwards, students should have an overview of Mobile Computing and BYOD (Bring Your Own Device). While going through BYOD, they must know the emerging threats arising due to the same. Then, they should read the Web 2.0 and Social Media along with other related concepts. Finally, students should study the topic of Green IT and its associated sub topics like Green IT Security Services and Challenges. The main objective of this chapter is to make the students familiar with the latest technological developments in the related areas.

#### **Examination related tips**

1. In the paper of ISCA, first question may be based on a case study. These case studies may be from the practical oriented topics such as GRC, SDLC, Protection of Information Systems, BCP/DRP, and IS Audit Guidelines/Standards etc. The case study may also be based on the concepts taken from 3-4 chapters of the study material. Hence, students should read the case study carefully and identify the relevant concept/s based on which, the questions are to be answered.
2. It is observed that sometimes students write the answers in brief while attempting long answer type questions and accordingly, they do not get good marks. Hence, before writing the answer, students should clearly understand the weightage assigned to that particular question.
3. Wherever possible, students should try to include relevant diagrams, tables, rough sketch etc.
4. At the Final level, sometimes, questions are also framed on generalized topics of IT, which may not be adequately discussed in the study material. To answer such questions, students should not feel any psychological pressure; rather they should write the answer based on their general understanding of the topic/s with reference to IT.

## CONTENTS

### CHAPTER 1 – CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

1.1	Introduction.....	1.2
1.2	Key Concepts of Governance.....	1.3
1.3	Information Technology and Governance.....	1.5
1.4	Corporate Governance and IT Governance.....	1.6
1.5	IT Governance and Governance of Enterprise IT (GEIT).....	1.7
1.6	Corporate Governance, Enterprise Risk Management and Internal Controls.....	1.9
1.7	Role of IT in Enterprises.....	1.12
1.8	IT Strategy Planning.....	1.14
1.9	Risk Management.....	1.19
1.10	COBIT 5 Business Framework – Governance and Management of Enterprise IT... ..	1.26
1.11	IT Compliance Review.....	1.35
1.12	Information System Assurance.....	1.37
1.13	Summary.....	1.43

### CHAPTER 2 – INFORMATION SYSTEMS CONCEPTS

2.1	Introduction.....	2.2
2.2	Overview of Information Systems and Practical Aspects of their Applications in Enterprise Processes.....	2.3
2.3	Relative Importance of Information Systems from Strategic and Operational Perspectives.....	2.35
2.4	Information as a Key Business Asset and its Relation to Business Objectives and Processes.....	2.37
2.5	Various types of Business Applications.....	2.39
2.6	Overview of Underlying IT Technologies.....	2.41
2.7	Summary.....	2.43

### CHAPTER 3 – PROTECTION OF INFORMATION SYSTEMS

3.1	Introduction.....	3.1
3.2	Need for Protection of Information Systems.....	3.2

3.3	Information System Security .....	3.3
3.4	Information Security Policy.....	3.4
3.5	Information Systems Controls .....	3.8
3.6	Classification of Information Systems Control .....	3.12
3.7	Managerial Controls and their Categories .....	3.38
3.8	Application Controls and their Categories .....	3.41
3.9	General Controls.....	3.55
3.10	Controls over Data Integrity and Security.....	3.70
3.11	Cyber Frauds .....	3.74
3.12	Summary .....	3.77

#### **CHAPTER 4 – BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING**

4.1	Introduction.....	4.1
4.2	Need of Business Continuity Management (BCM).....	4.2
4.3	BCM Policy .....	4.4
4.4	Business Continuity Planning .....	4.5
4.5	Developing a Business Continuity Plan.....	4.6
4.6	Components of BCM Process.....	4.10
4.7	Business Continuity Management Process.....	4.11
4.8	BCM Information Collection Process.....	4.13
4.9	BCM Strategy Process.....	4.16
4.10	BCM Development and Implementation Process .....	4.16
4.11	BCM Testing and Maintenance Process.....	4.17
4.12	BCM Training Process .....	4.19
4.13	Types of Plans .....	4.20
4.14	Types of Back-ups.....	4.22
4.15	Alternate Processing Facility Arrangements .....	4.23
4.16	Disaster Recovery Procedural Plan .....	4.24
4.17	Audit of the BCP/DRP .....	4.25
4.18	Summary .....	4.28

## **CHAPTER 5 – ACQUISITION, DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SYSTEMS**

5.1	Introduction.....	5.2
5.2	Business Process Design.....	5.2
5.3	System Development.....	5.4
5.4	Systems Development Methodology.....	5.8
5.5	System Development Life Cycle (SDLC).....	5.19
5.6	Operation Manuals.....	5.59
5.7	Auditors' Role in SDLC.....	5.61
5.8	Summary.....	5.64

## **CHAPTER 6 – AUDITING OF INFORMATION SYSTEMS**

6.1	Introduction.....	6.1
6.2	Controls and Audit.....	6.2
6.3	The IS Audit.....	6.6
6.4	Performing IS Audit.....	6.11
6.5	IS Audit and Audit Evidence.....	6.16
6.6	Audit and Evaluation Techniques for Physical and Environmental Controls.....	6.23
6.7	Application Controls and their Audit Trails.....	6.27
6.8	Audit of Application Security Controls.....	6.30
6.9	Summary.....	6.33

## **CHAPTER 7 – INFORMATION TECHNOLOGY REGULATORY ISSUES**

7.1	The IT Act and its Objectives.....	7.1
7.2	Key Definitions.....	7.3
7.3	[Chapter-II] Digital Signature and Electronic Signature.....	7.7
7.4	[Chapter III] Electronic Governance.....	7.8
7.5	[Chapter V] Secure Electronic Records and Secure Electronic Signatures.....	7.12
7.6	[Chapter IX] Penalties, Compensation and Adjudication.....	7.12
7.7	[Chapter XI] Offences.....	7.15
7.8	[Chapter XII] Intermediaries not to be liable in Certain Cases.....	7.24
7.9	[Chapter XIIA] Examiner of Electronic Evidence.....	7.25

7.10	[Chapter XIII] Miscellaneous .....	7.26
7.11	Requirements of Various Authorities for System Controls & Audit .....	7.28
7.12	Cyber Forensic and Cyber Fraud Investigation.....	7.35
7.13	Security Standards .....	7.35
7.14	Summary .....	7.48

#### **CHAPTER 8 – Emerging Technologies**

8.1	Introduction .....	8.1
8.2	Cloud Computing.....	8.2
8.3	Mobile Computing.....	8.15
8.4	Bring Your Own Device (BYOD) .....	8.16
8.5	Social Media and Web 2.0 .....	8.18
8.6	Green IT .....	8.24
8.7	Summary .....	8.26

References.....	i
-----------------	---

Glossary.....	ii – x
---------------	--------



# Concepts of Governance and Management of Information Systems

## Learning Objectives

- To understand the concept of Governance, Risk and compliance (GRC) and relationship between governance and management;
- To understand the Role of Information Technology (IT), how to align Information Systems (IS) Strategy with business strategy and ensure Business Value from use of IT;
- To understand the business impact of IS risks, different types of Information Systems Risks and how IS Risk management is implemented;
- To understand the key aspects of IT Compliance and the specific role and responsibilities of top management relating to IT-GRC;
- To understand the key concepts of Governance of Enterprise IT (GEIT) and using COBIT as framework of GEIT; and
- To understand role of Information Systems Assurance in GEIT.

## Task Statements

- To distinguish among key aspects of enterprise governance, corporate governance, GEIT, GRC and IT Management;
- To examine the role of IT in formulating IT strategy, aligning IT as per business strategy and identify key processes and practices required for ensuring value creation from IT;
- To review IS Risk management strategy based on different types of risks and their impact;
- To identify regulatory aspects of IT Compliance and the specific role and responsibilities in IT-GRC implementation;
- To use best practices frameworks such as COBIT as framework of GEIT to meet enterprises need for implementing GEIT; and
- To provide Information Systems Assurance in GEIT.

## Knowledge Statements

- To know Governance, Risk and compliance and relationship between governance and management;
- To know the role of IT, aligning IS Strategy in business strategy and ensuring business value from IT.
- To know IS Risk Management Strategy, business impact of IS risks and different types of IS Risks;
- To know IT Compliance overview – Responsibilities of top management for IT-GRC;
- To know the concepts of GEIT and using GEIT frameworks such as COBIT; and
- To know the role of Information Systems Assurance in GEIT.

### 1.1 Introduction

The primary objective for the inclusion of the 'Information Systems Control and Audit' paper at the Final Level of the Chartered Accountancy course is to provide conceptual understanding of different aspects of IT risks, security, controls and auditing of IT processes. This paper leverages and builds on the advanced IT Training and enables to understand the enterprise level aspects of governance, risk, compliance, assurance as applicable to enterprises. The topics covered here are closely integrated with Auditing and Assurance Paper. While updating this paper, the primary rationale has been to ensure the coverage of the latest concepts of **Governance, Risk and Compliance (GRC)**, which has been a regulatory requirement not only for listed enterprises but also for all types of enterprises. Further, implementing GRC in an IT environment requires updated knowledge and skills based on the latest developments and the best practices and this is sought to be provided by this paper. Students are advised to read these topics not only from examination point of view but keeping in mind the fact that these topics are highly relevant to their work as articles and in their careers whether they seek to be employed in enterprises or self-employed.

The topics have been organized so as to link all of them topics together from the macro perspective of Governance, risk, compliance and assurance to the micro perspective and implementation level so that a blend of both concepts as well as the practical aspects could be provided. This knowledge will equip CA students with holistic approach to IT assurance rather than function oriented IS controls and audit perspective. This will provide the required competency to meet the challenges of IT environment, which they face in their work area.

Before moving forward, it is important to understand the overall learning objective of the Paper, which is: *"To develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant"*. The detailed learning objectives are given below:

- To understand the key concepts of Governance, Risk and Compliance aspects in enterprises as relevant to IT;
- To identify and review IT risks, security, controls and risk management approach;
- To assess the impact on controls and organizational structure on account of integration of technological applications and resources into operational processes;
- To assess Business Continuity Plans of enterprises for adequacy from perspective of going concern;
- To assess information systems acquisition, development and implementation strategy including review of Systems Development Life Cycle process;
- To understand how to perform auditing including collecting and evaluating evidence in an IT environment; and
- To understand and apply IT best practices and impact of emerging technologies.

It is noteworthy to mention here that understanding of this chapter on "Governance, Risk and Compliance aspects in enterprises as relevant to IT" is very important as it provides the macro

concepts and provides a solid platform for understanding of the topics, which are covered in the later chapters.

## 1.2 Key Concepts of Governance

It is needless to emphasize that enterprises whether they are commercial or non-commercial, exist to deliver value to their stakeholders. Delivering value is achieved by operating within value and risk parameters that are acceptable and advantageous, and by using resources including IT responsibly. In the rapidly changing environment that most enterprises operate in, swift direction setting and agility to change are essential. Senior management is responsible for ensuring that the right structure of decision-making accountabilities are shared among many people in the enterprise and when accountability is shared, governance comes into play.

- Governance:** The term “**Governance**” is derived from the Greek verb meaning “to steer”. Governance refers to “all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language.” It relates to “the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions. A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives. Governance is a very general concept that can refer to all manner of organizations and can be used in different ways. We shall here understand what is meant by the term- **Enterprise Governance**.
- Enterprise Governance:** **Enterprise Governance** can be defined as: ‘The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization’s resources are used responsibly.’ Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit. Examples include codes on corporate governance and financial reporting standards.

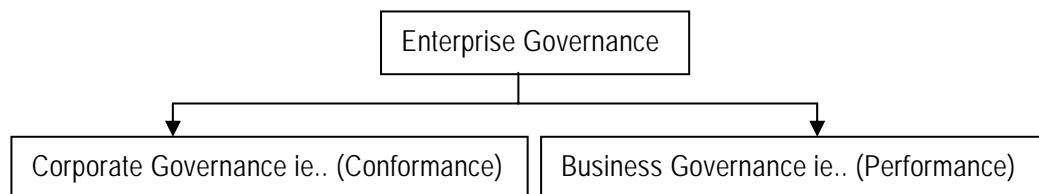


Fig. 1.2.1: Enterprise Governance Framework\*

\* [http://www.cimaglobal.com/Documents/ImportedDocuments/cid\\_enterprise\\_governance\\_\\_feb08.pdf](http://www.cimaglobal.com/Documents/ImportedDocuments/cid_enterprise_governance__feb08.pdf)

## 1.4 Information Systems Control and Audit

---

The enterprise governance constitutes the entire accountability framework of an organization as it involves establishing accountability for decision-making. Enterprise Governance has two dimensions as shown in the Fig. 1.2.1:

- Corporate Governance or Conformance, and
- Business Governance or Performance.

These dimensions are discussed as follows:

- **Corporate Governance or Conformance:** Corporate Governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.

Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business to protect shareholders' interest. Corporate Governance drives the corporate information needs to meet business objectives.

Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of Audit Committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. These are intended to guide companies to achieve their business objectives in a manner such that those who are entrusted with the resources or power to run the companies to meet stakeholder needs without compromising the shareholders' interest. Legally, the directors of a Company are accountable to the shareholders for their actions in directing and controlling the business, and for the actions of the company's employees, who are in the position of trust to discharge their responsibilities in the best interest of the company. Corporate governance is thus necessary for the purpose of monitoring and measuring their performance.

Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee or its equivalent in countries where the two tier board system is the norm. Other committees are usually the nominations committee and the remuneration committee. The **Sarbanes Oxley Act of US** and the Clause 49 listing requirements

of SEBI are examples of providing for such compliances from conformance perspective.

Good corporate governance is important and it is critical so that any weakness in this area is addressed properly. However, good corporate governance by itself cannot make an organization successful. There is always a risk that inadequate attention is paid to the need for enterprises to create wealth or stakeholder value. Hence, it is important to remember that strategy and performance are also very important. The key message of enterprise governance is that an enterprise must balance the two dimensions of conformance and performance so as to meet stakeholder requirements and ensure long-term success.

- **Business Governance or Performance:** The **Business Governance** is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required.

The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. There is thus an oversight gap in respect of strategy. One of the ways of dealing with this lacuna is to establish a strategy committee of similar status to the other board committees which will report to the board.

### 1.3 Information Technology and Governance

The usage of IT is rapidly increasing in most of the large enterprises and also to a great extent even in small and medium enterprises and is at the core of most of the key business operations. Further, there is an increasing thrust on corporate governance by regulators encompassing governance, risk management and controls. The use of IT covering all key aspects of business processes of an enterprise impacts not only 'how information is processed' but also 'how computerized information systems are used for strategic and competitive advantage'. Internal controls are integral part of information systems of an enterprise. Hence, it is important to understand 'how information systems are organized' and 'how controls are integrated'. Thus, as IT is used extensively in enterprises and encompasses all aspects of business, the relevant internal controls get embedded in the IT systems.

### 1.3.1 Benefits of Governance

Before we proceed further, let us understand the major benefits of governance. These can be summarized as follows:

- Achieving enterprise objectives by ensuring that each element of the mission and strategy are assigned and managed with a clearly understood and transparent decisions rights and accountability framework;
- Defining and encouraging desirable behavior in the use of IT and in the execution of IT outsourcing arrangements;
- Implementing and integrating the desired business processes into the enterprise;
- Providing stability and overcoming the limitations of organizational structure;
- Improving customer, business and internal relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework; and
- Enabling effective and strategically aligned decision making for the IT Principles that define the role of IT, IT Architecture, IT Infrastructure, Application Portfolio and Frameworks, Service Portfolio, Information and Competency Portfolios and IT Investment & Prioritization.

Based on the above, it can be seen that IT is an integral part of the governance. The successful design and deployment of information systems using IT, determines the success of an enterprise. Hence, it is critical to ensure that the required controls are implemented not only from IT perspective but also from management and regulatory perspective. This requires that the controls are implemented from Governance perspective using a holistic approach and has involvement of the senior management as required. Implementing IT Governance as subset of enterprise governance ensures that implementation of IT meets all the stakeholder requirements including regulators and management. Regulatory requirements mandate not only implementation of governance but also its independent evaluation. Hence, auditors are required to evaluate these aspects in their roles as internal or external auditors. As IT proliferates, there is increasing demands for pro-active objective assessments of governance, risk, compliance and controls of information systems.

## 1.4 Corporate Governance and IT Governance

There is no doubt to say that IT is a key enabler of corporate business strategy. **Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chief Information Officers (CIO)** agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives. IT has to provide critical inputs to meet the information needs of all the required stakeholders or it can be said that enterprise activities require information from IT activities in order to meet enterprise objectives. Hence, corporate governance drives and sets IT governance.

There are multiple definitions of IT Governance. However, one of the well-known definitions is: "IT Governance is the system by which IT activities in a company or enterprise are directed

and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs". Hence, the overall objective of IT governance is very much similar to corporate governance but with the focus on IT. Hence, it can be said that there is an inseparable relationship between Corporate Governance and IT Governance or IT Governance is a sub-set of Corporate or Enterprise Governance.

## 1.5 IT Governance and Governance of Enterprise IT (GEIT)

Let us now specifically understand the key concepts of IT Governance and the distinction between IT Governance and GEIT. Although the terms IT Governance and Governance of Enterprise IT (GEIT) are used inter-changeably, the term GEIT is more macro and broader in its scope of coverage. In this chapter, we shall be using both the terms as relevant and as specifically required as some of the regulatory requirements still refer to the term IT Governance.

### 1.5.1 IT Governance

The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT. IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT. The active distribution of decision-making rights and accountabilities among different stakeholders in an organization and the rules and procedures for making and monitoring those decisions to determine and achieve desired behaviors and results. It may be noticed that governance and IT governance are similar in their definition and approach except that in case of IT governance the focus is on IT and related areas.

### 1.5.2 Key practices to determine status of IT Governance

Some of the key practices, which determine the status of IT Governance in the enterprise, are:

- Who makes directing, controlling and executing decisions?
- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

As per regulatory requirements and best practices frameworks of Governance of enterprise IT, it is important for the Board of Directors and senior management to play critical roles in evaluating; directing and monitoring IT Effectiveness of the IT governance structure and processes are directly dependent upon the level of involvement of the board and senior management. Different levels of the framework require different tools, techniques, and standards addressing specific needs of an effective IT governance structure, which consists of the organizational structure, leadership, and processes that ensure IT support of the organization's strategies and objectives.

### 1.5.3 Benefits of IT Governance

The benefits, which are achieved by implementing/improving governance or management of enterprise, IT would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;
- Improved agility in supporting business needs;
- Better cost performance of IT;
- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;
- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

For every defined benefit, it is critical to ensure that:

- Ownership is defined and agreed;
- It is relevant and links to the business strategy;
- The timing of its realization of benefit is realistic and documented;
- The risks, assumptions and dependencies associated with the realization of the benefits are understood, correct and current;
- An unambiguous measure has been identified; and
- Timely and accurate data for the measure is available or is easy to obtain.

### 1.5.4 Governance of Enterprise IT (GEIT)

**Governance of Enterprise IT** is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

### 1.5.5 Benefits of GEIT

These are given as follows:

- It provides a consistent approach integrated and aligned with the enterprise governance approach.
- It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.



- It ensures that IT-related processes are overseen effectively and transparently.
- It confirms compliance with legal and regulatory requirements.
- It ensures that the governance requirements for board members are met.

#### 1.5.6 Key Governance Practices of GEIT

The key governance practices required to implement GEIT in enterprises are highlighted here:

- **Evaluate the Governance System:** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- **Direct the Governance System:** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and
- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

### 1.6 Corporate Governance, Enterprise Risk Management and Internal Controls

Various prominent frauds committed by some large enterprises across the world including India in the last two decades have awakened regulators to the need of mandating the implementation of corporate governance integrated with Enterprise Risk Management and Internal controls. The concept of Corporate Governance has succeeded in attracting a good deal of public interest because of its importance for the economic health of corporations, protect the interest of stakeholders including investors and the welfare of society, in general. As discussed earlier, Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. Some of the best practices of corporate governance include the following:

- Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors;
- Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;
- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;

## 1.10 Information Systems Control and Audit

---

- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. traders);
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

### 1.6.1 Enterprise Risk Management (ERM)

In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise. Hence, the type of controls implemented in information systems in an enterprise would depend on this risk management strategy. The **Sarbanes Oxley Act (SOX)** in the US, which focuses on the implementation and review of internal controls as relating to financial audit, highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented. How controls are implemented would be dependent on the overall risk management strategy and risk appetite of the management. SOX have used **Committee of Sponsoring Organizations (COSO)** as one of the important guidelines for implementing risk management and internal controls.

The Executive Summary of Enterprise Risk Management — Integrated Framework published by COSO of the Treadway Commission highlights the need for management to implement a system of risk management at the enterprise level. Enterprise Risk Management deals with risks and opportunities affecting value creation or preservation, defined as follows: "Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise

### 1.6.2 Internal Controls

The (The US Security and Exchange Commission) SEC's final rules define "internal control over financial reporting" as a "process designed by, or under the supervision of, the

company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company;
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements."

Under the final rules, a company's annual report must include "an internal control report of management that contains:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting;
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting; and
- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting."

**(a) Responsibility for Implementing Internal Controls:** SOX made a major change in internal controls by holding Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) personally and criminally liable for the quality and effectiveness of their organization's internal controls. Part of the process is to attest to the public that an organization's internal controls are effective. Internal controls can be expected to provide only a reasonable assurance, not an absolute assurance, to an entity's management and board. An organization must ensure that its financial statements comply with **Financial Accounting Standards (FAS)** and **International Accounting Standards (IAS)** or local rules via policy enforcement and risk avoidance methodology called "Internal Control." There must be a system of checks and

## 1.12 Information Systems Control and Audit

---

balances of defined processes that lead directly from actions and transactions reporting to an organization's owners, investors, and public hosts.

**(b) Internal Controls as per COSO:** According to COSO, Internal Control is comprised of five interrelated components:

- **Control Environment:** For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.
- **Risk Assessment:** Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **Control Activities:** Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.
- **Information and Communication:** Associated with control activities are information and communication systems. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.
- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

**(c)** Clause 49 of the listing agreements issued by SEBI in India is on similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation. Further, it also provides for certification of these aspects by the external auditors.

It may be noted that COSO and COBIT together have been internationally used as best practices framework for complying with SOX. The details of how IT compliance can be best implemented or reviewed by using best frameworks such as COBIT 5 is covered in the further sections.

## 1.7 Role of IT in Enterprises

In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to decision support systems to online transactions/services. IT has not only automated the business processes but also transformed the way business processes are performed. The way in which business processes are performed/services rendered and how an organization is structured could be transformed through right deployment of IT. It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

The extent of technology deployment also impacts the way internal controls are implemented in an enterprise. Further, extensive organization restructuring or business process re-

engineering may be facilitated through IT deployments. Implementing IT has to consider not only implementation of IT controls from conformance perspective but also IT could be a key enabler for providing strategic and competitive advantage. This requires that senior management considers IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services. This makes it imperative to develop an IT strategy, which is aligned with business strategy and ensures value creation and facilitates benefit realization from the IT investments.

### 1.7.1 Business and IT Strategy

Management Strategy determines at the macro level the path and methodology of rendering services by the enterprise. Strategy outlines the approach of the enterprise and is formulated by the senior management. Based on the strategy adapted, relevant policies and procedures are formulated. From business strategy perspective, IT is affecting the way in which enterprises are structured, managed and operated. One of the most dramatic developments affecting enterprises is the fusion of IT with business strategy. Enterprises can no longer develop business strategy separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business planning and the incorporation of effective financial and management controls within new systems. Management primarily is focused on harnessing the enterprise resources towards achievement of business objectives. This would involve the managerial processes of planning, organizing, staffing, directing, coordinating, reporting and budgeting.

Every enterprise regardless of its size needs to have an internal control system built into its enterprise structure. 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". We are aware that auditors could be involved in providing assurance requiring review of Information Systems as implemented from control perspective. However, auditors may also be required to provide consulting before, during or after implementation of information systems strategy. It becomes imperative for the auditor to understand the concepts of the enterprise strategy as relevant. Hence, auditors must have good understanding of management aspects as relevant to deployment of IT and IT strategy. This would include understanding of the IS Strategy, policies, procedures, practices and enterprise structure, segregation of duties, etc.

IT organizations should define their strategies and tactics to support the organization by ensuring that day-to-day IT operations are delivered efficiently and without compromise. Metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of enterprise leaders. Internal audit can determine whether the linkage of IT metrics and objectives aligns with the organization's goals, adequately measure progress being made on approved initiatives, and express an opinion on whether the metrics are relevant and useful. Additionally, auditors can validate that metrics are being measured correctly and represent realistic views of IT operations and governance on a tactical and strategic basis.

### 1.7.2 IT Steering Committee

Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives. As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee. Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management. As the members comprise of function heads of departments, they would be responsible for taking decisions relating to their departments as required. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. The key functions of the committee would include of the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

## 1.8 IT Strategy Planning

Planning is basically deciding in advance 'what is to be done', 'who is going to do' and 'when it is going to be done'. There are three levels of managerial activity in an enterprise:

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top

management determines overall organizational purposes and objectives and how they are to be achieved. Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among those businesses.

- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation. Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise. Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

### 1.8.1 IT Strategic Planning Process

The strategic planning process has to be dynamic in nature and IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the enterprise's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long and short-range plan are developed and maintained. IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

### 1.8.2 Objective of IT Strategy

The primary objective of IT strategy is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives. Alignment of the strategic IT plans with the business objectives is done by clearly communicating the objectives and associated accountabilities so they are understood by all and all the IT strategic options are identified, structured and integrated with the business plans as required.

### 1.8.3 Classification of Strategic Planning

In the context of Information Systems, **Strategic Planning** refers to the planning undertaken by top management towards meeting long-term objectives of the enterprise.

IT Strategy planning in an enterprise could be broadly classified into the following categories:

## 1.16 Information Systems Control and Audit

---

- Enterprise Strategic Plan,
- Information Systems Strategic Plan,
- Information Systems Requirements Plan, and
- Information Systems Applications and Facilities Plan.

These aforementioned plans are discussed as follows:

- (i) **Enterprise Strategic Plan:** Business Planning determines the overall plan of the enterprise. The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate. It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise. It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives, a specification of constraints that apply, and a listing of priorities. In an IT environment, it is important to ensure that the IT plan is aligned with the enterprise plan.
- (ii) **Information Systems Strategic Plan:** The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment. This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals. Some of the enablers of the IS Strategic plan are:
  - Enterprise business strategy,
  - Definition of how IT supports the business objectives,
  - Inventory of technological solutions and current infrastructure,
  - Monitoring the technology markets,
  - Timely feasibility studies and reality checks,
  - Existing systems assessments,
  - Enterprise position on risk, time-to-market, quality, and
  - Need for senior management buy-in, support and critical review.
- (iii) **Information Systems Requirements Plan:** Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems. This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information. Based on the information architecture requirements of an enterprise, the Information Systems Requirements Plan has to be drawn up so as to meet the information requirements of the enterprise. Some of the key enablers of the information architecture are as follows:
  - Automated data repository and dictionary,



- Data syntax rules,
- Data ownership and criticality/security classification,
- An information model representing the business, and
- Enterprise information architectural standards.

The information system requirements plan defines information system architecture for the information systems department. The architecture specifies the major organization functions needed to support planning, control and operations activities and the data classes associated with each function. The business planning will determine the information needs of an enterprise. The information architecture will determine information needs and flow in an enterprise. Based on the information architecture, the organization structure is determined. This in turn will lead to specific information systems, which include the relevant IT and related processes. For example, depending on the business, information architecture and organization structure, the enterprise will decide whether to acquire or develop the solution and the relevant controls which are required to meet the business requirements.

**(iv) Information Systems Applications and Facilities Plan:** On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan. This plan includes:

- Specific application systems to be developed and an associated time schedule,
- Hardware and Software acquisition/development schedule,
- Facilities required, and
- Organization changes required.

Senior management is responsible for developing and implementing long and short-range plans that enable achievement of the enterprise mission and goals. Senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the enterprise's long- and short-range plans. IT long and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the enterprise. Strategic plan period could vary from 1 year to 3 years. It is important to ensure that the IT strategic plans are aligned with the business strategic plans as IT is ultimately used for achieving business objectives. Strategic planning could be done by the top management or by the steering committee. Strategic planning facilitates in putting organization objectives into time-bound plans and action. Comprehensive planning helps to ensure an effective and efficient enterprise. Strategic planning is time and project oriented, but must also address and help determine priorities to meet business needs.

#### **1.8.4 Key Management Practices for Aligning IT Strategy with Enterprise Strategy**

The key management practices, which are required for aligning IT strategy with enterprise strategy, are highlighted here:

## 1.18 Information Systems Control and Audit

---

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals, extent of stakeholder satisfaction with scope of the planned portfolio of programs and services and the percentage of IT value drivers, which are mapped to business value drivers.

### 1.8.5 Business Value from Use of IT

Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost. The benefit of implementing this process will ensure that enterprise is able to secure optimal value from IT-enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

The key management practices, which need to be implemented for evaluating 'Whether business value is derived from IT', are highlighted as under:

- **Evaluate Value Optimization:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.
- **Direct Value Optimization:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.
- **Monitor Value Optimization:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented. Some of the key metrics, which can be used for such evaluation, are:

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where expected benefits realized;
- Percentage of IT enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

## 1.9 Risk Management

Enterprise Risk Management and IT Risk Management are key components of an effective IT governance structure of any enterprise. Effective IT governance helps to ensure close linkage to the enterprise risk management activities, including Enterprise Risk Management (ERM) and IT Risk Management. IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite. The risk assessment approach adapted has to consider business impact of IS risk and different types of risks. There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile. This section will provide an overview of related terms like

## 1.20 Information Systems Control and Audit

---

threats, vulnerabilities etc., IS Risks and exposures and risk mitigation strategies, which can be adapted by the organizations.

### 1.9.1 Information Systems Risks and Risk Management

There are numerous changes in IT and its operating environment that emphasizes the need to better manage IT related risks. Dependency on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. Increasing disclosures of information system disasters and increasing electronic fraud, in turn, drive this. The management of IT related risks is now being understood as a key part of enterprise governance.

Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. This security has to be implemented as per required control system envisaged by the management of the enterprise. Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them. Based on the point of impact of risks, controls are classified as Preventive, Detective and Corrective. Preventive controls prevent risks from actualizing. Detective controls detect the risks as they arise. Corrective controls facilitate correction.

The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

### 1.9.2 Sources of Risk

The most important step in risk management process is to identify the sources of risk, the areas from where risks can occur. This will give information about the possible threats, vulnerabilities and accordingly appropriate risk mitigation strategy can be adapted. Some of the common sources of risk are as follows:

- Commercial and Legal Relationships,
- Economic Circumstances,
- Human Behavior,
- Natural Events,
- Political Circumstances,
- Technology and Technical Issues,
- Management Activities and Controls, and

- Individual Activities.

Broadly, risk has the following characteristics:

- Loss potential that exists as the result of threat/vulnerability process;
- Uncertainty of loss expressed in terms of probability of such loss; and
- The probability/likelihood that a threat agent mounting a specific attack against a particular system.

### 1.9.3 Related Terms

Various terminologies relating to risk management are given as follows:

**Asset:** Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity, without which, the organization may be threatened.
- Their Data Classification would normally be Proprietary, Highly confidential or even Top Secret.

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

**Vulnerability:** Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, 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. Some examples of vulnerabilities are given as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the 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.

Simply, Vulnerability can be referred as the weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from flaws on the software's design, defects in its implementation, or problems in its operation. Some experts also define 'vulnerability' as opening doors for attackers. Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

## 1.22 Information Systems Control and Audit

---

- 'Allows an attacker to execute commands as another user' or
- 'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
- 'Allows an attacker to pose as another entity' or
- 'Allows an attacker to conduct a denial of service'.

**Threat:** Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. 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 organization.

Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

**Exposure:** An exposure is the extent of loss the enterprise has to face when a risk materializes. 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 etc.

**Likelihood:** 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:** An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.

Basically, it is a set of actions designed to compromise **CIA (Confidentiality, Integrity or Availability)**, or any other desired feature of an information system. Simply, it is the act of trying to defeat Information Systems (IS) safeguards. The type of attack and its degree of success determines the consequence of the attack.

**Risk:** Formally, risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization. Risk assessment includes the following:

- Identification of threats and vulnerabilities in the system;
- Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
- The identification and analysis of security controls for the information system.

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:

- 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 against organizations; and
- External factors such as legislative, legal and regulatory requirements or technological developments.

It means there are new risk areas that could have a significant impact on critical business operations, such as:

- External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information;
- Growing potential for misuse and abuse of information system affecting privacy and ethical values; and
- Increasing requirements for availability and robustness.

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 organization by contributing to interactions with the trading partners, closer customer relations, improved competitive advantage and protected reputation.

**Counter Measure:** An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure. For example, well known threat 'spoofing the user identity', has two countermeasures:

- Strong authentication protocols to validate users; and
- Passwords should not be stored in configuration files instead some secure mechanism should be used.

Similarly, for other vulnerabilities, different countermeasures may be used.

The relationship and different activities among these aforementioned terms may be understood by the Fig. 1.9.1.

Any risk still remaining after the counter measures are analyzed and implemented is called **Residual Risk**. An organization'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 minimized, 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.

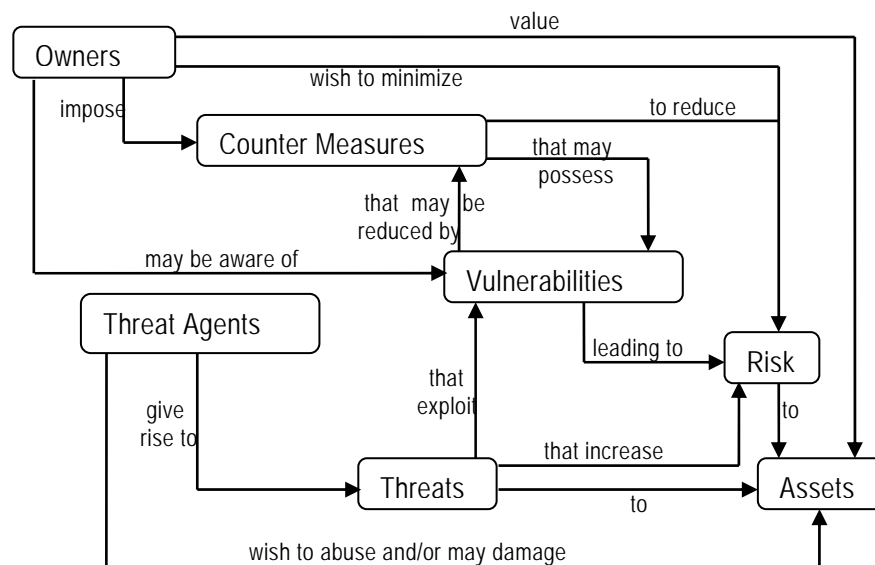


Fig. 1.9.1: Risk and Related Terms\*

### 1.9.4 Risk Management Strategies

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained and illustrated below:

- **Tolerate/Accept the risk.** One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

\* Source: <http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF> p.14



- **Treat/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

### 1.9.5 Key Governance Practices of Risk Management

The key governance practices for evaluating risk management are given as follows:

- **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;
- **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and
- **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

### 1.9.6 Key Management Practices of Risk Management

Key Management Practices for implementing Risk Management are given as follows:

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
- **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

### 1.9.7 Metrics of Risk Management

Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are as follows:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;

- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

### 1.10 COBIT 5 Business Framework – Governance and Management of Enterprise IT

We have already discussed that Enterprise Governance is not only a management requirement but is also mandated by law. IT is a key enabler of enterprises and forms the edifice on which the information and information systems are built. Implementing internal controls is not only a management requirement but is now a regulatory requirement too. In an IT environment, embedding the right level of controls within the information systems, which provides information to users securely and safely and as per business requirements, is critical not only for ensuring business success but is also a key requirement for the survival of the enterprise. In implementing internal controls in an IT environment, the legacy approach of considering IT and its contents as boxes to be secured by the IT department is fraught with extreme risk. Both from regulatory as well as enterprise perspective, senior management need to be involved in providing direction on how governance, risk and control are implemented using a holistic perspective based on the need for harnessing the power of information and information technology from a business perspective.

**Control Objectives for Information and Related Technology (COBIT)** is a set of best practices for Information Technology management developed by **Information Systems Audit & Control Association (ISACA)** and IT Governance Institute in 1996. ISACA develops and maintains the internationally recognized COBIT framework, helping IT professionals and enterprise leaders fulfill their IT Governance responsibilities while delivering value to the business. The latest ISACA's globally accepted framework COBIT 5 is aimed to provide an end-to-end business view of the governance of enterprise IT that reflects the central role of IT in creating value for enterprises.

**COBIT 5** is the only business framework for the governance and management of enterprise Information Technology. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. As per COBIT 5, Information is the currency of the 21<sup>st</sup> century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. This section explains the need for using the approach and latest thinking provided by globally recognized framework COBIT 5 as a benchmark for reviewing and implementing governance and management of enterprise IT. It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help enterprises to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities.

#### 1.10.1 Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues. COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and

geographies. It helps enterprises to create optimal value from their information and technology. COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes, including non-profit and public sector and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT;
- User satisfaction with IT engagement and services;
- Reduced IT related risks and compliance with laws, regulations and contractual requirements;
- Development of more business-focused IT solutions and services; and
- Increased enterprise wide involvement in IT-related activities.

### 1.10.2 Integrating COBIT 5 with Other Frameworks

COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO). COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as **Information Technology Infrastructure Library (ITIL)**, **The Open Group Architecture Framework (TOGAF)** and ISO 27001. It is also aligned with The GEIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behavior that the governing body (e.g., board) should evaluate, direct and monitor. Thus, COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language. The framework and resulting enablers should be aligned with and in harmony with (amongst others) the:

- Enterprise policies, strategies, governance and business plans, and audit approaches;
- Enterprise risk management framework; and
- Existing enterprise governance organization, structures and processes.

### 1.10.3 Components in COBIT

- **Framework** - *Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements*
- **Process Descriptions** - *A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.*
- **Control Objectives** - *Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.*
- **Management Guidelines** - *Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes*

- *Maturity Models - Assess maturity and capability per process and helps to address gaps.*

#### 1.10.4 Benefits of COBIT 5

*COBIT 5 frameworks can be implemented in all sizes of enterprises.*

- *A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.*
- *The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.*
- *Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.*
- *COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.*
- *COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.*
- *The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.*
- *COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.*

#### 1.10.5 Customizing COBIT 5 as per Requirement

COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, it can be applied to meet needs related to:

- Information security,
- Risk management,
- Governance and management of enterprise IT,
- Assurance activities,
- Legislative and regulatory compliance, and
- Financial processing or CSR reporting.

Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5. Further, the above examples show specific areas based on which best practices can be extracted from COBIT 5.

#### 1.10.6 Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just five principles. The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and

technology investment and use for the benefit of stakeholders. These principles are shown in Fig. 1.10.1 and are discussed below:

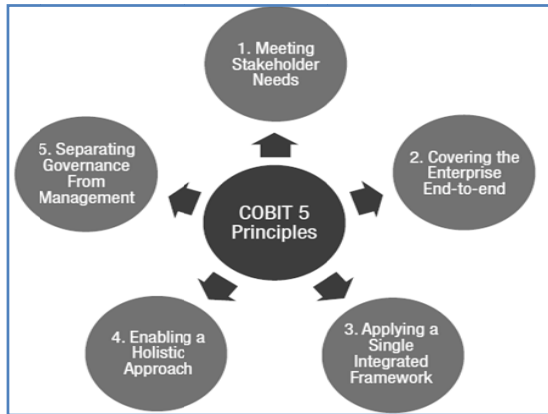


Fig. 1.10.1: Five Principles of COBIT 5\*

- Principle 1: Meeting Stakeholder Needs:** Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organization, risk appetite, etc.), and requires a customized governance and management system. Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

- Principle 2: Covering the Enterprise End-to-End:** COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone - internal and external that is relevant to governance and management of enterprise

\* Source: www.isaca.org

### 1.30 Information Systems Control and Audit

information and related IT. The end-to-end governance approach that is the foundation of COBIT 5 is depicted in Fig. 1.10.2 showing the key components of a governance system.

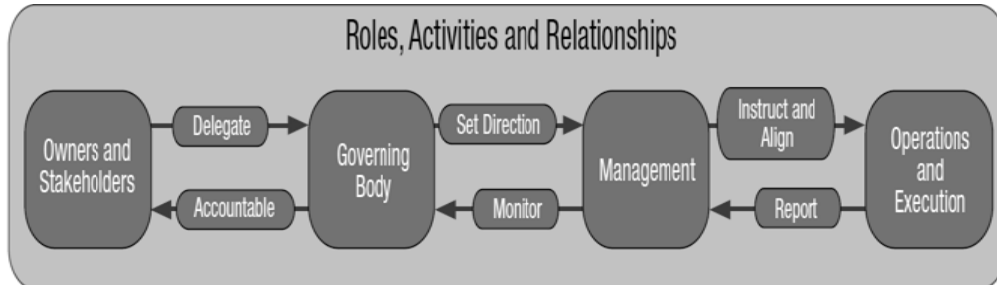


Fig. 1.10.2: Key Components of a Governance System\*

- **Principle 3: Applying a Single Integrated Framework:** There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.
- **Principle 4: Enabling a Holistic Approach:** Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.
- **Principle 5: Separating Governance from Management:** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

#### 1.10.7 COBIT 5 Process Reference Model

COBIT 5 includes a Process Reference Model, which defines and describes in detail a number of governance and management processes of enterprise IT into two main process domains- **Governance** and **Management** as shown in Fig. 1.10.3. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation. Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is one of the most important and critical steps towards good governance. It also provides a framework for measuring and monitoring IT performance,

\* Source: [www.isaca.org](http://www.isaca.org)

providing IT assurance, communicating with service providers, and integrating best management practices.

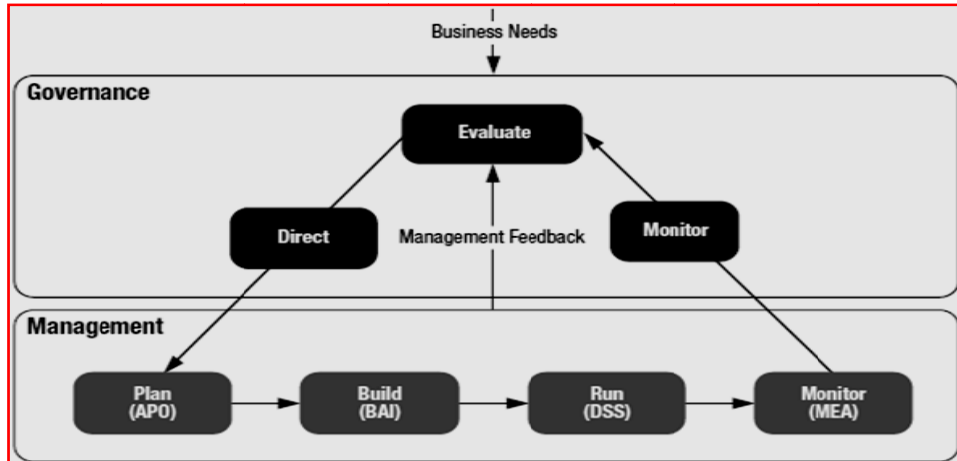


Fig. 1.10.3: Key Areas of Governance and Management\*

**Governance:** It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most of the enterprises, overall governance is the responsibility of the Board of Directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

**Management:** It contains four domains, in line with the responsibility areas of **Plan, Build, Run and Monitor (PBRM)**, providing the end-to-end coverage of IT in alignment with the direction set by the governance body to achieve the enterprise objectives. In most of the enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

*The COBIT 5 process reference model is the successor of the COBIT 4.1 process model, incorporating the both the Risk IT and Val IT frameworks. The complete COBIT 5 enabler model includes a total of 37 governance and management processes as mentioned below:*

Governance Processes

- Evaluate, Direct and Monitor Practices (EDM) – 5 processes (EDM01 to EDM05)

Management Processes

- Align, Plan and Organize (APO) - 13 processes (APO01 to APO13)
- Build, Acquire and Implement (BAI) - 10 processes (BAI01 to BAI10)

\* Source: www.isaca.org

- *Deliver, Service and Support (DSS) - 6 processes (DSS01 to DSS06)*
- *Monitor, Evaluate and Assess (MEA) - 3 processes (MEA01 to MEA03)*

#### 1.10.8 Seven Enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers, which are shown in Fig. 1.10.4 and discussed as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

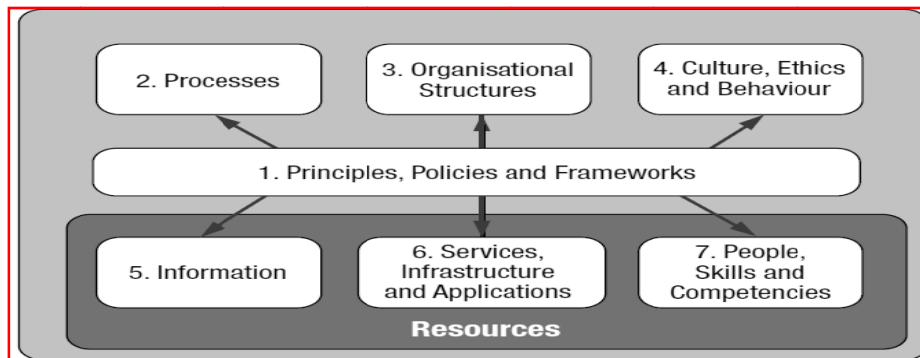


Fig. 1.10.4: Seven Enablers of COBIT 5\*

- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

---

\* Source: [www.isaca.org](http://www.isaca.org)



### 1.10.9 Risk Management in COBIT 5

The COBIT framework provides excellent guidance on risk management strategy and practices from governance and management practice.

The Governance domain contains five governance processes, one of which focuses on stakeholder risk-related objectives: “EDM03: Ensure risk optimization”. This process ensures that the enterprise’s risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed. This process provides guidance on how to ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

COBIT framework has management domain of “Align, Plan and Organize”, which contains a risk-related process: “APO12: Manage risk”. This process requires continually identifying, assessing and reducing IT-related risk within levels of tolerance set by enterprise executive management. The primary purpose of this process is to integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk. All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities.

The combination of Governance practices of “EDM03: Ensure risk optimization” (which ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated) and the management practices of “APO12 Manage risk” (which provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise) together ensured that Risk management covers the entire life cycle and covers both governance and management perspective. Further, detailed guidance is available in the form of specific practices and activities that are designed to treat related risk (avoid, reduce/mitigate/control, share/transfer/accept). In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process including risk-related roles at each level of management as appropriate. A pictorial representation of various activities relating to risk management is given in Fig. 1.10.5:



Fig. 1.10.5: Risk Management

### 1.10.10 Using COBIT 5 Best Practices for GRC

Although a GRC program (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also so as to optimize the investments made in implementing relevant processes, control structures and systems. GRC program implementation requires the following:

- Defining clearly what GRC requirements are applicable;
- Identifying the regulatory and compliance landscape;
- Reviewing the current GRC status;
- Determining the most optimal approach;
- Setting out key parameters on which success will be measured;
- Using a process oriented approach;
- Adapting global best practices as applicable; and
- Using uniform and structured approach which is auditable.

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is not only a regulatory requirement but it also makes business sense as effective GRC implementation helps in meeting not only compliance but business requirements as well. Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented. It is advisable that the board should mandate adaption of a GEIT framework such as COBIT 5, as an integral part of enterprise governance development. COBIT 5 frameworks would provide the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimized so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices would also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, specific success of a GRC program can be measured by using the following goals and metrics:

- The reduction of redundant controls and related time to execute (audit, test and remediate);
- The reduction in control failures in all key areas;
- The reduction of expenditure relating to legal, regulatory and review areas;
- Reduction in overall time required for audit for key business areas;

- Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
- Improvement in timely reporting of regular compliance issues and remediation measures; and
- Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

### 1.11 IT Compliance Review

Failures of some large enterprises in the last decade due to lack of adequate level of ERM has compelled regulators to mandate its enforcement thus necessitating compliance with **Governance, Risk and Compliance (GRC)**. Effective implementation of ERM requires consideration of multiple factors such as using a holistic approach, which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance.

In the US, Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. In India, Clause 49 of listing agreement issued by **Security and Exchange Board of India (SEBI)** mandates similar implementation of enterprise risk management and internal controls as appropriate for the enterprise. Further, the Information Technology Act, which was passed in 2000 and amended in 2008 provides legal recognition for electronic records and also mandates responsibilities for protecting information. The Act also identifies various types of cyber-crimes and has imposed specific responsibilities on corporate. Hence, it can be rightly said that implementing Governance, Risk, security and controls is not only a management requirement but is mandated by law, too. Hence, it is important for enterprises to be aware of and be well conversant of IT compliances and accordingly, implement processes and practices to manage these compliances both from conformance and performance perspective.

All listed Companies in India have to enter into an agreement with the Stock Exchange and this agreement is called the Listing Agreement. This agreement is more or less defined by SEBI and all Stock Exchanges have similar wordings. Apart from other clauses in the agreement some of the clauses in the listing agreement require additional disclosures from the listed companies and compliance with corporate governance and other requirements. One such clause is Clause 49 of the Listing Agreement that prescribes certain addition disclosure requirements and also corporate governance requirements. This requirement is similar to the requirement of the Sarbanes Oxley Act of the USA and there are similar legislations in Australia, Japan and other countries. In USA, the **Public Company Accounting Oversight Board (PCAOB)** has come out with detailed guidelines on Compliance by Auditors and Companies under the Act. In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members, which focuses primarily on audit requirements.

## 1.36 Information Systems Control and Audit

---

The Internal control requirements of Clause 49 are similar to SOX requirements. For example: Under section F.i.6, the agreement requires the Directors to cover their internal controls systems and their adequacy in the Management Analysis and Discussion. Under section V (c), the agreement requires the CEO/CFO to accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the effectiveness of internal control systems of the company pertaining to financial reporting and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies. Reporting on Internal control requirements are also mandated by the Indian Companies Act, 1956 for all companies and a separate annexure to the audit report has to be provided by auditors as per **Companies (Auditor's Report) Order, 2003 (CARO)**. Hence, implementing internal controls is mandated by law not only for listed companies but all companies.

### 1.11.1 Compliance in COBIT 5

The Management domain of "**Monitor, Evaluate and Assess (MEA)**" contains a compliance focused process: "**MEA03 Monitor, Evaluate and Assess Compliance with External Requirements**". This process is designed to evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. This requires that the enterprise has processes in place to obtain assurance and that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance. The primary purpose of this process is to ensure that the enterprise is compliant with all applicable external requirements.

Legal and regulatory compliance is a key part of the effective governance of an enterprise, hence its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03). In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures. In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process, which also include a compliance-related role.

The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities. The Governance activities related to GEIT are covered in the five processes of the Governance domain. The Risk management process and supporting guidance for risk management across the GEIT space meet the compliance need of regulations such as SOX and other similar regulations across the world. In fact, COBIT combined with COSO has been the most widely used framework for implementing IT controls as part of enterprise risk management to meet governance requirements. COBIT has a specific focus on compliance activities within the framework and explains how they fit within the complete enterprise picture. Inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements as silos of activity instead provides a comprehensive and holistic approach for ensuring compliance.

### 1.11.2 Key Management Practices of IT Compliance

COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. The practices are given as follows:

- **Identify External Compliance Requirements:** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
- **Optimize Response to External Requirements:** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements
- **Obtain Assurance of External Compliance:** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

### 1.11.3 Key Metrics for Assessing Compliance Process

Sample metrics for reviewing the process of evaluating and assessing compliance with external laws & regulations and IT compliances with internal policies are given as under:

- **Compliance with External Laws and Regulations:** These metrics are given as follows:
  - Cost of IT non-compliance, including settlements and fines;
  - Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;
  - Number of non-compliance issues relating to contractual agreements with IT service providers; and
  - Coverage of compliance assessments.
- **IT Compliance with Internal Policies:** These metrics are given as follows:
  - Number of incidents related to non compliance to policy;
  - Percentage of stakeholders who understand policies;
  - Percentage of policies supported by effective standards and working practices; and
  - Frequency of policies review and updates.

## 1.12 Information System Assurance

In the rapidly changing digital world, enterprises are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business

objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations. This dynamic changing environment provides a challenge for Chartered Accountants (as assurance providers) to provide assurance with the required level of confidence. However, with the right type of skills and toolsets, this provides an excellent opportunity for Chartered Accountants to act as consultants, who provide relevant IT enabled services. A key component of this knowledge base is usage of globally accepted good practices and frameworks and developing a holistic approach, which meets the needs of stakeholders.

### 1.12.1 Using COBIT 5 for Information System Assurance

Auditors will have to understand the business processes of the enterprises and organization structure to be effective. This understanding of the business process has to be coupled with understanding of the enterprise's policies, procedures and practices as implemented. Any enterprise executes its business operations through its staff. These staff needs to have defined job responsibilities, which are provided in the organization structure. The organization structure needs to have internal control structure. IT implementation in the enterprise makes it imperative that the internal control structure is built into the IT as deployed. Further, IT impacts the way business operations could be performed and internal controls are implemented. Hence, it is critical for auditors to understand the organization structure of the enterprise being audited as relevant to the objectives and scope of the assignment.

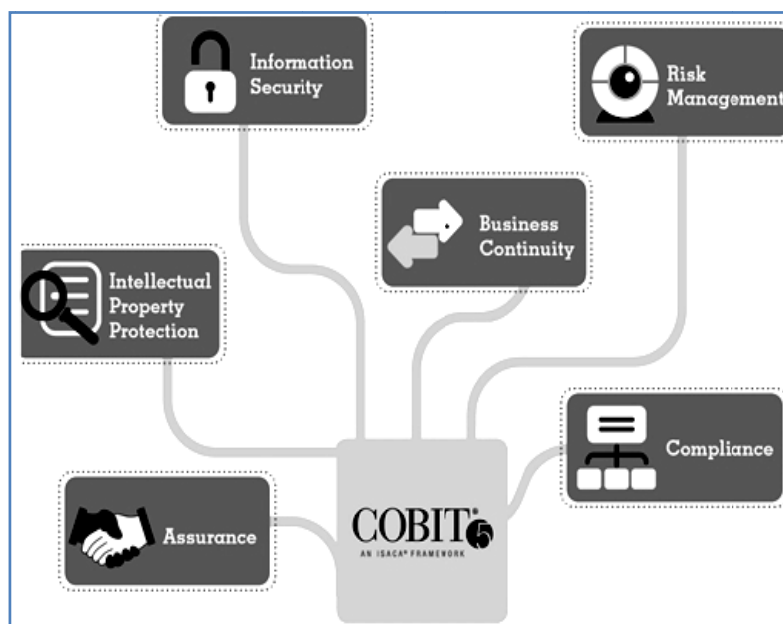


Fig. 1.12.1: Assurance Needs of COBIT 5\*

\* Source: [www.isaca.org](http://www.isaca.org)

COBIT 5 has been engineered to meet expectations of multiple stakeholders. It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc. It is written in a non-technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers; regulators for understanding and addressing IT related issues as relevant to them. Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, regulators and auditors (internal/external) for implementing or evaluating Governance and management practices from an end-to-end perspective. COBIT has been used as an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001 etc. have been integrated into overall enterprise governance. The Fig. 1.12.1 provides sample examples of the different assurance needs, which can be performed by using COBIT 5.

### 1.12.2 Evaluating IT Governance Structure and Practices by Internal Auditors

IT Governance can be evaluated by both external as well internal auditors. The following guidance is from internal audit perspective as issued by **The Institute of Internal Auditors (IIA)**. It outlines specific areas and critical aspects relating to governance structure and practices, which can be reviewed as part of internal audit. Internal audit activities in evaluating the IT governance structure and practices within an enterprise can evaluate several key components that lead to effective IT governance. These are briefly explained here.

- **Leadership:** The following aspects need to be verified by the auditor:
  - Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.
  - Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.
  - Determine how IT will be measured in helping the organization achieve these goals.
  - Review how roles and responsibilities are assigned within the IT organization and how they are executed.
  - Review the role of senior management and the board in helping establish and maintain strong IT governance.
- **Organizational Structure:** The following aspects need to be assessed by the auditor:
  - Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
  - This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. In addition, how IT mirrors the organization structure in its enterprise architecture should also be included.

## 1.40 Information Systems Control and Audit

---

- **Processes:** The following aspects need to be checked by the auditor:
  - Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems.
  - What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?
- **Risks:** The following aspects need to be reviewed by the auditor:
  - Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.
  - Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.
- **Controls:** The following aspects need to be verified by the auditor:
  - Assess key controls that are defined by IT to manage its activities and the support of the overall organization.
  - Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity.
  - Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.
- **Performance Measurement/Monitoring:** The following aspects need to be verified by the auditor:
  - Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

### 1.12.3 Sample Areas of GRC for Review by Internal Auditors

IIA provides areas, which can be reviewed by internal auditors as part of review of Governance, Risk and Compliance (GRC) areas. These are given as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
  - Promoting appropriate ethics and values within the organization;
  - Ensuring effective organizational performance management and accountability;



- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.
- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that:
  - Organizational objectives support and align with the organization's mission;
  - Significant risks are identified and assessed;
  - Appropriate risk responses are selected that align risks with the organization's risk appetite; and
  - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
- **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.
- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
  - Achievement of the organization's strategic objectives;
  - Reliability and integrity of financial and operational information;
  - Effectiveness and efficiency of operations and programs;
  - Safeguarding of assets; and
  - Compliance with laws, regulations, policies, procedures, and contracts.
- **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
- **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be

## 1.42 Information Systems Control and Audit

---

alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

### 1.12.4 Sample Areas of Review of Assessing and Managing Risks

This review covers the Controls over the IT process of assessing and managing risks and is expected to provide assurance to the management that the enterprise has identified all the risks relevant to the enterprise/business as relevant to IT Implementation. In addition, it is also expected to provide assurance that it has appropriate risk management strategy to mitigate these risks so as to satisfy the business requirement of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors.

This review broadly considers whether the enterprise is engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks. The specific areas evaluated are:

- Risk management ownership and accountability;
- Different kinds of IT risks (technology, security, continuity, regulatory, etc.);
- Defined and communicated risk tolerance profile;
- Root cause analyses and risk mitigation measures;
- Quantitative and/or qualitative risk measurement;
- Risk assessment methodology; and
- Risk action plan and Timely reassessment.

### 1.12.5 Evaluating and Assessing the System of Internal Controls

COBIT 5 has specific process: "MEA 02 Monitor, Evaluate and Assess the System of Internal Control", which provides guidance on evaluating and assessing internal controls implemented in an enterprise. The objective of such a review is to:

- Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews;
- Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions; and
- Plan, organize and maintain standards for internal control assessment and assurance activities.

Performing this review would provide assurance on the transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risks.

The key management practices for assessing and evaluating the system of internal controls in an enterprise are given as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

### 1.13 Summary

The chapter has highlighted the need for implementing the right type of IT controls as IT is all pervasive in enterprises today. For implementing IT controls, it is important to consider not only the regulatory but also the management perspective so as to ensure that both conformance and performance perspectives are covered. The key concepts of governance, enterprise governance, corporate governance, IT governance and Governance of enterprise IT

## 1.44 Information Systems Control and Audit

---

along with the Enterprise Risk Management and internal controls have been explained. This will enable to identify governance practices as implemented in enterprises and confirm their adequacy. This chapter has also provided an overview of the critical role of IT in achieving business objectives.

Risks are all pervasive and could lead to exposures, which could result in loss to enterprise. Hence, it is important to identify sources of risks, types of risks and exposures, the threats and vulnerabilities and the probability of occurrence and impact on the business. This is done through risk management strategy based on which risks are tolerated, terminated, treated, transferred or ignored depending on the cost and benefit analysis. Implementing risk management strategy is not only a management requirement but also a regulatory requirement. Usage of best practice guidance from frameworks such as COBIT enables enterprises to implement a holistic approach covering the complete life cycle of risk encompassing all aspects and ensures accountability is established both from governance and management perspective. Enterprises would be well served if they implement risk management not simply as a compliance issue but rather a new way of enhancing operational effectiveness and efficiency. This chapter has provided guidance and best practices for effective risk management which can be integrated with overall enterprise risk management and Governance.

IT compliance as part of Governance, Risk and Compliance under the umbrella of corporate governance is also discussed. This chapter has outlined the specific provisions pertaining to SOX, which has mandated the implementation of internal controls on management and its certification by external auditors. It has also provided the best practices guidance from COBIT 5, which can be applied for ensuring IT compliance within the enterprise. Clause 49 of listing agreement issued by SEBI of India and related provisions for implementing GRC are also discussed in the chapter.

The chapter has also provided a brief overview of COBIT 5 and highlighted the need for using globally accepted framework such as COBIT 5 for implementing GEIT. Information Technology increasingly impacts how electronic information and related controls are reviewed and accessed for providing compliance, assurance or consulting service for clients. Hence, it is imperative for auditors to update methodologies of how they provide services by using the relevant best practices and tools to ensure quality of services to clients. IT is an area which is a constant state of continuous improvement. Hence, it is vital for auditors to keep on updating knowledge and skills sets and explore innovative ways of delivering services using IT and related best practices.

Information Systems assurance is integral part of enterprise governance and this can be performed by internal as well as external auditors based on the scope and objectives of the review. As part of GEIT or GRC review, regulatory requirements mandate review of specific areas and certification to confirm whether the required Enterprise risk management and internal controls are in place. This chapter has provided a broad overview, sample areas and key management practices using best practices and guidance from COBIT 5 and IIA (The Institute of Internal Auditors) guidance. This could be used by external or internal auditors as per their requirement.

# 2

## Information Systems Concepts

---

### Learning Objectives

- To explain the basic concepts of Systems and their types;
- To understand the concepts of Information Systems;
- To explain various types of Information systems and their applications;
- To understand Information and its applications in businesses and organizations; and
- To explain the role of Information Technology (IT) in organizations and businesses.

### Task Statements

- To distinguish among different types of systems e.g. open, closed, probabilistic, deterministic, manual, physical etc.;
- To differentiate between data and information;
- To distinguish among different information systems e.g. TPS, MIS, DSS, EIS and office automation systems etc;
- To select the appropriate information system for a given problem; and
- To understand various terms e.g. database, data mining, data warehouse, ERP and business intelligence.

### Knowledge Statements

- To know the concepts of computer based information systems;
- To know the features, components and applications of different types of information systems e.g. TPS, MIS, DSS, OAS etc.;
- To know the types of information needed in top, middle and lower management levels of an organization;
- To know the role of information in different management levels of an organization;
- To know the attributes of information;
- To know the role of IT in various types of business applications e.g. E-business, wholesale marketing, retailing, public sectors etc.; and
- To know the underlying technologies for a computer based information system.

### 2.1 Introduction

An understanding of the effectual and accountable use as well as management of information systems/technologies is important for managers, business professionals, and other knowledge workers in today's inter-networked enterprises. Auditors in their role as reviewers of controls have to understand the key concepts and practice of information systems. Information system supports an organization's business processes and operations, business decision-making and strategic competitive advantage. There are various types of information systems available for use by an organization/business to achieve operational excellence, develop new products and services, and promote competitive advantages. Examples of information systems are: Management Information System, Decision Support System, Knowledge Management System etc.

An **Information System** is termed as a system that comprises of people, computer systems, data and network that helps to collect, store and analyze data to produce the desired information for the functioning, betterment and expansion of business. Information systems play a vital role in the enterprise collaboration and management and strategic success of businesses that must operate in an inter-networked global environment and also facilitate E-business and E-commerce operations. The field of information systems has become a major functional area of business administration and management.

The easy availability of internet enables even smaller enterprises the opportunity to compete against large companies. E-commerce enables buying, selling and exchanging of products, services and information between Business to Business, Business to Customer, Customer to Business and Customer to Customer via computer networks. By having online advertising, even smaller enterprises can reach to broad number of customers to increase the ability to find and sell to customers.

Senior management requires information to aid in planning and decision making whereas middle level management requires information that can help them in monitoring and controlling the business activities. Employees at operational level need information that can enable them to perform their day-to-day activities easily and speedily. This makes it clear that different types of information systems are required at different levels of management within the same enterprise.

Ensuring successful implementation of effective information system so as to obtain strategic and competitive advantage requires long term investment in an IT strategy as per the strategic needs of the management. This cannot be achieved by simply making one time heavy investment in one or more business applications but requires continuous and regular investment and monitoring effective implementation in the required areas so as to ensure that information system acts as the foundation to sustain and maintain growth.

In this chapter, the prime focus is on the systems, types of systems, general concept of information systems and its role in business. The chapter provides detailed description of classification of the information systems, its components, their use in various business applications and the role of IT in businesses and organizations.

## 2.2 Overview of Information Systems and Practical Aspects of their Applications in Enterprise Processes

In the present era of rapid growth in the technology, IT is a key enabler in all walks of life for all types of enterprises whether commercial or non-commercial. IT helps the storage, processing, transmission and exploitation of information so as to meet the needs of individuals, enterprises or government. IT has ushered in rapid and dynamic changes in business environment and the way enterprises operate and provide products or services. Because of the global competition, enterprises are in greater need of efficient and timely provision of information to enhance the ability to make decisions based on relevant information.

With the advent of new tools for information and knowledge gathering in IT, we can expect continued refinement in the traditional skills of management i.e. planning, organizing, decision making and controlling processes and operations.

### 2.2.1 Information

Technically, Information means processed Data. Data is facts or values of results, and information is the relations between data and other relations. e.g. in spread sheet student name, roll number and marks obtained in science and arts subjects represents data whereas the graph that shows the percentage of students acquire more than 80% in science subjects and 65% in arts subjects represents information. Information may be represented in the form of text, graph, pictures, voice, videos etc. Let us take another example "85", "Ira", "scored", "Maths", "in", "marks" itself represents data but it conveys information when we write sentence "Ira scored marks in Maths = 85" which is obtained after manipulating the data.

The collection of data is not information and collection of information is not knowledge. Information relates to description, definition, or perspective (what, who, when, where). Information is essential because it adds knowledge, helps in decision making, analyzing the future and taking action in time. Information products produced by an information system can be represented by number of ways e.g. paper reports, visual displays, multimedia documents, electronic messages, graphics images, and audio responses.

**Attributes of Information:** Some of the important attributes of useful and effective information are given as follows:

- **Availability** - It is a very important aspect of information. Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- **Purpose/Objective** - Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. Depending upon the activities in an organization the Information communicated to people has a purpose. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.

## 2.4 Information Systems Control and Audit

---

- **Mode and format** - The modes of communicating information to humans should be in such a way that it can be easily understood by the people. The mode may be in the form of voice, text and combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information the different formats can be used e.g. diagrams, graphs, curves are best suited for representing the statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- **Current/Updated** - The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed interval of time so that the current score will be available. Similar is the case with broker who wants the latest information about the stock market.
- **Rate** - The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example- the information available from internet site should be available at a click of mouse, one should not wait for it an hour.
- **Frequency** - The frequency with which information is transmitted or received affects its value. For example- the weekly reports of sales shows little change as compared to the quarterly and contribute less for accessing salesman capability.
- **Completeness and Adequacy** - The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example- the position of student in a class can be found out only after having the information of the marks of all students and the total number of students in a class.
- **Reliability** - It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **Validity** - It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
- **Quality** - It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- **Transparency** - It is essential in decision and policy making. 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.
- **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.

### 2.2.2 System

To understand the concepts of Information system, one should begin with the understanding of basic concepts of system. Let us first understand, what is a system? A system is a group of inter connected components working towards the accomplishment of a common goal by accepting inputs and producing outputs in an ordered transformation process. A system generally consists of input, processing, storage and output. Input is the data entering the system. Processing is the manipulation of the input data. Output is the data/instruction given by the system after processing and storage refers to the storage of data for current or future use. For example; a business is said to be system because it contains input e.g. people, machine, money, materials etc., which are processed by means of different processes such as production, marketing, finance etc. and produces output i.e. services and goods.

### 2.2.3 Classification of System

System can be classified on the basis of various parameters like elements, interactive behaviour, degree of human intervention and working output as shown in Fig. 2.2.1.

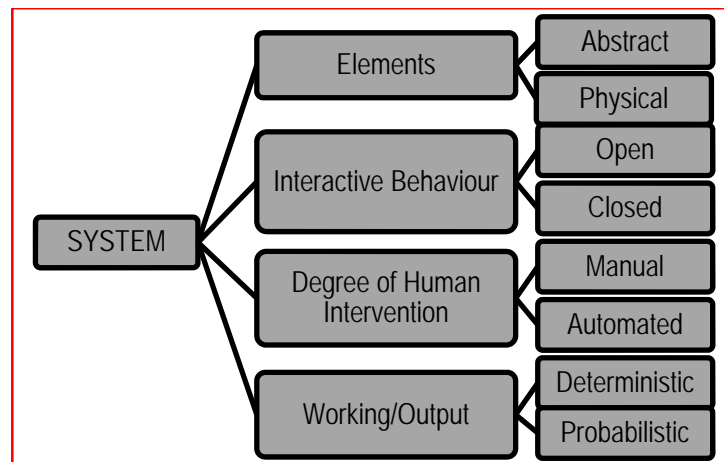


Fig. 2.2.1: Classification of System

- (i) **On the basis of Elements:** System may be categorized as **Abstract** or **Physical System** on the basis of the elements used in the 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.
  - **Physical System**, on the other hand, is a set of tangible elements, which operated together to accomplish an objective e.g. Computer system, University system etc.

## 2.6 Information Systems Control and Audit

---

- (ii) **On the basis of Interactive behavior:** Systems may be classified as **Open Systems** or **Closed System** based on 'how the system interacts with environment'.
- An **Open System** interacts with other systems in its environment. For example; Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.
  - **Closed System** does not interact with the environment and does not change with the changes in environment. 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.
- (iii) **On the basis of Degree of Human intervention:** According to the degree of human intervention, the system may be classified as **Manual** or **Automated System**.
- In a **Manual System**, the activities like data collection, maintenance and final reporting are done by human.
  - In an **Automated System**, the activities like data collection, maintenance and final reporting are carried out by computer system or say machine itself.
- (iv) **On the basis of Working/Output:** On the basis of working style and the output, the systems can be classified as **Deterministic** and **Probabilistic System**.
- A **Deterministic System** operates in a predictable manner. For example - software that performs on a set of instructions is a deterministic system.
  - A **Probabilistic System** can be defined in terms of probable behavior. For example - inventory system is a probabilistic system where the average demand, average time for replenishment, etc may be defined, but the exact value at any given time is not known.

### 2.2.4 Information Systems and its Components

With the help of information systems, enterprises and individuals are able to use computers to collect, store, process, analyze, and distribute information. There are different types of information systems, i.e. Manual (paper and pencil) information system, Informal (word to mouth) information system, Formal (written procedures) information system and Computer based information system. This chapter mainly focuses on computer based information system. A Computer Based Information system is a combination of people, IT and business processes that helps management in taking important decisions to carry out the business successfully.

An Information System comprise of **People, Hardware, Software, Data** and **Network** for communication support shown in Fig. 2.2.2. Here, people mean the IT professionals i.e. system administrator, programmers and end users i.e. the persons, who can use hardware and software for retrieving the desired information. The hardware means the physical components of the computers i.e. server or smart terminals with different configurations like

corei3/corei5/corei7 processors etc. and software means the system software (different types of operating systems e.g. UNIX, LINUX, WINDOWS etc.), application software (different type of computer programs designed to perform specific task) and utility software (e.g. tools). The data is the raw fact, which may be in the form of database. The data may be alphanumeric, text, image, video, audio, and other forms. The network means communication media (Internet, Intranet, Extranet etc.).

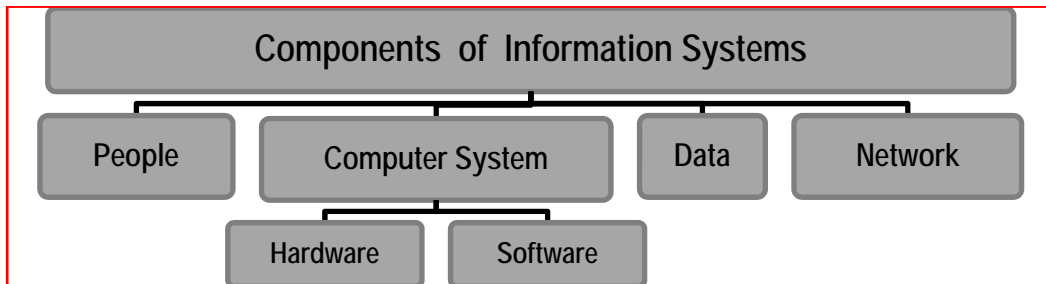


Fig. 2.2.2: Components of Information Systems

An Information System model comprises of following steps:

- Data is collected from an organization or from external environments and converted into suitable format required for processing (**Input**);
- This is converted into information (more meaningful form) obtained after manipulation of these collected data (**Processing**); and
- Then information is stored for future use or communicated to user after application of respective procedure on it (**Output**).

Three basics activities of an information system that are defined above, helps enterprise in making decisions, control operations, analyze problems and create new products or services as an output, as shown in Fig. 2.2.3. Apart from these activities, information systems also need feedback that is returned to appropriate members of the enterprises to help them to evaluate at the input stage.

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

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- 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.
- If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
- 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.

## 2.8 Information Systems Control and Audit

- 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.

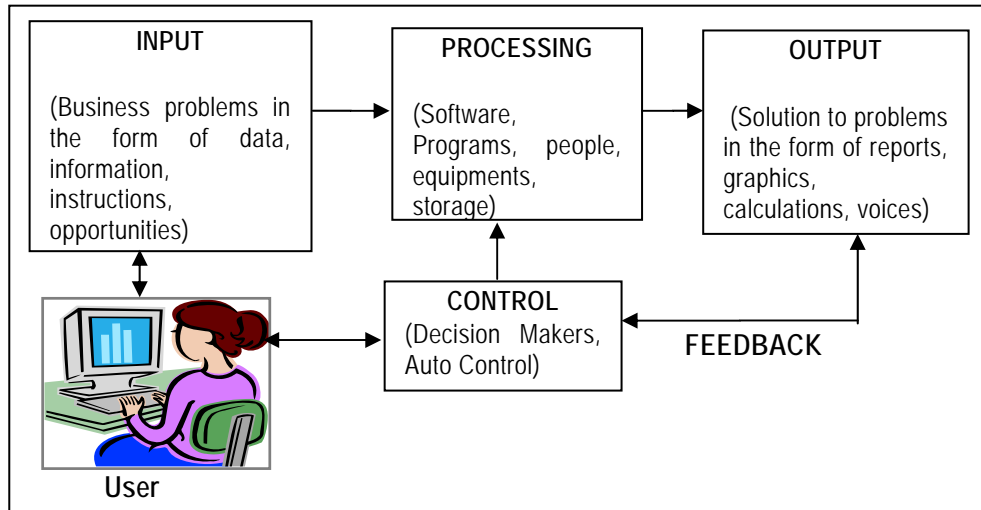


Fig. 2.2.3: Functions of Information Systems

Major areas of computer based applications are finance and accounting, marketing and sales, manufacturing, inventory/stock management, human resource management etc., which are given as follows:

- **Finance and Accounting** – The main goal of this subsystem (considering Business functions as whole system) is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget. It also helps in 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 a key role for running a business successfully in a competitive environment. The objective of this subsystem is to maximize the 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 the 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, sales man 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 the 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 the most effective and efficient way is an important function for any enterprise. Effective and efficient utilization of manpower in a dispute-free environment in this key functional area ensures to facilitate disruption free and timely services in business. Human Resource Management System (HRMS) 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.

### 2.2.5 Types of Information Systems

Information system performs important operational and managerial support roles in businesses and other enterprises. Conceptually, information systems are categorized as follows:

These aforementioned systems are described as follows:

**I. Operational-Level Systems:** These support operational managers in tracking elementary activities. These can include tracking customer orders, invoice tracking, etc. Operational-level systems or Operational Support Systems (OSS) ensure that business procedures are followed. Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use. Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database. The main objective of OSS is to improve the operational efficiency of the enterprise. These are further categorized as follows:

## 2.10 Information Systems Control and Audit

TYPES OF SYSTEMS		GROUPS SERVED
ESS	<p style="text-align: center;"><u>Strategic Level Systems</u></p> <p>5-year operating plan    5-year budget forecasting    5-year sales trend forecasting    Profit planning    Manpower planning</p>	Senior Managers
MIS DSS	<p style="text-align: center;"><u>Management Level Systems</u></p> <p>Sales management    Inventory Control    Annual budgeting    Capital Investment analysis    Relocation analysis Sales region analysis    Production Scheduling    Cost analysis    Pricing/profitability analysis    Contract cost analysis</p>	Middle Managers
KMS OAS	<p style="text-align: center;"><u>Knowledge Level Systems</u></p> <p>Engineering workstations    Graphics workstations    Managerial workstations Word processing    Document Imaging    Electronic Calendars</p>	Knowledge and Data Workers
TPS	<p style="text-align: center;"><u>Operational Level Systems</u></p> <p>Machine control    Securities trading    Payroll    Compensation Order Tracking    Plant scheduling    Accounts payable    Training &amp; development Order processing    Material movement control    Cash management    Accounts receivable    Employee record keeping</p> <p>Sales and marketing    Manufacturing    Finance    Accounting    Human Resources</p>	Operational Managers

Fig. 2.2.4: Types of Information Systems and the Groups Served

(A) **Transaction Processing Systems (TPS)** - At the lowest level of management, TPS 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. TPS will thus record and manipulate transaction data into usable information. Typically, a TPS involves the following activities:

- Capturing data to organize in files or databases;
- Processing of files/databases using application software;
- Generating information in the form of reports; and
- Processing of queries from various quarters of the organization.

A TPS may follow the 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.

(a) **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 in to 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 common 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 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.

(b) **Features of TPS**

Basic features of TPS are given as follows:

- **Large volume of data** - As TPS is transaction oriented and generally consists of large volumes of data, it requires greater storage capacity. Their primary objective is to ensure that the data regarding the economic events in the enterprises are captured quickly and correctly.
- **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.
- **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

## 2.12 Information Systems Control and Audit

---

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.

- **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.

**II. Knowledge-Level Systems:** These systems support discovery, processing and storage of knowledge and data workers. These support the business to integrate new knowledge into the business and control the flow of paperwork and enable group working. It helps the organization's knowledge and data workers and is especially in the form of workstations. It is the fastest growing application in business today.

**(A) Office Automation Systems (OAS)** – It is most rapidly expanding computer based information systems. Different office activities can be broadly grouped into the following types of operations:

- **Document Capture** – Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- **Document Creation** – This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- **Receipts and Distribution** – This basically includes distribution of correspondence to designated recipients.
- **Filling, Search, Retrieval and Follow up** – This is related to filling, indexing, searching of documents, which takes up significant time.
- **Calculations** – These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- **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, efficient and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

**(a) Benefits of Office Automation Systems** – Major benefits of OAS are given as follows:

- Office Automation Systems improve communication within an organization and between enterprises.
- They reduce the cycle time between preparation of messages and receipt of messages at the recipients' end.
- They also reduce the costs of office communication both in terms of time spent by executives and cost of communication links.



- Office Automation Systems ensure accuracy of information and smooth flow of communication.
- (b) **Computer Based Office Automation Systems** – Major computer based OAS are given as follows:
  - **Text Processing Systems** – The key points relating to Text Processing systems are given as follows:
    - 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.
  - **Electronic Document Management System** – The key points relating to these systems are given as follows:
    - The computer based document management systems capture the information contained in documents, stored for future reference and make them available 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.
- **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** – Three basic components based message communication systems are given as follows:

(a) **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 integration helps in ensuring that the message if accurate and the information required for the message is accesses quickly.
- ✓ **Portability** - Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal computer/tablet/smart phones 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 for sending and receiving 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 enterprise.

- (b) **Facsimile (Fax)** – It 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. The use of fax is gradually fading away with more and more use of electronic communication through emails.
- (c) **Voice Mail** – Voice mail is 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.

- **Teleconferencing and Video-conferencing Systems** - Teleconferencing is conducted in 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 visual communication software. The communication links are still quite expensive making the desktop video conferencing useful only for selected applications.

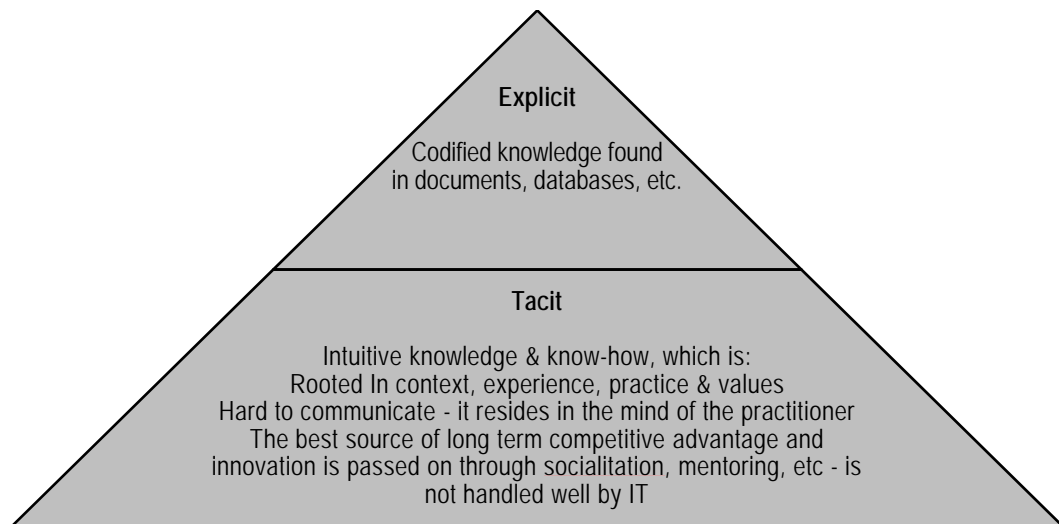
- (B) ***Knowledge Management System (KMS)*** - *The world is moving swiftly in the direction of a knowledge-based system as enterprises adapt more and more cost-cutting measure. There is a paradigm shift from an economy principally concerned by the management of tangible resources (equipment, machinery, buildings, ...) to an economy in which renovation and growth are determined by intangible resources and investments (knowledge, technology, competencies, abilities to innovate....). Information and Knowledge are the key elements of this economy. A firm's competitive gain depends on its knowledge processing i.e. what it knows; how it uses & how fast it can know something new. It's much more influential than the harmony of land, labour & capital (i.e. three most important production factors). Even though there is not a lucid and exclusive definition of the so-called*

*knowledge-based or knowledge-driven economy, it seems to be unstated as the 'upshot of a set of structural changes'.*

*Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organizational knowledge. It refers to a multi-disciplined approach to achieving organizational objectives by making the best use of knowledge. Knowledge Management Systems (KMS) refers to any kind of IT system that stores and retrieves knowledge, improves collaboration, locates knowledge sources, mines repositories for hidden knowledge, captures and uses knowledge, or in some other way enhances the KM process. KMS treats the knowledge component of any organization's activities as an explicit concern reflected in strategy, policy, and practice at all levels of the organization.*

*There are two broad types of knowledge - Explicit and Tacit as shown in the Fig. 2.2.5. KMS makes a direct connection between an organization's intellectual assets — both Explicit [recorded] and Tacit [personal know-how] — and positive results.*

- ◆ **Explicit knowledge:** *Explicit knowledge is that which can be formalized easily and as a consequence is easily available across the organization. Explicit knowledge is articulated, and represented as spoken words, written material and compiled data. This type of knowledge is codified, easy to document, transfer and reproduce. For example – Online tutorials, Policy and procedural manuals.*
- ◆ **Tacit knowledge:** *Tacit knowledge, on the other hand, resides in a few often-in just one person and hasn't been captured by the organization or made available to others. Tacit knowledge is unarticulated and represented as intuition, perspective, beliefs, and values that individuals form based on their experiences. It is personal, experimental and context-specific. It is difficult to document and communicate the tacit knowledge. For example – hand-on skills, special know-how, employee experiences.*



*Fig. 2.2.5: Types of Knowledge*

*It is this tacit knowledge that differentiates between organizations when push comes to shove, and hence provides the strategic edge to any organization. A regular example in the software industry is how to write code to get around a particular limitation, or to include a particularly tricky condition.*

**III. Management-Level Systems:** It supports the middle managers in monitoring, decision-making and administrative activities. This is helpful in answering questions like are things working well and in order? It provides periodic reports rather than instant information on operations. For example- a college control system gives report on the number of leaves availed by the staff, salary paid to the staff, funds generated by the fees, finance planning etc. This type of systems mainly answer "what if" questions. For example - What would be quality of teaching if college has to achieve top ranking in academics? These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems.

MSS supports managers in effective decision making by providing relevant and required information at the right time to the right people. Management Information System and Decision Support Systems are types of Management Level systems. Each of them is briefly discussed below:

**(A) Management Information Systems (MIS)** – Management Information System enables management at different levels 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. Since 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.

Many experts have defined MIS in different ways. MIS 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". Other notable definition of MIS is "**MIS is a computer based system that provides flexible and speedy access to accurate data**". MIS supports 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 but is condensed or summarized compared to the information provided to those at middle level management. MIS provide reports to management that can help in making effective, structured types as applicable to decisions of day-to-day operations. These reports and displays can be made available on demand, periodically or whenever exceptional conditions occurred.

**(a) Characteristics of an effective MIS:** Major characteristic of an effective MIS are given as follows:

## 2.18 Information Systems Control and Audit

---

- **Management Oriented** – It means that efforts 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 but may also meet the information requirements of middle level or operating levels of management as well.
- **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.
- **Integrated** – The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- **Common Data Flows** – It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they 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.
- **Heavy Planning Element** – An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- **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 phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- **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.
- **Computerized** - Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use

equips 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.

**(b) Misconceptions about MIS** – Following are the major misconceptions about MIS:

- Any computer based information system is a MIS.
- Any reporting system is MIS.
- MIS is a management technique.
- MIS is a bunch of technologies.
- MIS is an implementation of organizational systems and procedures. It is a file structure.
- The study of MIS is about use of computers.
- More data in generated reports refers more information to managers.
- Accuracy plays vital role in reporting.

**(c) Pre-requisites of an Effective MIS** – The pre-requisites of an effective MIS are given as follows:

- **Database** - It is collection of files, which is collection of records and records are nothing but collection of data. The data in database is organized in such a way that accessing to the data is improved and redundancy is reduced. The main characteristics of database are given 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 Database Management System (DBMS).
- **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 experts 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/s should also be capable of understanding management concepts to facilitate the understanding of problems faced by the

## 2.20 Information Systems Control and Audit

---

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.
- **Support of Top Management** – The support from top management is required for the effectiveness of MIS in an organization. The reasons for the same are as follows:
  - Any implementation, which does not receive the support of top management will not be effectively controlled and tends to be get lesser priority and may be delayed or abandoned.
  - 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.
- **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. Formal methods for changing and documenting changes must be provided.
- (d) **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 major 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.
- (e) **Constraints in operating a MIS** – Major constraints, which come in the way of operating an information system, are given as follows:



- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- 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.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
- 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.

**(f) Limitations of MIS** – Major Limitations of MIS are given as follows:

- The quality of the outputs of MIS is basically governed by the quantity of input and processes.
- 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.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- 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 or senior management.
- MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

**(B) Decision Support System (DSS)** – Decision Support System is a type of computerized information system that supports business and organizational decision-making activities.

## 2.22 Information Systems Control and Audit

---

A properly-designed DSS is an interactive software-based system intended to help decision makers to compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions. 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. A DSS supports the human decision-making process, rather than a means to replace it.

Two types of planning languages that are commonly used in DSS are: **General-purpose planning languages** and **Special-purpose planning languages**. These are discussed below:

- **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.

(a) **Characteristics of DSS** – The key characteristics of DSS are given as follows:

- This supports decision making and occurs at all levels of management.
- Instead of helping individuals working on independent tasks, it should be able to help group making decisions.
- It should be flexible and adaptable, i.e. it should be able to fit itself in the style of a particular manager and ready to change according to changes in the environment.
- DSS focuses on decision rather than data and information.
- It should be easy to use. A user should not have knowledge of computer programming to generate reports that helps in decision making.
- DSS can be used for structured problems.
- DSS should be user-friendly.
- DSS should be extensible and evolve overtime.
- DSSs are used mainly for decision making rather than communicating decisions and training purposes.
- The impact of DSS should be on decision where the manager's judgment is essential and there is sufficient structure for computers.

- (b) **Components of DSS** – A Decision Support System comprise of four basic components, which are discussed below:
- **The user** - The user of a DSS 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. The key points relating to these users are given as follows:
    - **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.
  - **Databases** – A DSS includes 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 of an organization. For example; data about economic conditions, market demand for the organization's goods or services, and industry competition. DSS 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:

- **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.
- **Logical Level** – It is designed by professional programs, which 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.
- **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.

- **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.
- (c) **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 enterprises 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 Auto Man, which allows decision makers to consider financial, non financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. Then they can 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 DSS 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.

- (d) **Difference between DSS and traditional MIS:** Major difference between the DSS and the traditional MIS are shown in following Table 2.2.1.

**Table 2.2.1: Difference between DSS and Traditional MIS**

Dimensions	Decision Support System	Traditional MIS
Philosophy	Providing integrated tools, data, models, and languages to end users	Providing structured information to end users
Orientation	External orientation	Internal orientation
Flexibility	Highly flexible	Relatively inflexible
Analytical capability	More analytical capability	Little analytical capability
System analysis	Emphasis on tools to be used in decision process	Emphasis on information requirement analysis
System design	Interactive process	System development based on static information requirements

**IV. Strategic Level Systems:** For strategic managers to track and deal with strategic issues, assisting long-range planning. It supports the senior level management to tackle and address strategic issues and long term trends, both inside organization and the outside world. It answers questions like what products should be launched to increase the profit and capture the market. It helps in long term planning. A principle area is tracking changes in the external conditions (market sector, employment levels, share prices, etc.) and matching these with the internal conditions of the organization.

- (A) **Executive Information Systems (EIS)** – It is sometimes referred to as an Executive Support System (ESS). It serves the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any preset applications or specific competence.

- (a) **Characteristics of EIS** – Major Characteristics of an EIS are given as follows:
- EIS is a Computer-based-information system that serves the information need of top executives.
  - EIS enables users to extract summary data and model complex, problems without the need to learn query languages statistical formulas or high computing skills.
  - EIS provides rapid access to timely information and direct access to management reports.
  - EIS is capable of accessing both internal and external data.
  - EIS provides extensive online analysis tool like trend analysis, market conditions etc.
  - EIS can easily be given as a DSS support for decision making.
- (b) **The Executive Decision-Making Environment** – The type of decisions that executives must make are very broad. Often, executives make these decisions based on a vision they have regarding 'what it will take to make their enterprise 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 given as follows:
- **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, enterprises 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 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.

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.

- (c) **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 management and then expand in response to questions asked by those managers as they use the system. Over the 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:

- 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.
- 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.
- 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.
- 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.
- 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.
- EIS measures must evolve to meet the changing needs of the organization.

## 2.28 Information Systems Control and Audit

- (d) **Difference between EIS and Traditional Information Systems** - The main difference between EIS and Traditional Information Systems are shown in the following Table 2.2.2:

Table 2.2.2: Difference between EIS and Traditional Information Systems

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	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 levels	Available	Not available
Information format	Text with graphics	Tabular
Nature of interface	User-friendly	Computer-operator generated

Based on the aforementioned facts, the following Table 2.2.3 describes all the major information systems at-a-glance.

Table 2.2.3: Different Information Systems

Information System	Description
<b>Transaction Processing Systems (TPS)</b>	These are designed to process and carry out routine transactions efficiently and accurately. A business will have several TPS. For example, Billing systems and invoices to customers, to calculate the weekly and monthly payroll and tax payments of an organization, to calculate raw material requirements, stock control systems to process all movements into, within and out of the business etc.
<b>Office Automation Systems (OAS)</b>	These are systems that help in the enhancement of performance of or productivity of employees who are dealing with the data processing and information. For example, the use of MS-Office can generate the list of customers who have done purchase of certain type of products, number of sales of products done on a particular date etc.



<b>Knowledge Management Systems (KMS)</b>	<p>These help businesses in creation and sharing of information and are typically used in a business where employees create new knowledge and expertise, which can then be shared by other people in the enterprise to create further commercial opportunities. For example, KMS are most effectively used in firms of lawyers, accountants and management consultants.</p> <p>One can say that these are effective in systems, which allow efficient categorization and distribution of knowledge. For example, Knowledge discovery in database and Data mining tools can be used to extract the knowledge from word processing documents, spread sheets, PowerPoint presentations, internet pages, databases, data warehouses.</p>
<b>Decision Support Systems (DSS)</b>	<p>These are specifically designed to help management to make decisions in situations where there is uncertainty about the possible outcomes of those decisions. DSS consists of tools and techniques that gather relevant information and helps in analysis of the options and alternatives. It usually uses complex spread sheet and databases to generate information.</p>
<b>Management Information Systems (MIS)</b>	<p>It is mainly concerned with internal sources of information. It inputs data usually from the transaction processing systems and gives output as a series of management reports.</p> <p>MIS reports can be used by middle management and operational supervisors to gather desired information.</p>
<b>Executive Support System (ESS)</b>	<p>Executive Support System (ESS) is a reporting tool (software) that allows us to turn our organization's data into useful summarized reports. These reports are generally used by executive level managers for quick access to reports coming from all company levels and departments such as billing, cost accounting, staffing, scheduling, and more.</p>

### 2.2.6 Specialized Systems

Apart from the information systems discussed above, there exists other categories of information systems also that provide comprehensive end to end IT solutions and services (including systems integration, implementation, engineering services, software application customization and maintenance) to various corporations globally. Some of them are Expert Systems, Cross Functional Information Systems, and Core Banking System (CBS) etc.

- (A) **Expert System** - An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert Systems 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 –

## 2.30 Information Systems Control and Audit

---

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

- **Accounting and Finance** - It provides tax advice and assistance, helping with credit- authorization decisions, selecting forecasting models, providing investment advice.
- **Marketing** - It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
- **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.
- **Personnel** - It is useful in assessing applicant qualifications, giving employees assisting at filling out forms.
- **General Business** - It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

(a) **Need for Expert Systems** – Major reasons for the need of expert systems is given as follows:

- 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.
- 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.

(b) **Benefits of Expert Systems** – The key benefit of expert systems are given as follows:

- Expert Systems preserve knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.
- Expert Systems put information into an active-form so it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professional do.

- Expert Systems are not subjected to such human fallings as fatigue, being too busy, or being emotional.
- Expert Systems can be effectively used as a strategic tool in 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 possess to qualify for Expert System development are given as follows:

- **Availability** – One or more experts are capable of communicating ‘how they go about solving the problems to which the Expert System will be applied.’
- **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.
- **Domain** – The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.
- **Expertise** – Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure** – The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

- (B) **Cross Functional Information Systems** – It is also known as integrated information system that combines most of information systems and designed to produce information and support decision making for different levels of management and business functions. Example – Enterprise Resource Planning (ERP).

**Enterprise Resource Planning (ERP)** - *Enterprise resource planning (ERP) is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing. ERP software is considered an enterprise application as it is designed to be used by larger businesses and often requires dedicated teams to customize and analyze the data and to handle upgrades and deployment. In contrast, Small business ERP applications are lightweight business management software solutions, customized for the business industry we work in.*

(a) **Components of ERP**

*ERP model is consists of four components which are implemented through a methodology. All four components are as follows:*

(i) **Software Component**: *The software component is the component that is most visible part and consists of several modules such as*

*Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligent.*

*(ii) Process Flow: It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.*

*(iii) Customer mindset: By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.*

*(iv) Change Management: In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.*

**(b) Benefits of ERP**

- Streamlining processes and workflows with a single integrated system.*
- Reduce redundant data entry and processes and in other hand it shares information across the department.*
- Establish uniform processes that are based on recognized best business practices.*
- Improved workflow and efficiency.*
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.*
- Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.*
- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.*
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.*
- Track actual costs of activities and perform activity based costing.*
- Provide a consolidated picture of sales, inventory and receivables.*

**(C) Core Banking System (CBS) - Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices. Normal core banking functions will include transaction accounts, loans, mortgages**

*and payments. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.*

*Most commonly, Core Banking System (CBS) may be defined as a back-end system that processes daily banking transactions, and posts updates to accounts and other financial records. These systems typically include deposit, loan and credit-processing capabilities, with interfaces to general ledger systems and reporting tools. Core banking functions differ depending on the specific type of bank. Examples of core banking products include Infosys' Finacle, Nucleus FinnOne and Oracle's Flexcube application (from their acquisition of Indian IT vendor i-flex). Elements of core banking include:*

- *Making and servicing loans.*
- *Opening new accounts.*
- *Processing cash deposits and withdrawals.*
- *Processing payments and cheques.*
- *Calculating interest.*
- *Customer Relationship Management (CRM) activities.*
- *Managing customer accounts.*
- *Establishing criteria for minimum balances, interest rates, number of withdrawals allowed and so on.*
- *Establishing interest rates.*
- *Maintaining records for all the bank's transactions.*

### 2.2.7 Application of Information Systems in Enterprise Processes

Information Systems perform following three vital roles in business firms:

- (i) **“Support an organization's business processes and operations”**: This includes operations support systems such as Transaction Processing Systems, Process Control Systems.
- (ii) **“Support business decision-making”**: This includes Management Information Systems, Decision Support Systems, and Executive Information Systems.
- (iii) **“Support strategic competitive advantage”**: This includes Expert Systems, Knowledge Management Systems, Strategic Information Systems, and Functional Business Systems.

To operate Information Systems (IS) effectively and efficiently a business manager should have following knowledge about it:

- **Foundation Concepts** – It includes fundamental business, and managerial concepts e.g. 'what are components of a system and their functions', or 'what competitive strategies are required'.

## 2.34 Information Systems Control and Audit

- **Information Technologies (IT)** – It includes operation, development and management of hardware, software, data management, networks, and other technologies.
- **Business Applications** – It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.
- **Development Processes** – It comprise how end users and IS specialists develop and execute business/IT solutions to problems.
- **Management Challenges** – It includes ‘how the function and IT resources are maintained’ and utilized to attain top performance and build the business strategies.

IT can be viewed as a subsystem of information system that includes hardware, software, databases, networks and other electronic devices. Sometimes, the term Information Technology can be used interchangeably with information systems. Information Technology refers to the technology of the production, storage and communication and management of information using computers and micro-electronics and is a crucial part of information systems. Most of the businesses use IT to create and process data.

Small businesses generally need to purchase software packages, and may need to contract with IT businesses that provide services such as hosting, marketing web sites and maintaining networks. However, larger companies can consider having their own IT staffs to develop software, and otherwise handle IT needs in-house. IT has changed the working styles of staff at all levels of enterprises, from the executives to middle management and lower level staff e.g. Supervisors etc. The primary areas where IT enabled tools are used in any organization is shown in Fig. 2.2.6 whereas Fig. 2.2.7 showcases different IT enabled tools used at three layers i.e. top, middle and lower management of an organization.

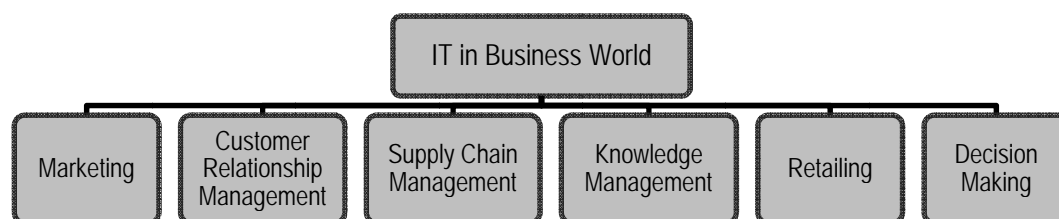


Fig. 2.2.6: IT in Prime Business Areas

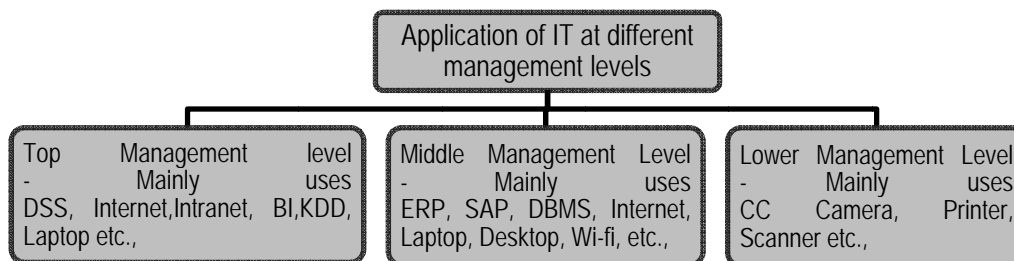


Fig. 2.2.7: Application of IT at Different Management Levels

Following are some of the important implications of information systems in business:

- Information system helps managers in efficient decision-making to achieve the organizational goals.
- An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.
- Information systems helps in making right decision at the right time i.e. just on time.
- A good information system may help in generating innovative ideas for solving critical problems.
- 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.

In recent years, the advent of IT has transformed the way marketing is done and how companies manage information about their customers. The first step in marketing is the identification of patterns in a large data set of the customer and making critical marketing decisions. The technologies used to implement knowledge management are artificial intelligence, extranet, groupware, decision support system, document management system, data warehousing, data mining, intranet and internet.

By the use of IT tools, large volume of data related to customers can be stored and is available for use. This has created opportunities as well as challenges for businesses to gain competitive advantage.

### **2.3 Relative Importance of Information Systems from Strategic and Operational Perspectives**

A **Business Model** can be defined as an outline of 'how business is to be done by a company to generate maximum revenue'. A **Business Strategy** is defined as a long term planning for success i.e. tactics that are applied to manage business for increasing business revenue. It emphasizes on competition that business model does not. A good business strategy is one that enables company to satisfy customers, uses resources efficiently and explore business opportunities outside of the standard business practice to help inspire company expansion.

An Information System can be large or small depending upon the size of the company and can help in decision making, produce high quality of products and perform logistical functions. An information system can assist in determining scenarios such as unifications and achievements, and streamline the strategic planning process that can help top management to take corporate decision, easily. In operations management, information systems design can apply to production control, research, development, and manufacturing to produce desired results of the products in terms of quality and cost. Information systems applications in the area of human resources management can help in retaining highly qualified employees by having important data concerning employees obtained after several processes used by human resource managers or personnel. Information systems also support logistical processes in various ways, such as real time inquiries to track an item from the point of shipment, receiving

## 2.36 Information Systems Control and Audit

---

and storage of the item and inventory status of the item. Not only this, information systems can also provide the structure for programmers, database managers and data administrators to collaborate on new and existing projects.

In this age of technology and competition, enterprises are looking for novel ideas and information that can enhance and expand their business. In order to achieve this, they are becoming more and more dependent on information systems. Information system is used in every aspects of business right from customer relationship management, marketing strategies, retailing, communication, product promotion, product development, forecast future sales to supply chain management etc. ERP, Data Mining tools, Data warehouse, Business intelligence, MIS, internet, intranet, extranet etc. are the information systems and information technologies that support managers in every step of business.

Information Systems have accelerated the pace of processing of enterprise information using IT and integrating all aspects of the operations of the business e.g. instead of gathering data manually and taking out hidden information from it by conducting meeting of executives, which is crucial in decision making for marketing strategies, customer relationship management etc., the same can be obtained by using the respective data mining tools and data warehouse. Not only this, Information System also provides new platform to business world where space and time is no more obstacle. For example, selling and purchasing of products can be done on web any time and from anywhere.

There are different kinds of systems depending upon the different interest, specialties and levels in an organization. The organization comprise of strategic, management, knowledge and operational levels, which is further divided into functional areas e.g. sales, marketing, manufacturing, finance, accounting and human resources.

For example - the sales area uses operational level system to keep track of daily sales figures, a knowledge level systems designs the promotional displays of the organization, a management level system generate report of the monthly sales by territory and a strategic level system predicts the sale of the product in coming five years.

Managers or business professionals are not required complete understanding of complex technologies, concepts and the specialized applications in the area of information systems but what they should know is illustrated in Fig. 2.3.1. This outlines five key areas of knowledge requirements, which are given below:

- Foundation concepts,
- Information technologies,
- Business applications,
- Development processes, and
- Management challenges.



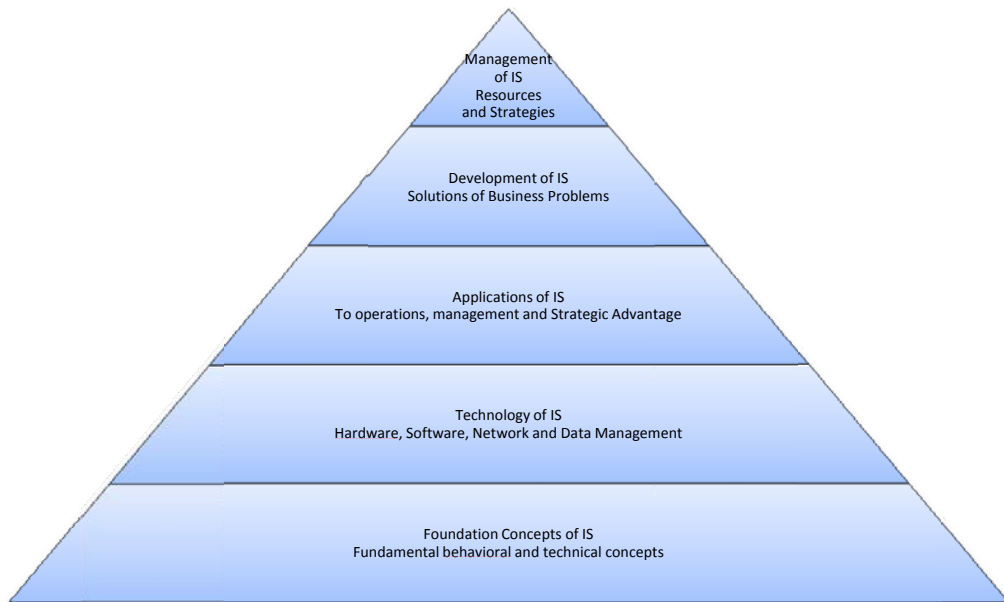


Fig. 2.3.1: Framework of Information Systems for Business Professionals

## 2.4 Information as a Key Business Asset and its Relation to Business Objectives and Processes

Information is a strategic resource that helps enterprises in achieving long term objectives and goals. In today's competitive and unpredictable business environment, only those enterprises survive, which have complete information and knowledge of customer buying habits and market strategy. Information management enhances an organization ability and capacity to deal with and achieve its mission by meeting challenges of competition, timely performance and change management. This is critical as the managed information and knowledge enables the enterprise to deal with dynamic challenges and effectively envision and create their future. This requires coordination between people, processes and technology.

### 2.4.1 Role of Information in Business

In today's dynamic business environment, it becomes mandatory to have complete information and knowledge of customer buying habits and market strategy for any enterprise. Timeliness, accurate, meaningful and action oriented information enhances an organization ability and capacity to deal with and develop in mission, competition, performance and change.

The information can be categorized on the basis of its requirement by the top, middle and lower level management as seen in Fig. 2.4.1.

The top management generally comprise of owners/shareholders, board of directors, its chairman, managing director, or the chief executive, or the managers committee having key officers, the middle management comprise of heads of functions departments e.g. purchase manager, production manager, marketing managers, financial controller, and divisional sectional officers

## 2.38 Information Systems Control and Audit

working under these functional heads, whereas the lower level managers are superintendents, supervisor, etc.

Top level management strives for the information that can help them in major policy decisions such as establishment of new plant, launching of new product etc. In other words, we can say that the top management requires strategic information that helps them in making strategy of an enterprise in terms of scope of products, targets of products i.e. customers, competition with market i.e. price, quality, long term planning etc. The information about the customers buying habits such as what combination of products and type of products they are likely to purchase together helps top managers to decide the launching of new products. e.g. if the information like a customer whose income is more than one lakh per month and working in IT sector and are in habit of buying latest model of laptops are more in a city where large number of IT companies are existing then it's better to launch notebook with latest operating system there. Such information can help top management of company to decide to work on new products as well as the location where it has to be launched for maximum profit and sale which is one of the objectives and goals of the top management.

Middle managements require tactical information that helps in implementing decisions taken by the top management. For example - information of customers likely to purchase certain product in a particular location can help sales managers to fulfill their sales target efficiently. Tactical information is used for short term planning whereas strategy information is used for long term planning. For example, the offers of companies during festive seasons are a short term planning, which is done by having information about the customers buying capacity in that location.

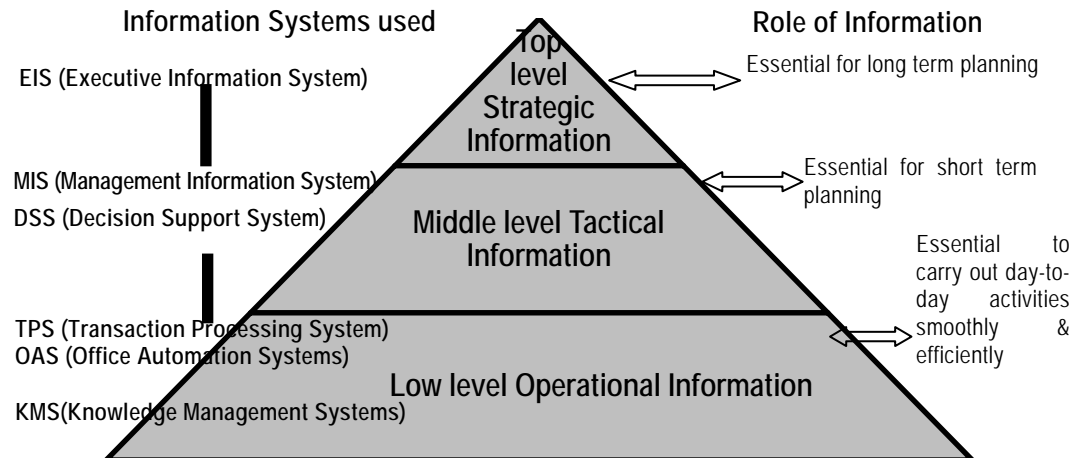


Fig. 2.4.1: Types of Information Systems at Different Management Levels

The lower management requires operational information, which is required in day-to-day activities. The operational information mainly comprises of information about stock on hand, information about customer order pending, information about bill payable by customer etc. These are essential for smooth running of the daily activities of a business at primary level. For example, if a regular customer demands for a product other than the daily purchase then this information is important for salesman because it will help him in providing better service.

## 2.5 Various types of Business Applications

Information system has changed traditional business system in their entirety. With the advent of IT, everything is just a mouse click away and is available anytime, anywhere. IT has increased the communication between executives by providing for online meeting and instant exchange of information, irrespective of their location. Information system also contributes to an organization's success by providing information that provides innovative ideas to managers and helps them in decision making which is very important to keep the organization ahead in this competitive era. Financial, trading, manufacturing, retail industries etc. are moving towards a real time business model where transaction and information sharing are near instantaneous. The impact of IT on Information Systems for different sectors is explained below:

- (i) **E-business** – This is also called electronic business and includes purchasing, selling, production management, logistics, communication, support services and inventory management through the use of internet technologies. The primary components of E-business are infrastructure (computers, routers, communication media e.g. wire, satellite etc., software and programmers), electronic commerce and electronically linked devices and computer aided networks. The advantage of E-business are 24 hour sale, lower cost of doing business, more efficient business relationship, eliminate middlemen, unlimited market place and access with broaden customer base, secure payment systems, easier business administration and online fast updating. This is so because it does not require land for store or shops and anyone from anywhere can do business anytime as information regarding products etc. is available on the web. Only investment is needed in the purchase of space on internet, designing and maintenance of website. Different types of business can be done e.g. it may be B2B (Business to Business), B2C (Business to Customer), C2C (Customer to Customer) and C2B (Customer to Business). Because of no limitations of time and space, people prefer to involve in E-business. Thus, we can say that IT has given new definition to business.
- (ii) **Financial Service Sector** – The financial services sector (banks, building societies, life insurance companies and short term insurers) manages large amounts of data and processes enormous numbers of transactions every day. Owing to application of IT, all the major financial institutions operate nationally and have wide networks of regional offices and associated electronic networks. The associated substantial client databases are handled via large central mainframe systems that characterize the industry. IT has changed the working style of financial services and makes them easier and simpler for customers also. Now-a-days most of the services are offered by the financial services on internet, which can be accessed from anywhere and anytime that makes it more convenient to the customers. It also reduces their cost in terms of office staff and office building. It has been observed that automated and IT enabled service sectors reduces cost effectively. Through the use of internet and mobile phones financial service sectors are in direct touch with their customers and with adequate databases it will be easier for service sectors to manage customer relationships. For example, through emails or SMS

## 2.40 Information Systems Control and Audit

---

the customers can be made aware of launch of new policies; they can be informed on time the day of maturity of their policies etc.

In traditional banking system, the customer has to visit bank branch to deposit or withdraw money and get updated passbook from the respective counter. With the advancement of IT, the customer can do transactions by using internet banking, phone banking and the deposit or withdraw of money can also be done by using ATM (Automatic Teller Machine), internet or mobile banking. Banks also offers most of direct banking services free of charge to the customers. The customers can check the status of their accounts in different banks by using of direct banking. Retail banking in India has assured great importance recently with a number of retail banking products available to the consumer like real time account status, transfer of funds, bill payments and so on e.g. HDFC, SBI and ICICI are the banks in India that offer real time online transactions etc.

- (iii) **Wholesaling and Retailing** – A visit to any large store will show that IT has become a vital part of retailing. Retail business uses IT to carry out basic functions including till systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information and accounting. The laser scanners used in most grocery supermarkets and superstores to read product bar codes are among the most distinctive examples of modern computer technology. By using internet or mobile phones retailers can collect and exchange data between stores, distribution centers, suppliers and head offices.

IT can be used in wholesale for supply chain logistics management, planning, space management, purchasing, re-ordering, and analysis of promotions. Data mining and data warehousing applications helps in the analysis of market baskets, customer profiles and sales trends. E-commerce among partners (suppliers, wholesalers, retailers, distributors) helps in carrying out transactions.

**Public sectors** – It includes services provided by the government mainly hospitals, police stations, universities etc. IT/IS can be used here, to keep records of the cases, respective people involved it, other related documents and can consult the existing data warehouse or databases to take appropriate actions. For example, IS like ERP can be implemented in a university to keep record of its employees in terms of their designation, leaves availed, department, achievements that can be used further in analyzing their performance. Owing to application of IT and IS, it becomes easy to file FIR of a case without going to police station personally and also important documents like passports can be made easily by applying online.

- (iv) **Others** – IT is efficiently used in entertainment industry (games, picture collection etc.), agriculture industry (information is just a mouse click away to the farmers), Tour industry (railway, hotel and airline reservations) and consultancy etc.

Thus, we can say that IT has changed the working style of business world drastically and make it simpler day-by-day with its advancement.

## 2.6 Overview of Underlying IT Technologies

Now day's business uses IT to carry out basic functions including systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information, decision making, accounting etc. Here, we discuss some of the IT tools crucial for business growth.

(i) **Business Website** – By having a website, enterprise/business becomes reachable to large amount of customers. In addition, it can also be used in an advertisement, which is cost effective and in customer relationship management. These websites can be designed by using HTML, XML, ASP.NET etc.

(ii) **Internet and Intranet** – It is the best source of communication. Time and space is no more obstacles for conducting meeting of people working in a team from multiple locations, or with different vendors and companies.

Intranet is system that permits the electronic exchange of business data within an organization, mostly between managers and senior staff. E-commerce among partners (suppliers, wholesalers, retailers, distributors) using intranets, e-mail etc. provides new platform to the business world for conducting business in a faster and easier way. E-commerce provides business to business, business to customer, customer to customer and customer to business communication with a click of mouse.

(iii) **Software and Packages** – DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making that can boost the business in the competitive world. e.g. by having information of buying habits of customer, sales of product; marketing strategy can be built quickly and effectively with the use of data mining tools and Knowledge Discovery In Database (KDD). These can be used in Supply chain logistics, including planning, purchasing, replenishment, logistics, and space management.

### Enterprise Resource Planning (ERP) Packages

Now, progressively firms are replacing legacy systems with newer client/server based solutions. Data warehousing, data mining tools and knowledge discovery applications for analysis of market baskets, customer profiles and sales trends can be used in retailing. 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. ERP can be defined as a system, which 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. The objective of ERP is to provide support for adopting best business practices; to implement these practices with a view towards enhancing productivity and to empower the customers and suppliers to modify the implemented business processes to suit their needs.

## 2.42 Information Systems Control and Audit

---

An ERP System is a multi module software system that integrates all business process and functions of the entire Enterprise into a single software system, using a single integrated database. Each module is intended to collect, process, and store data of a functional area of the organization and to integrate with related processes. For example, a module may be designed to process purchasing transactions and record all data about purchase orders. This module must integrate with accounts payable and inventory, since the vendor must be paid and inventory increased as the purchased goods arrive. Each of the software modules of an ERP system automates business activities of a functional area within an organization. Information is updated instantly using the same database and each functional area can easily share information with other areas of the organization as data is input once and processed as required and also linked to all related processes and made available for users as required. For example, when customer order is entered in an ERP system, a customer representative can have access to information such as the production schedules, and shipping schedules. Therefore, employee can answer any questions that the customer may ask, such as the following:

- Is the product in stock?
- If not, when will it be produced or restocked?
- How soon can it be shipped?
- When did we place the last order for this item?

To answer these questions, the customer service representative must have access to inventory information, production planning and scheduling information, shipping scheduling information, and customer history information. All of these functional areas have data stored in a single, shared database to enable the necessary integration.

Data Mining (DM) can be applied in database analysis and decision support i.e. market analysis and management by finding patterns that are helpful in target marketing, customer relation management, market basket analysis, cross selling, market segmentation, risk analysis, customer retention, improved underwriting, quality control, competitive analysis and fraud detection. Other applications of DM are:

1. text mining,
2. web analysis,
3. customer profiling - it can list out what types of customers buy what products by using clustering or classification,
4. identifying customer requirements- it can identify the most demanding and appropriate products for different customers, and also can list the factors that will attract new customers by using prediction etc.,
5. provide summary information i.e. various multidimensional summary reports and statistical summary information,
6. finance planning and asset evaluation

7. cross-sectional and time series analysis, and
8. resource planning- it can summarize and compare the resources and spending.

**(iv) Business Intelligence (BI)** refers to applications and technologies that are used to collect and provide access and analyze data and information about companies operations. BI software consists of range of tools. Some BI applications are used to analyze performance or internal operations e.g. EIS (executive information system), business planning, finance and budgeting tools.

While others are used to store and analyze data e.g. Data mining, data warehouses, Decision support system etc. Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools. A complete Business Intelligence provides consistent and standard information essential in enterprise operations.

**(v) Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc.-** Webcam, microphone etc. are used in conducting long distance meeting. Use of computer systems, printer; scanner increases accuracy; reduce processing times; enable decisions to be made more quickly and speed up customer service. For example, one can charge accurate prices and eliminates the need to apply price labels to individual items by the use of scanning system.

## 2.7 Summary

Although information systems has set high hopes to companies for their growth as it reduces processing speed and helps in cutting cost, but in reality, most of the research studies show that there is a remarkable gap between its capabilities and the business-related demands that senior management is placing on it. Secondly, Information system is not simply one time investment but needs continuous updating.

This Chapter has provided an overview of different types of information system, the importance of information systems in an IT environment and how information is generated. Further, the information needs of different levels of managements differ and how these information systems have to be organized to process and present this, have been discussed. Use of technology impacts how enterprise can use information for not only data processing but for competitive and strategic advantage. Source of the enabling technologies with examples of business applications have also been briefly discussed.

## Protection of Information Systems

### Learning Objectives

- To understand the need for Protection of Information Systems;
- To know Information Security Policies, Procedures, related Standards and Guidelines;
- To understand the term 'Controls';
- To know about various types of Controls - IT General Controls, Logical Access Controls & Application Controls, Technologies and Security Management Features;
- To discuss the role of technology in Control Monitoring and Segregation of Duties; and
- To discuss Cyber Frauds.

### Task Statements

- To understand the need of Information Security;
- To evaluate the Security Policy and its Components;
- To identify the Significant Security Aspects and Organization' need to look into it;
- To perform detailed analysis of the Controls that an Organization has put in place;
- To identify the nature of Controls put in place; and
- To identify the possibilities of Frauds relating to technology.

### Knowledge Statements

- To know Information Security and its related concepts;
- To know various components of Information Security Policy;
- To know different controls and their related aspects; and
- To know various frauds that may hamper an organisation due to lack of controls.

### 3.1 Introduction

In the computerized information systems, most of the business processes are automated. Organizations are increasingly relying on Information Technology (IT) for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and generated need for reengineered business processes. IT



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 assume that the information required by the business managers is available all the time; it is accurate, it is complete 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. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to information security threats than ever before. The Denial of Service (DoS) attacks on the websites of yahoo.com, amazon.com and lots of other web sites is a significant case. Those websites were down for several hours to a few days jeopardizing the business of those organizations. The virus threats are also in real. The horror stories of 'Melissa' and 'I love you' viruses are fresh in the minds of the IT professionals of those organizations, which were affected by them. Further, the hacking and cracking on the Internet is a real threat to virtual organizations, which are vulnerable to information theft and manipulations.

### 3.2 Need for Protection of Information Systems

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. 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 processing 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.

Information security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information.

### 3.3 Information Systems Control and Audit

---

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 (fire, flood), 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.) can potentially result in a loss of management control and oversight. 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.

### 3.3 Information System Security

Information security refers 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 of the organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc., which is not understood well by many organizations. In organizations, where a security breach has been experienced, the effectiveness of information security policy and procedures has to be reassessed.

This concept of information 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 and logical measures.

**Information Security Objective:** The objective of information system security is “the protection of the interests of those relying on information, and protect 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; and
- **Availability** : Prevention of the unauthorized withholding of information.

The relative priority and significance of Confidentiality, Integrity and Availability (CIA) vary according to the data within the information system and the business context in which it is used.

### 3.3.1 What Information is Sensitive?

The following examples highlight some of the factors, necessary for an organization to succeed. The common aspect in each case is the critical information that each organization generates.

- **Strategic Plans:** Most of the organizations readily acknowledge that strategic plans are crucial to the success of a company. But many of them 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 test marketing 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 is that the company lost several million, rupees as its product sales faltered.

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 competitor. 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 many 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, precise salary information can provide a competitive edge. This information if available can help competitive enterprises to understand and re-configure their salary structure accordingly. Similarly, availability of information about product pricing may also be used by competitive enterprises to price its products, competitively. When competitors' costs are lower, they can either under-price the market or increase prices. In either case, the damage to an organization may be significant.

## 3.4 Information Security Policy

An **Information Security Policy** is the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, a information security policy is a document that describes an organization's information security controls and activities. The policy does not specify

### 3.5 Information Systems Control and Audit

---

technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business.

An Information Security Policy is the essential foundation for an effective and comprehensive information security program. It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems. Information Security policy invariably includes rules intended to:

- Preserve and protect information from any unauthorized modification, access or disclosure;
- Limit or eliminate potential legal liability from employees or third parties; and
- Prevent waste or inappropriate use of the resources of an organization.

An information security policy should be in written form. It provides instructions to employees about 'what kinds of behaviour or resource usage are required and acceptable', and about 'what is unacceptable'. An information security policy also provides direction to all employees about how to protect organization's information assets, and instructions regarding acceptable (and unacceptable) practices and behavior.

#### 3.4.1 Tools to Implement Policy: Standards, Guidelines, and Procedures

As policy is in the form of a broad general statement, organizations also develop standards, guidelines, and procedures that offer users, managers and others a clearer approach to implementing policy and meeting organizational goals.

Standards specify technologies and methodologies to be used to secure systems. Guidelines help in smooth implementation of information security policy. Procedures are more detailed steps to be followed to accomplish particular security related tasks. Standards, guidelines, and procedures should be promulgated throughout an organization through handbooks or manuals. Organizational standards specify uniform use of specific technologies across the organization. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are compulsory within an organization. Guidelines assist users, systems personnel, and others in effectively securing their systems. Guidelines are often used to ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

Procedures normally assist in implementing applicable information security Policy. These are detailed steps to be followed by users, system operations personnel, and others to accomplish a particular task (e.g., preparing new user accounts and assigning appropriate privileges). Some organizations issue overall computer security manuals, regulations, handbooks, or similar documents.

An information Security policy addresses many issues such as confidentiality, 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.

### 3.4.2 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 organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities; and
- 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 of the employees 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.

### 3.4.3 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.

### 3.4.4 Information Security Policies and their Hierarchy

**Information Security Policy** – This policy provides a definition of Information Security, its overall objective and the importance that applies to all users. Various types of information security policies are:

- ◆ **User Security Policies** – These include User Security Policy and Acceptable Usage Policy.

### 3.7 Information Systems Control and Audit

---

- **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, Internet services and other IT resources.
- ◆ **Organization Security Policies** – These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.
  - **Organizational Information Security Policy** – This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, 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 the 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. 3.4.1.

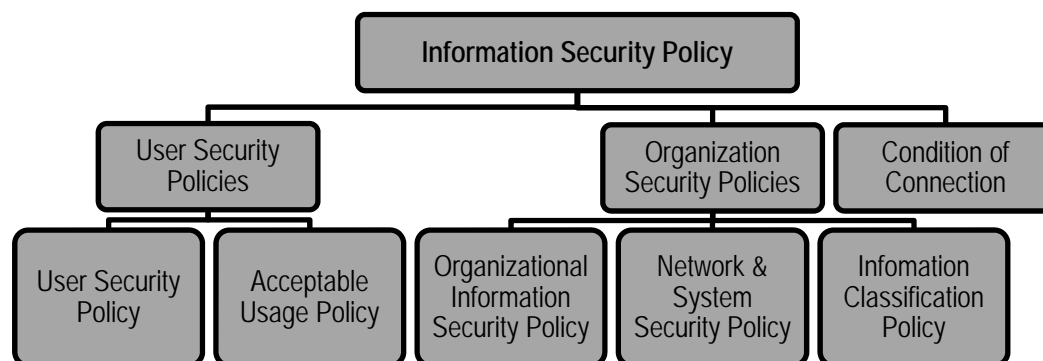


Fig 3.4.1: The Hierarchy of Information Security Policies

#### 3.4.5 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; and
- Monitoring and Auditing Requirements.

### 3.5 Information Systems Controls

The increasing use of IT in organizations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business processes of an enterprise and should have 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 to achieve business objectives. 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, 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.

#### 3.5.1 Need for Controls in Information Systems

Technology has impacted what can be done in business in terms of information 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. IT 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 data centre. In the past, the financial information would have been spread throughout the organisation in many filing cabinets. If a poorly controlled computer system is 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.

Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization. The goals to reduce the probability of organizational costs of data loss, computer loss, computer abuse, incorrect decision making

### 3.9 Information Systems Control and Audit

---

and to maintain the privacy; an organization's management must set up a system of internal controls. Safeguarding assets to maintain accurate data readily available and its integrity to achieve system effectiveness and efficiency is a significant control process.

A well designed information system should have controls built in for all its sensitive or critical sections. For example, the general procedure to ensure that adequate safeguards over access to assets and facilities can be translated into an IS-related set of control procedures, covering access safeguards over computer programs, data and any related equipment. IS control procedure may include:

- Strategy and direction,
- General Organization and Management,
- Access to IT resources, including data and programs,
- System development methodologies and change control,
- Operation procedures,
- System Programming and technical support functions,
- Quality Assurance Procedures,
- Physical Access Controls,
- BCP and DRP,
- Network and Communication,
- Database Administration, and
- Protective and detective mechanisms against internal and external attacks.

#### 3.5.2 Objectives of Controls

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, 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.

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; and
- Inefficient activity in procedures, processing and comparison.

Some of the critical control lacking in a computerized environment are:

- Lack of management understanding of IS risks and related controls;



- Absence or inadequate IS control framework;
- Absence of 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; and
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

The control objectives serve two main purposes:

- Outline the policies of the organization as laid down by the management; and
- A benchmark for evaluating whether control objectives are met.

### 3.5.3 Components of Internal Controls

In a computerised environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if an organization's management sets up a system of internal controls. Internal controls 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 way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that 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 records. 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. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

### 3.5.4 Impact of Technology on Internal Controls

These are discussed as follows:

- **Competent and Trustworthy Personnel:** *Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.*
- **Segregation of Duties:** *In a manual system, during the processing of a transaction, there are split between different people, such that one person does not process a transaction right from start to finish. 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. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT 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.*
- **Authorization Procedures:** *In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: 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).*
- **Adequate Documents and Records:** *In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trace the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.*
- **Physical Control over Assets and Records:** *Physical control over access and records is critical in both manual systems and computer systems. In the manual systems, protection from unauthorised access was 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 can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster. The nature and types of control available have changed to address these new risks.*

- **Adequate Management Supervision:** *In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried out remotely. The Management's supervision and review helps to deter and detect both errors and fraud.*
- **Independent Checks on Performance:** *In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.*
- **Comparing Recorded Accountability with Assets:** *Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a manual system, independent staff prepares the basic data used for comparison purposes. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.*
- **Delegation of Authority and Responsibility:** *A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.*

### 3.6 Classification of Information Systems Controls

Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on information systems on different basis. These categories have been represented in the Fig. 3.6.1:

#### 3.6.1 Classification on the basis of "Objective of Controls"

The controls can be classified as under:

- (A) **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 as follows:
- A clear-cut understanding about the vulnerabilities of the asset;

### 3.13 Information Systems Control and Audit

---

- Understanding probable threats; and
- Provision of necessary controls for probable threats from materializing.

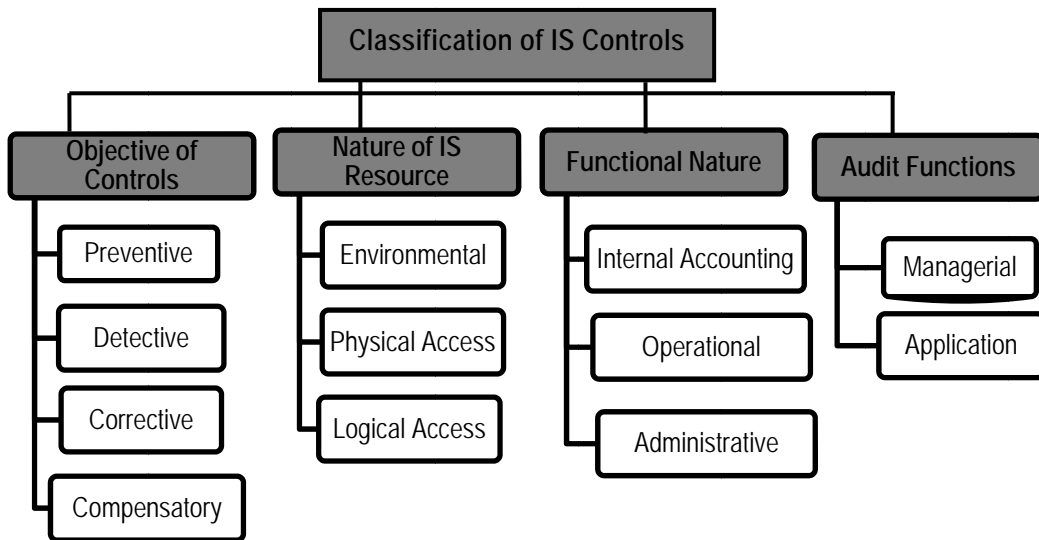


Fig. 3.6.1: Categories of Controls

As discussed earlier, any control can be implemented in both manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Examples of preventive controls are given as follows:

- 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., and
- Passwords.

The above list contains both of manual and computerized, preventive controls. The following Table 3.6.1 shows how the same purpose is achieved by using manual and computerized controls.

**Table 3.6.1: Preventive 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.

(B) **Detective Controls:** 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 given 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; and
- Surprise checks by supervisor.

Examples of detective controls include:

- Hash totals,
- Check points in production jobs,
- Echo control in telecommunications,
- 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, and
- Monitoring expenditures against budgeted amount.

### 3.15 Information Systems Control and Audit

---

(C) **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 (BCP) is considered to be a corrective control. The main characteristics of the corrective controls are:

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing Remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying the processing systems to minimize future occurrences of the incidents.

Examples of Corrective Controls are given as follows:

- Contingency planning,
- Backup procedure,
- Rerun procedures,
- Change input value to an application system, and
  - Investigate budget variance and report violations.

(D) **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, but reduce the probability of loss to the assets. Such measures are called compensatory controls.

#### 3.6.2 Classification on the basis of “Nature of Information System Resources”

These are given as follows:

(A) **Environmental Controls:** These are the controls relating to IT environment such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc. This section deals with the external factors in the Information System and preventive measures to overcome these conflicts.

(i) **Environmental Issues and Exposures:** Environmental exposures are primarily due to elements of nature. However, with proper controls, exposures can be reduced. Common occurrences are Fire, Natural disasters-earthquake, volcano, hurricane, tornado, Power spike, Air conditioning failure, 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, and 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 from dust, smoke and other particulate matter?

From the perspective of environmental exposures and controls, Information systems resources may be categorized as follows (with the primarily focus on facilities):

- **Hardware and Media:** Includes Computing Equipment, Communication equipment, and Storage Media.
- **Information Systems Supporting Infrastructure or Facilities:** This typically includes the following:
  - Physical Premises like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities, Staging Room, and Storage Areas,
  - Communication Closets,
  - Cabling ducts,
  - Power Source, and
  - Heating, Ventilation and Air Conditioning (HVAC).
- **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.
- **Supplies:** The third party maintenance procedures viz. 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.
- **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.

(ii) Controls for Environmental Exposures

These are given as follows:

- **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 initiated 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 in to zones 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 it is usually one of the following:

- **Dry-Pipe sprinkling systems:** These 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:** These 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,

- **Halon:** 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 in case of false alarm. The drawback is, since halon adversely affects the ozone layer, its usage is banned; alternative to Halon is effective.
- **Strategically Locating the Computer Room:** To reduce the risk of flooding, the computer room should not be located in the basement or ground floor of a multi-storey building. Studies reveal that the computer room located in the top floors is 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 three 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 System (UPS).
- **Uninterruptible Power System (UPS)/Generator:** A UPS system consists of a battery or gasoline powered generator that interfaces between the main electrical power entering the facility and the electrical power supplied to 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 battery to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to permit an orderly computer shutdown.
- **Power Leads from Two Substations:** Electrical power lines that are exposed to many environmental dangers such as waters fire, lightning, cutting due to

### 3.19 Information Systems Control and Audit

---

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 arise a necessity of immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations 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 floor in the computer room.
- **Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility:** These activities 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 proof.
- **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. In all circumstances saving human life should be given paramount importance.

**(B) Physical Access Controls:** These are the 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, CCTV monitoring etc.

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outside. 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 supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals. 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 zero visibility.

This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths. In addition, the section emphasizes on

physical access issues and exposures along with appropriate physical access controls. Afterwards, various access control mechanisms are also discussed.

**(i) Physical Access Issues and Exposures**

The following points elaborate 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,
- Public disclosure of sensitive information, and
- Unauthorized 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 for their termination,
- On strike, and
- Threatened by disciplinary action or dismissal.

Exposures to confidential matters may be in form the unaware, accidental or anonymous persons, although the greatest impact may be from those with malicious intent. Other 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?

### 3.21 Information Systems Control and Audit

---

The facilities that need to be protected from the auditor's perspective are as follows:

- Communication channels,
- Computer room,
- Control units and front-end processors,
- Dedicated telephones/telephone lines,
- Disposal sites,
- Input/Output devices,
- Local area networks,
- 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, and
- 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 Auditor has to confirm whether similar controls exist within service providers or other third parties.

#### (ii) Controls for Physical Access Exposures

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 should be explicit. Some of the more common access control techniques are discussed categorically as follows:

(a) **Locks on Doors:** These are given as follows:

- **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, 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.

- **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 reader to gain access in these systems. The reader device upon reading the special code that is internally stored within the card activates the door locking mechanism.

The following are 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:** These are discussed below:

- **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/her entry will be matched with the PIN number available in the security database.
- **Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.

### 3.23 Information Systems Control and Audit

---

- **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.
- (c) **Logging on Facilities:** These are given as under:
  - **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 fronts - 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 allowing entry inside the company.
  - **Electronic Logging:** This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted.
- (d) **Other means of Controlling Physical Access:** Other important means of controlling physical access are given as follows:
  - **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.
  - **Security Guards:** Extra security can be provided by appointing guards aided with CCTV feeds. 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 one person permitted in the holding area.
  - **Non-exposure of Sensitive Facilities:** There should be no explicit indication such as presence of windows of 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 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.
- (C) **Logical Access Controls:** These are the 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.

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 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.

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.

(i) Logical Access Paths

These are given as follows:

- (a) **Online Terminals** - To access an online terminal, a user has to provide a valid login-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.

- (b) **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.

- (c) **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., 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.

(ii) 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 opportunities of access in an online system, is more; hence, the level of control for this system must be more complex, as shown in Fig. 3.6.1.

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/s. 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,
- Operating systems Password library,
- Procedure libraries,
- Spool queues,
- System software,
- Tape files,
- Telecommunication lines,
- Temporary disk files, and
- Utilities.

The aforementioned utilities should be properly secured to assure security to data.

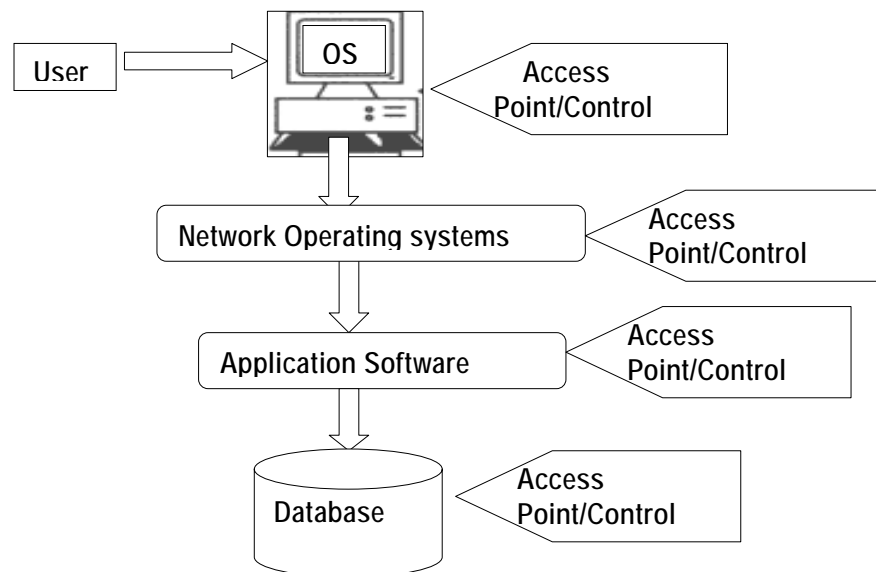


Fig. 3.6.1: Logical Access Paths in an Enterprise Information System

### (iii) Issues and Revelations related to Logical Access

Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures and computer crimes. These are given as follows:

(a) **Technical Exposures:** Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include the following:

- **Data Diddling:** Data diddling involves the change of data before or after 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 the data.
- **Bomb:** 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 low. Bombs are generally of two types, which are given as follows:
  - **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), likewise 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.
- **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.

- **Worm:** 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. 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.
  - **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.
  - **Salami Techniques:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, ₹ 21,23,456.39 becomes ₹ 21,23,456.40, while in the Salami technique the transaction amount ₹ 21,23,456.39 is truncated to either ₹ 21,23,456.30 or ₹ 21,23,456.00, depending on the logic.
  - **Trap Doors:** Trap doors 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 are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations. These are given as follows:

- **Financial Loss:** Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.
- **Legal Repercussions:** An organization has to adhere to many 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 have no proper security measures. The IS auditor should take legal counsel while reviewing the issues associated with computer security.

- **Loss of Credibility or Competitive Edge:** In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
  - **Blackmail/Industrial Espionage:** By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
  - **Disclosure of Confidential, Sensitive or Embarrassing Information:** These events can spoil the reputation of the organization. Legal or regulatory actions against the company may be also a result of disclosure.
  - **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.
  - **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 s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.
- (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 is 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; some of them are given as follows:
- **Data Leakage:** Data is a 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.
  - **Wire-tapping:** This involves spying on information being transmitted over telecommunication network as shown in the Fig. 3.6.2.

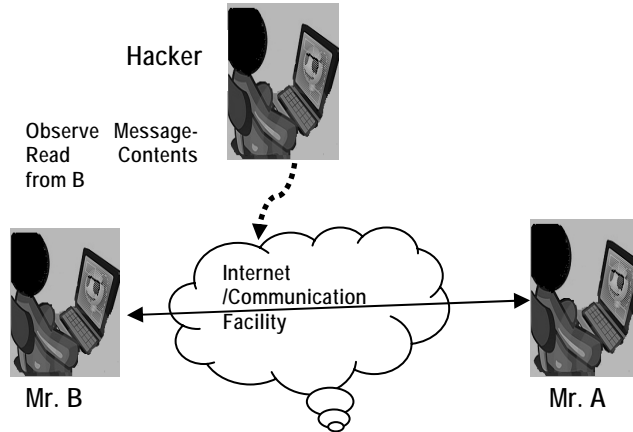


Fig. 3.6.2: Wire Tapping

- 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 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 as shown in the Fig. 3.6.3.

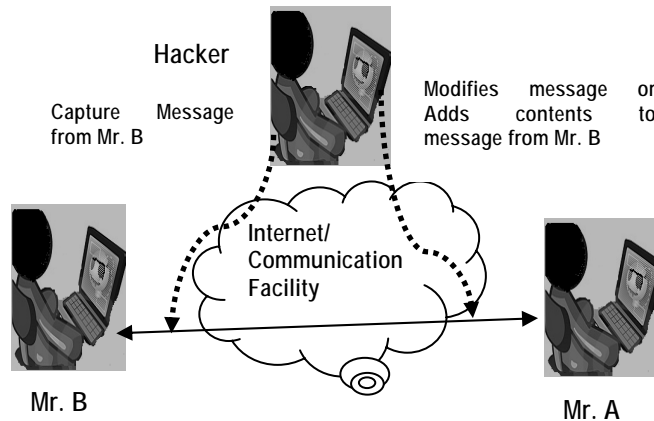


Fig. 3.6.3: Piggybacking

- Shutting 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. The security measure will function effectively if there are appropriate access controls on the 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, as shown in the Fig. 3.6.4.

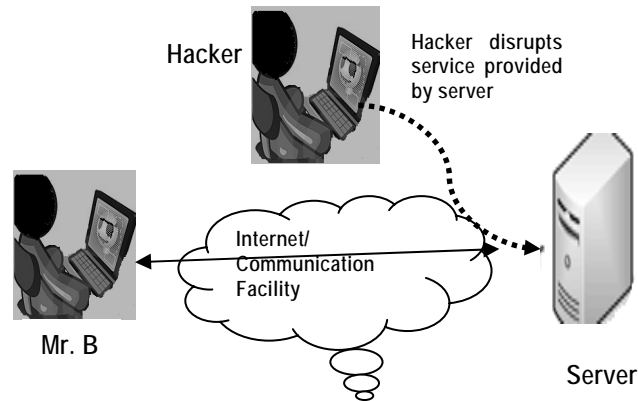


Fig. 3.6.4: Denial of Service

(d) Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- 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 user's access to 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.

**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. They are mainly:

- Hackers: Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally;
- Employees (authorized or unauthorized);
- IS Personnel: They have easiest access to computerized information since they come across information during discharging their duties. Segregation of duties and supervision help to reduce 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; and
- Accidental Ignorant – Violation done unknowingly.

**(iv) 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 do 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:

- Used by an application (Data at Process);
- Stored in some medium (Back up) (Data at Rest);
- 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. The details are given in the following Table 3.6.2:

Table 3.6.2: Logical Access Controls

<p><b>User Access Management</b></p>	<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. S/he 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>
<p><b>User Responsibilities</b></p>	<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> <p><b>Unattended user equipment</b> 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><b>Network Access Control</b></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> An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.</p> <p><b>Enforced path</b> Based on risk assessment, it is necessary to specify the exact path or</p>



	<p>route connecting the networks; e.g., internet access by employees will be routed through a firewall and proxy.</p> <p><b>Segregation of networks</b> 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</p> <p><b>Network connection and routing control</b> 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> The techniques of authentication and authorization policy should be implemented across the organization's network.</p>
<p><b>Operating System Access Control</b></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> 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> 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> 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> An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.</p> <p><b>Use of system utilities</b> System utilities are the programs that help to manage critical functions of the operating system e.g. 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> If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.</p>

	<p><b>Terminal time out</b> 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> 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>
<b>Application and Monitoring System Access Control</b>	<p><b>Information access restriction</b> 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, s/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> 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> <p><b>Event logging</b> 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> 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> 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 the network as per a standard time is mandatory.</p>
<b>Mobile Computing</b>	<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 the management to maintain information security.</p> <p><b>Mobile computing</b> Theft of data carried on the disk drives of portable computers is a high</p>

	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.
--	--

### 3.6.3 Classification on the basis of “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. These controls are given as follows:

- (i) **Internal Accounting Controls:** The Controls which are intended to safeguard the client’s assets and ensure the reliability of the financial records are called internal accounting controls.
- (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.

### 3.6.4 Classification on the basis of “Audit Functions”

*Auditors might choose to factor systems in several different ways. Auditors have found two ways to be especially useful when conducting information systems audits. These are discussed below:*

- (A) **Managerial Controls:** *In this part, we shall examine controls over the managerial controls that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis as discussed in Table 3.6.3.*

*Table 3.6.3: Types of Management Subsystem and their description*

<i>Management Subsystem</i>	<i>Description of Subsystem</i>
<i>Top Management</i>	<i>Top management must ensure that information systems function is well managed. It is responsible primarily for long – run policy decisions on how Information Systems will be used in the organization.</i>
<i>Information Systems Management</i>	<i>IS management has overall responsibility for the planning and control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.</i>
<i>Systems Development Management</i>	<i>Systems Development Management is responsible for the design, implementation, and maintenance of application systems.</i>

<i>Programming Management</i>	<i>It is responsible for programming new system; maintain old systems and providing general systems support software.</i>
<i>Data Administration</i>	<i>Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.</i>
<i>Quality Assurance Management</i>	<i>It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.</i>
<i>Security Administration</i>	<i>It is responsible for access controls and physical security over the information systems function.</i>
<i>Operations Management</i>	<i>It is responsible for planning and control of the day-to-day operations of information systems.</i>

- (B) **Application Controls:** These include the programmatic routines within the application program code. 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, legal and regulatory requirements. Any function or activity that works to ensure the processing accuracy of the application can be considered an application control. Necessary controls belonging to this category are discussed in separate headings.

The categories of Application controls are listed below in the Table 3.6.4.

Table 3.6.4: Types of Application Subsystem and their description

<i>Application Subsystem</i>	<i>Description of Subsystem</i>
<i>Boundary</i>	<i>Comprises the components that establish the interface between the user and the system.</i>
<i>Input</i>	<i>Comprises the components that capture, prepare, and enter commands and data into the system.</i>
<i>Communication</i>	<i>Comprises the components that transmit data among subsystems and systems.</i>
<i>Processing</i>	<i>Comprises the components that perform decision making, computation, classification, ordering, and summarization of data in the system.</i>
<i>Database</i>	<i>Comprises the components that define, add, access, modify, and delete data in the system.</i>
<i>Output</i>	<i>Comprises the components that retrieve and present data to users of the system.</i>

We shall study Managerial and Application Controls in detail now.

### 3.7 Managerial Controls and their Categories

*In this part, we shall examine controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.*

#### 3.7.1 Top Management and Information Systems Management Controls

*The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior manager must perform are as follows:*

- *Planning – determining the goals of the information systems function and the means of achieving these goals;*
- *Organizing – gathering, allocating, and coordinating the resources needed to accomplish the goals;*
- *Leading – motivating, guiding, and communicating with personnel; and*
- *Controlling – comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.*

*Top management must prepare two types of information systems plans for the information systems function: a Strategic plan and an Operational plan. The strategic Plan is the long-run plan covering, say, the next three to five years of operations whereas the Operational Plan is the short-plan covering, say, next one to three years of operations. Both the plans need to be reviewed regularly and updated as the need arises. The planning depends upon factors such as the importance of existing systems, the importance of proposed information systems, and the extent to which IT has been integrated into daily operations*

#### 3.7.2 Systems Development Management Controls

*Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. Three different types of audits may be conducted during system development process as discussed in the Table 3.7.1:*

*Table 3.7.1: Different types of Audit during System Development Process*

<i>Concurrent Audit</i>	<i>Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.</i>
<i>Post-implementation Audit</i>	<i>Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.</i>

<i>General Audit</i>	<i>Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements in systems effectiveness and efficiency.</i>
----------------------	---

### 3.7.3 Programming Management Controls

*Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. The program development life cycle comprises six major phases – Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases as shown in the Table 3.7.2. The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.*

*Table 3.7.2: Phases of Program Development Life Cycle*

<i>Phase</i>	<i>Controls</i>
<i>Planning</i>	<i>Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.</i>
<i>Design</i>	<i>A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.</i>
<i>Coding</i>	<i>Programmers must choose a module implementation and integration strategy (like Top-down, bottom-up and Threads approach), a coding strategy (that follows the precepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).</i>
<i>Testing</i>	<p><i>Three types of testing can be undertaken:</i></p> <ul style="list-style-type: none"> <li>• <i>Unit Testing – which focuses on individual program modules;</i></li> <li>• <i>Integration Testing – Which focuses in groups of program modules; and</i></li> <li>• <i>Whole-of-Program Testing – which focuses on whole program.</i></li> </ul> <p><i>These tests are to ensure that a developed or acquired program achieves its specified requirements.</i></p>
<i>Operation and Maintenance</i>	<p><i>Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used –</i></p> <p><i>Repair Maintenance – in which program errors are corrected;</i></p> <p><i>Adaptive Maintenance – in which the program is modified to meet changing user requirements; and</i></p> <p><i>Perfective Maintenance - in which the program is tuned to decrease the resource consumption.</i></p>

### 3.7.4 Data Resource Management Controls

Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed better users must be able to share data, data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed. Further it must be possible to modify data fairly easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

### 3.7.5 Quality Assurance Management Controls

Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work. Organizations are undertaking more ambitious information systems projects that require more stringent quality requirements and are becoming more concerned about their liabilities if they produce and sell defective software.

### 3.7.6 Security Management Controls

Information security administrators are responsible for ensuring that information systems assets are secure. Assets are secure when the expected losses that will occur over some time are at an acceptable level. Some of the major threats and to the security of information systems and their controls are as discussed in the Table 3.7.3:

Table 3.7.3: Major threats and their control measures

<i>Threat</i>	<i>Control</i>
<i>Fire</i>	<i>Well-designed, reliable fire-protection systems must be implemented.</i>
<i>Water</i>	<i>Facilities must be designed and sited to mitigate losses from water damage</i>
<i>Energy Variations</i>	<i>Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.</i>
<i>Structural Damage</i>	<i>Facilities must be designed to withstand structural damage.</i>
<i>Pollution</i>	<i>Regular cleaning of facilities and equipment should occur.</i>
<i>Unauthorized Intrusion</i>	<i>Physical access controls can be used.</i>
<i>Viruses and Worms</i>	<i>Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.</i>
<i>Misuse of software, data and services</i>	<i>Code of conduct to govern the actions of information systems employees.</i>
<i>Hackers</i>	<i>Strong, logical access controls to mitigate losses from the activities of hackers.</i>

### 3.7.7 Operations Management Controls

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions like Computer Operations, Communications Network Control, Data Preparation and Entry, Production control, File Library; Documentation and Program Library; Help Desk/Technical support; Capacity Planning and Performance Monitoring and Outsourced Operations. Operations management control must continuously monitor the performance of the hardware/software platform to ensure that systems are executing efficiently, an acceptable response time or turnaround time is being achieved, and an acceptable level of uptime is occurring.

## 3.8 Application Controls and their Categories

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/her job description and assigned responsibilities. S/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. Different Application Controls are as follows:

### 3.8.1 Boundary Controls

(i) **Boundary Controls:** The major controls of the boundary system are the access control mechanisms. Access controls mechanism links the authentic users to the authorized resources, they are permitted to access. The access control mechanism has three steps of identification, authentication and authorization with respect to the access control policy implemented as shown in the Fig. 3.8.1.

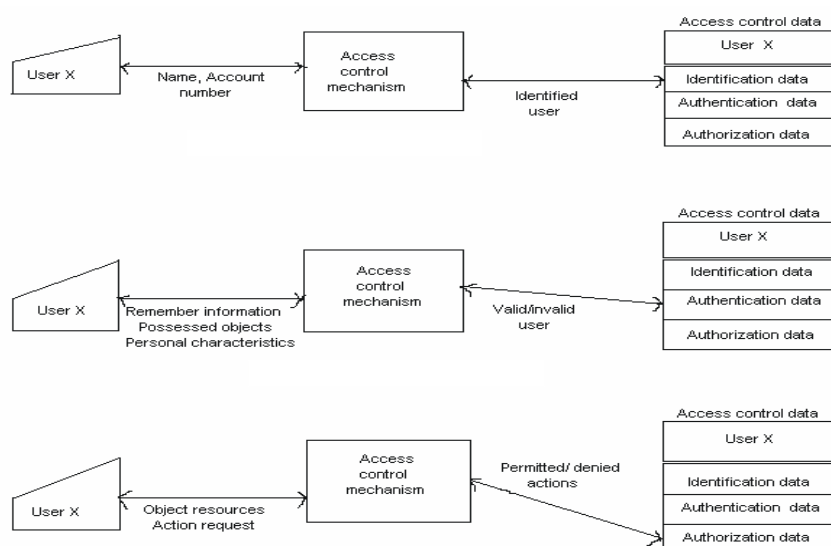


Fig. 3.8.1: Identification/Authentication /Authorization Process



The user can provide three factors of input information for the authentication process and gain access to his required resources. The three factors of information with respect to the corresponding input to the boundary control are summarized in the Table 3.8.1.

Table 3.8.1: Authentic Information

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.

Major Boundary Control techniques are given as follows:

- Cryptography:** It deals with programs for transforming data into cipher text 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. 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). A pictorial representation of the same is given in Fig. 3.8.2.

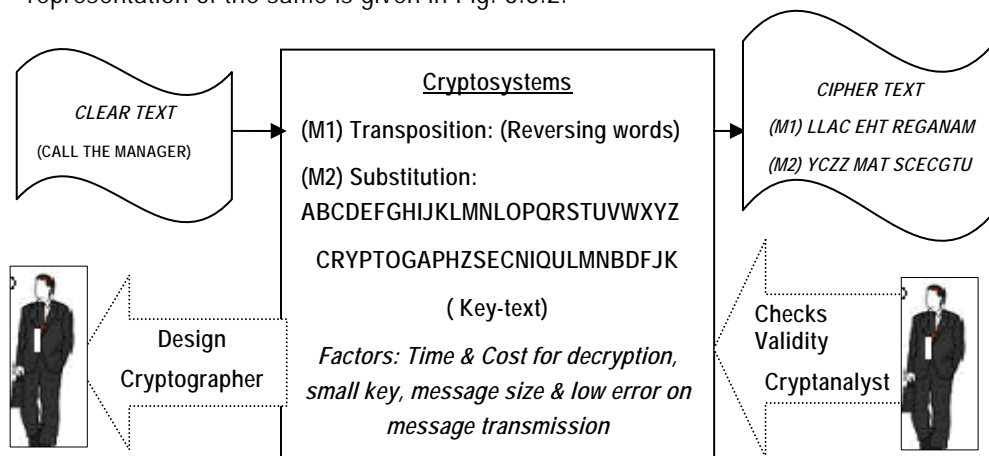


Fig. 3.8.2: Cryptography Techniques

- 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, hashing of passwords and number of entry attempts.
- Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user

### 3.43 Information Systems Control and Audit

---

identification details, or a customer selected number. Hence, a PIN may be 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 are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric Devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

#### 3.8.2 Input Controls

These 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.

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. Input controls are divided into the following broad classes:

Input controls are divided into the following broad classes:

- Source Document Control,
- Data Coding Controls
- Batch Controls, and
- Validation Controls.

The details of each aforementioned class are given as under:

**(a) Source Document Controls:** In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. If these documents were entered into the data processing stream along with a fictitious vendor's invoice, the system could process these documents as if a legitimate transaction had taken place. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

- **Use pre-numbered source documents:** Source documents should come pre-numbered from the printer with a unique sequential number on each document. Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.

- **Use source documents in sequence:** Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be kept under lock and key and access to source documents should be limited to authorized persons.
- **Periodically audit source documents:** Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

**(b) Data Coding Controls:** Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors, which are as discussed below:

- **Transcription Errors:** These fall into three classes:
  - Addition errors occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
  - Truncation errors occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
  - Substitution errors are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.
- **Transposition Errors:** There are two types of transposition errors.
  - Single transposition errors occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.
  - Multiple transposition errors occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

Any of these errors can cause serious problems in data processing if they go undetected. For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed. These simple errors can severely disrupt operations.

**(c) Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercised over the batch to prevent or detect errors or irregularities. Two types of batches occur:

- **Physical Controls:** These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.
- **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use

### 3.45 Information Systems Control and Audit

---

the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.

To identify errors or irregularities in either a physical or logical batch, three types of control totals can be calculated as shown in Table 3.8.2.

**Table 3.8.2 : Control Totals on Logical / Physical Batch**

Control Total Type	Explanation
Financial totals	Grand totals calculated for each field containing money amounts.
Hash totals	Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totaled.
Document/Record Counts	Grand totals for the number of documents in record in the batch.

In case of Physical Controls, these totals can be written on the batch cover sheet and keyed into the application system prior to the key entry of the transactions in the batch. The input program then computes the batch totals as the transactions are entered. When keying of all the transactions in the batch has been completed, it compares the computed total against the entered total and signals any discrepancy.

In case of logical batch, the person responsible for keying data must keep an independent record of transactions entered into the application system. Periodically, the batch totals calculated by the input program must then be compared against the batch totals calculated on the basis of these independent records.

**(d) Validation Controls:** Input validation controls are intended to detect errors in the transaction data before the data are processed. There are three levels of input validation controls:

- Field interrogation,
- Record interrogation, and
- File interrogation.

The details of the same are given as follows:

- **Field Interrogation:** It involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation. Various field checks used to ensure data integrity have been described below:
  - **Limit Check:** This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre-established limits has occurred.
  - **Picture Checks:** These check against entry into processing of incorrect/invalid characters.

- **Valid Code Checks:** Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.
- **Check Digit:** One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle.
- **Arithmetic Checks:** Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.  
**Example:** The discounted amount for ₹ 4,000 at 5% discounted may be computed twice by the following different ways:  
 $4,000 - 4,000 \times 5/100 = 3,800$  or  
 Next time again at  
 $(3800/(100-5))*100$ .
- **Cross Checks:** may be employed to verify fields appearing in different files to see that the result tally.
- **Record Interrogation:** These are discussed as follows:
  - **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?
  - **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
  - **Sequence Check:** If physical records follow a required order matching with logical records.
- **File Interrogation:** These are discussed as follows:
  - **Version Usage:** Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
  - **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.
  - **Data File Security:** Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.
  - **Before and after Image and Logging:** The application may provide for reporting of before and after images of transactions. These images combined with the logging of

### 3.47 Information Systems Control and Audit

---

events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.

- **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.
- **Parity Check:** When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

#### 3.8.3 Communication Controls

*Three major types of exposure arise in the communication subsystem:*

- *Transmission impairments can cause difference between the data sent and the data received;*
- *Data can be lost or corrupted through component failure; and*
- *A hostile party could seek to subvert data that is transmitted through the subsystem.*

*These controls discusses exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.*

*(a) **Physical Component Controls:** These controls incorporate features that mitigate the possible effects of exposures. The Table 3.8.1 below gives an overview of how physical components can affect communication subsystem reliability.*

*Table 3.8.1: Physical Components affecting reliability of Communication subsystem*

<u>Transmission Media</u>	<p><i>It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types:</i></p> <ul style="list-style-type: none"> <li>• <i>Guided/Bound Media in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber.</i></li> <li>• <i>In Unguided Media, the signals propagate via free-space emission like – satellite microwave, radio frequency and infrared.</i></li> </ul>
<u>Communication Lines</u>	<p><i>The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.</i></p>
<u>Modem</u>	<ul style="list-style-type: none"> <li>• <i>Increases the speed with which data can be transmitted over a</i></li> </ul>

	<p><i>communication line.</i></p> <ul style="list-style-type: none"> <li>• <i>Reduces the number of line errors that arise through distortion if they use a process called equalization.</i></li> <li>• <i>Reduces the number of line errors that arise through noise.</i></li> </ul>
<u>Port Protection Devices</u>	<ul style="list-style-type: none"> <li>• <i>Used to mitigate exposures associated with dial-up access to a computer system. The port-protection device performs various security functions to authenticate users.</i></li> </ul>
<u>Multiplexers and Concentrators</u>	<ul style="list-style-type: none"> <li>• <i>These allow the band width or capacity of a communication line to be used more effectively.</i></li> <li>• <i>These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.</i></li> </ul>

(b) Line Error Control: Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

- Error Detection: The errors can be detected by either using a loop (echo) check or building some form of redundancy into the message transmitted.
- Error Correction: When line errors have been detected, they must then be corrected using either forward error correcting codes or backward error correcting codes.

(c) Flow Controls: Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data. For example, a main frame can transmit data to a microcomputer terminal. The microcomputer can not display data on its screen at the same rate the data arrives from the main frame. Moreover, the microcomputer will have limited buffer space. Thus, it cannot continue to receive data from the mainframe and to store the data in its buffer pending display of the data on its screen. Flow controls will be used, therefore, to prevent the mainframe swamping the microcomputer and, as a result, data is lost.

(d) Link Controls: In WANs, line error control and flow control are important functions in the component that manages the link between two nodes in a network. The link management components mainly use two common protocols HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

(e) Topological Controls: A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes. Specifying the optimum topology for a network can be a problem of immense complexity.

- Local Area Network Topologies: Local Area Networks tend to have three characteristics: (1) they are privately owned networks; (2) they provide high-speed

communication among nodes; and (3) they are confined to limited geographic areas (for example, a single floor or building or locations within a few kilometers of each other). They are implemented using four basic types of topologies: (1) bus topology, (2) Tree topology, (3) Ring topology, and (4) Star topology. Hybrid topologies like the star-ring topology and the star-bus topology are also used.

- **Wide Area Network Topologies:** Wide Area Networks have the following characteristics:
  - they often encompass components that are owned by other parties (e.g. a telephone company);
  - they provide relatively low-speed communication among nodes; and
  - they span large geographic areas

With the exception of the bus topology, all other topologies that are used to implement LANs can also be used to implement WANs.

(f) **Channel Access Controls:** Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used. These techniques fall into two classes: Polling methods and Contention methods.

- **Polling:** Polling (non contention) techniques establish an order in which a node can gain access to channel capacity.
- **Contention Methods:** Using contention methods, nodes in a network must compete with each other to gain access to a channel. Each node is given immediate right of access to the channel. Whether the node can use the channel successfully, however, depends on the actions of other nodes connected to the channel.

(g) **Internetworking Controls:** Internetworking is the process of connecting two or more communication networks together to allow the users of one network to communicate with the users of other networks. The networks connected to each other might or might not employ the same underlying hardware-software platform.

Three types of devices are used to connect sub-networks in an internet as shown in Table 3.8.3.

Table 3.8.3: Internetworking Devices

<i>Device</i>	<i>Functions</i>
<b><u>Bridge</u></b>	A bridge connects similar local area networks (e.g. one token ring network to another token ring network).
<b><u>Router</u></b>	A router performs all the functions of a bridge. In addition, it can connect heterogeneous local area networks (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine



	<i>channel availability.)</i>
<u>Gateway</u>	<i>Gateways are the most complex of the three network connection devices. Their primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.</i>

### 3.8.4 Processing Controls

*The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are the Central Processor in which programs are executed, the real or virtual memory in which program instructions and data are stored, the operating system that manages system resources, and the application programs that execute instructions to achieve specific user requirements.*

*(i) Processor Controls: The processor has three components: (a) A Control unit, which fetches programs from memory and determines their type; (b) an Arithmetic and Logical Unit, which performs operations; and (c) Registers, that are used to store temporary results and control information. Four types of controls that can be used to reduce expected losses from errors and irregularities associated with Central processors are explained in the Table 3.8.4.*

*Table 3.8.4: Operating System Control*

<i>Control</i>	<i>Explanation</i>
<i>Error Detection and Correction</i>	<i>Occasionally, processors might malfunction. The causes could be design errors, manufacturing defects, damage, fatigue, electromagnetic interference, and ionizing radiation. Various types of error detection and correction strategies must be used.</i>
<i>Multiple Execution States</i>	<i>It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities, such as gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes.</i>
<i>Timing Controls</i>	<i>An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.</i>
<i>Component Replication</i>	<i>In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected. If processor failure is permanent in multicomputer or multiprocessor architectures, the system might reconfigure itself to isolate the failed processor.</i>

(ii) ***Real Memory Controls:*** This comprises the fixed amount of primary storage in which programs or data must reside for them to be executed or referenced by the central processor. Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

(iii) ***Virtual Memory Controls:*** Virtual Memory exists when the addressable storage space is larger than the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.

**Access Control Mechanisms:** An Access Control Mechanism is associated with identified, authorized users the resources they are allowed to access and action privileges. The mechanism processes the users request for Real time Memory and Virtual Memory resources in three steps:

- **Identification:** First and foremost, the users have to identify themselves.
- **Authentication:** Secondly, the users must authenticate themselves and the mechanism must authenticate itself. 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. Users may provide four factor of authentication information as described in Table 3.8.5.

**Table 3.8.5: Classes of Authentication**

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

- **Authorization:** Third, the users request for specific resources, their need for those resources and their areas of usage of these resources. There are two approaches to implementing the authorization module in an access control mechanism:

- a "ticket oriented approach", and
- 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 3.8.6 given below illustrates the authorization matrix in an access control mechanism.

**Table 3.8.6: Authorization Matrix**

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

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 major 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.

(iv) **Data Processing Controls:** These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Normally, the processing controls are enforced through 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. Various processing controls are given as follows:

- **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 ₹ 150,000 and the additional invoices for the period total ₹ 20,000 then the total sales value should be ₹ 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.

### 3.53 Information Systems Control and Audit

---

- **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/blank before inserting the field or record.
- **Exception Reports:** Exception reports are generated to identify errors in the data processed. Such exception reports give the transaction code and why a 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 the 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.

#### 3.8.5 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 update controls and report controls. Major update controls are given as follows:

- **Sequence Check between 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 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, and 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 (e.g. 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 reflects the errors to be corrected.

Major Report controls are given as follows:

- **Standing Data:** Application programs use many internal tables to perform various functions like 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 monitored 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 logs 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.

### 3.8.6 Output Controls

These 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 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. Various Output Controls are given as follows:

- **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, these should be logged and monitored; otherwise confidentiality/integrity of the data may 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, while the print operation is getting 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 should not be subject to unauthorized modifications.
- **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. 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 prevent 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 for reports that were generated and to whom these were distributed. Where users have to collect reports the user should be responsible for

### 3.55 Information Systems Control and Audit

---

timely collection of the report, especially if it is printed in a public area. A log should be maintained about reports that were printed and 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.

## 3.9 General Controls

Some of the general controls that are quite commonly used are derived and presented in Fig. 3.9.1.

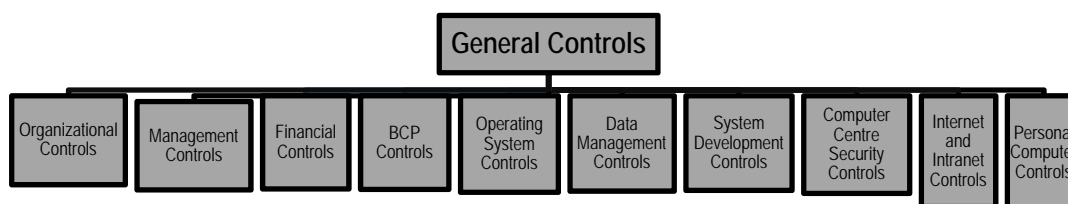


Fig. 3.9.1: General Control

### 3.9.1 Organizational Controls

These controls are concerned with the decision-making processes that lead to management authorization of transactions. In manual environment, the task may be segregated in the following manner:

- Segregate the task of transaction authorization from transaction processing;
- Segregate record keeping from asset custody; and
- Divide transaction-processing tasks among individuals.

In a Computer Based Information System (CBIS), as transaction initiation is a critical activity, it requires segregation of duties at authorization, processing and recording all aspects of a transaction. Segregation is done at the following functional levels, to adhere the following principles of internal controls:

- Segregating the maker / creator from checker;
- Segregating the asset record keeper from physical asset keeper; and
- Regular checking of effectiveness of internal controls.

To save from the compromises that may occur due to above, it is required that following must be done:

- Documentation is improved because the maintenance group requires documentation to perform its maintenance duties.

The programmer is denied the access to the production environment, to mitigate the programmed frauds.

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 the following:

- Reporting responsibility and authority of each function,
- Definition of responsibilities and objectives of each functions,
- Policies and procedures,
- Job descriptions, and
- Segregation of duties.

These are discussed as follows:

**(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; and
- Implementing activities and functions that support accomplishment of company's strategic plan.

**(ii) Policies, standards, procedures and practices:** Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. These are the standards and instructions that all IS personnel must follow when completing their assigned duties.

Procedures establish the instructions that individuals must follow to complete their daily assigned tasks. Mandating 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 from whom obtain the approvals are examples of procedures. Documented policies should exist in IS for:

- Use of IS resources,
- Physical security,
- Data security

### 3.57 Information Systems Control and Audit

---

- On-line security,
- Use of Information systems,
- 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:** Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts going undetected because the activities of one group or individual will serve as a check on the activities of the other. The irregularities are frauds due to various facts e.g.:

- Theft of assets like funds, IT equipment, the data and programs;
- Modification of the data leading to misstated and inaccurate financial statements; and
- Modification of programs in order to perpetrate irregularities like rounding down, salami etc.

The controls ensure that the threats and irregular acts minimize the potential damage from the actions of a person or persons. The organization structure and allied controls should be structured in a manner that ensures the highest level of separation of duties. The critical factors to be considered in segregation of duties in a computerized information system are:

- Nature of business operations;
- Managerial policy;
- Organization structure with job description; and
- IT resources deployed such as: Operating system, Networking, Database, Application software, Technical staff available, IT services provided in-house or outsourced, Centralized or decentralized IT operations.

This is a very 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;
- Systems analyst function from the programming function;
- Physical, data, and online security group(s) from the other IS functions; and
- IS Audit from business operations groups.

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, and
- Security audit.

There are various general guidelines, with reference to 'Segregation of Duties', which may be followed in addition with concepts like, the maker should not be the checker:

- Separate those, who can run live programs e.g. operations department, from those who can change programs e.g. programmers. This is required in order to ensure that unauthorized programs are prevented from running.
- Separate those, who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can input data e.g. data entry, from those, who can reconcile or approve data e.g. data authorization persons. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can test programs e.g. users, quality assurance and security, from those, who can develop programs e.g. application programmers. This is required in order to ensure that unauthorized programs cannot be allowed to run.

### 3.59 Information Systems Control and Audit

---

- Separate those, who can enter errors in a log e.g. data entry operator, who transfer the data to an error log, from those who can correct the errors like the end user departments. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorized data entry or data modification cannot take place.

#### 3.9.2 Management Controls

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and 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 organization. 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 organization to down; the responsibility still lies with the senior management.

The controls considerations while reviewing management controls in an IS system shall include:

- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
- **An IT Organization Structure:** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.
- **An IT Steering Committee:** The steering committee shall comprise of 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.

#### 3.9.3 Financial Controls

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:

- **Authorization:** This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.
- **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period, 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.

- **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.
- **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.
- **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.
- **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.
- **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
- **Supervisory review:** This refers to review of specific work by a supervisor but 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.

#### 3.9.4 BCP (Business Continuity Planning) Controls

These controls are related 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 impact on business in the event of a major disruption. The controls include Critical 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.

### 3.9.5 Operating System Controls

Operating System is the computer control program. It allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Operating system performs the following major tasks:

- **Scheduling Jobs:** They can determine the sequence in which jobs are executed, using priorities established.
  - **Managing Hardware and Software Resources:** They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
  - **Maintaining System Security:** They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
  - **Enabling Multiple User Resource Sharing:** They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
  - **Handling Interrupts:** An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation that does not require the CPU, such as input or output, or when the program exceeds some predetermined time limit.
  - **Maintaining Usage Records:** They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices. Such information is usually maintained for the purpose of charging users' departments for their use of the organization's computing resources.
- (a) **Control Objectives:** Operating Systems being one of most critical software of any computer need to work in a well controlled environment. Following are the major control objectives:
- Protect itself from user;
  - Protect user from each other;
  - Protect user from themselves;
  - The operating system must be protected from itself; and
  - The operating system must be protected from its environment.
- (b) **Operating System Security:** Operating system security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access', and 'what action they can take'. The following security components are found in secure operating system:
- **Log-in Procedure:** A log-in procedure is the first line of defense against unauthorized access. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid

users. If the system finds a match, then log-on attempt is authorized. If password or user-id is entered incorrectly, then after a specified number of wrong attempts, the system should lock the user from the system.

- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
  - **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compares his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.
  - **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.
- (c) **Remedy from destructive programs:** The following can be used as remedies from destructive programs like viruses, worms etc.:
- Purchase software from reputed vendor;
  - Examine all software before implementation;
  - Establish educational program for user awareness;
  - Install all new application on a standalone computer and thoroughly test them;
  - Make back up copy of key file; and
  - Always use updated anti-virus software.

### 3.9.6 Data Management Controls

These Controls fall in two categories:

- Access Control, and
  - Backup Control.
- (a) **Access Controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:
- User Access Controls through passwords, tokens and biometric Controls; and

### 3.63 Information Systems Control and Audit

---

- Data Encryption: Keeping the data in database in encrypted form.
- (b) **Back-up Controls:** Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases.

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are given as follows:

- **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.
- **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.
- **Logging changes to the data:** This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

Apart from database backup strategies as mentioned above, it is important to implement email and personal files backup policies. The policy can be like burning CDs with the folders and documents of importance periodically to more detailed and automated functions. The choice depends and varies with the size, nature and complexity of the situation. The restoration should be done for all backups at least twice a year.

#### 3.9.7 System Development Controls

System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities: The six activities discussed below deal with system development controls in IT setup. These are given as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.
- **User Specification Activities:** Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user

can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remains a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.

- **Technical Design Activities:** The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.
- **Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.
- **Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.

Program testing is time-consuming, the principal task being the creation of meaningful test data. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests. For example, if a program has undergone no maintenance changes since its implementation, the test results from the audit should be identical to the original test results. Having a basis for comparison, the auditor can thus quickly verify the integrity of the program code. On the other hand, if changes have occurred, the original test data can provide evidence regarding these changes. The auditor can thus focus attention upon those areas.

- **User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

The formal test and acceptance of the system should consider being the most important control over the SDLC. It is imperative that user acceptance be documented. Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability. Although discovering a major flaw at this juncture is costly, discovering the flaw during the production operations may be devastating.

#### 3.9.8 Computer Centre Security and Controls

These are of the following types:

- Physical Security,
- Software & Data Security, and
- Data Communication Security.

(a) **Physical Security:** The security required for computer system can be categorized as security from accidental breach and incidental breach. Accidental breach of security due to such natural calamities as fire, flood and earthquake etc. may cause total destruction of important data and information. Incidental or fraudulent modification or tampering of financial records maintained by the organization can cause considerable amount of money to be disbursed to fraudulent personnel. Similarly, unauthorized access to secret records of the organization can cause leakage of vital information. Hence, there is a great need for physical security of the computer system. Physical security includes arrangements for:

- fire detection and fire suppression systems,
- security from water damage,
- safeguards from power variation, and
- pollution and unauthorized intrusion.

These are discussed as follows:

- **Fire Damage:** It is a major threat to the physical security of a computer installation. Some of the major features of a well-designed fire protection system are given below:
  - Both automatic and manual fire alarms are placed at strategic locations.
  - A control panel may be installed which shows where in the location an automatic or manual alarm has been triggered.
  - Besides the control panel, master switches may be installed for power and automatic fire suppression system.
  - Manual fire extinguishers can be placed at strategic locations.
  - Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
  - All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are: Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
  - Less Wood and plastic should be in computer rooms.



- **Water Damage:** Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc. Some of the major ways of protecting the installation against water damage are as follows:
  - Wherever possible have waterproof ceilings, walls and floors;
  - Ensure an adequate positive drainage system exists;
  - Install alarms at strategic points within the installation;
  - In flood areas have the installation above the upper floors but not at the top floor;
  - Use a gas based fire suppression system;
  - Water proofing; and
  - Water leakage Alarms.
- **Power Supply Variation:** Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power. UPS Battery back-up can be provided in case a temporary loss of power occurs. A generator is needed for sustained losses in power for extended period.
- **Pollution Damage:** The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors. Due consideration should be given for dust free environment in the computer room. Regular cleaning of walls, floors and equipment etc. is essential. Only such materials and finishing may be used inside the room, which enables it to remain dust free. These are:
  - air conditions,
  - dust protection, and
  - regular cleaning.
- **Unauthorized Intrusion:** Unauthorized intrusion takes two forms. First, the intruder by physically entering the room may steal assets or carry out sabotage. Alternatively, the intruder may eavesdrop on the installation by wire tapping, installing an electronic bug or using a receiver that picks up electro-magnetic signals. Physical entry may be restricted to the computer room by various means. A badge system may be used to identify the status of personnel inside the computer room. Various devices are available to detect the presence of bugs by the intruder; these are:
  - Physically or Electronically logging,
  - Guard, dogs,
  - Entry in computer area restricted,

### 3.67 Information Systems Control and Audit

---

- Log books,
  - Alarms,
  - Preventing wire tapping,
  - Physical Intrusion detectors, and
  - Security of Documents, data & storage media.
- (b) **Software & Data Security:** In today's business world, trade is through networks & has spread over geographical area, so security is must. Following are some of the examples of requirements:
- Authorization of persons to use data,
  - Passwords & PINs,
  - Monitoring after office hours activity,
  - Segregation, check & control over critical information,
  - Frequent audits,
  - Screening and background checks before recruitment,
  - Encryption of data:- Viewing & recognition of data only by PINs & passwords (Like P & L & B/S viewing),
  - Security software,
  - Management checks,
  - Back up of data/information, and
  - Antivirus software.
- (c) **Data Communication Security:** This is another important aspect to be covered. This can be implemented through the following controls:
- Audit trails of crucial network activities,
  - Sign on user identifier,
  - Passwords to gain access,
  - Terminal locks,
  - Sender & receiver authentications,
  - Check over access from unauthorized terminals,
  - Encryption of data / information,
  - Proper network administration,
  - Hardware & system software built in control,
  - Use of approved networks protocols,

- Network administrations, and
- Internally coded device identifier.

### 3.9.9 Internet and Intranet Controls

(a) Major exposures in the communication sub-system including Internet and Intranet, which are given as follows:

- **Component Failure:** Data may be lost or corrupted through component failure. The primary components in the communication sub-systems are given as follows:
  - Communication lines viz. twisted pair, coaxial cables, fiber optics, microwave and satellite etc.
  - Hardware – ports, modems, multiplexers, switches and concentrators etc.
  - Software – Packet switching software, polling software, data compression software etc.
  - Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.
- **Subversive Threats:** An intruder attempts to violate the integrity of some components in the sub-system. An intruder attempts to violate the integrity of some components in the sub-system by:
  - **Invasive tap:** By installing it on communication line, s/he may read and modify data.
  - **Inductive tap:** It monitors electromagnetic transmissions and allows the data to be read only.
  - **Denial of Service:** When a user establishes a connection on the Internet through TCP/IP, a three way handshake takes place between Synchronize (SYN) packets, SYN ACK (Acknowledgement) packets and ACK packets. Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate requests are prevented from access. This is known as Connection Flooding.

Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways.

#### (b) Controls for Subversive Threats

- **Firewall:** Organizations connected to the Internet and Intranet often implements an electronic firewall to insulate their network from intrude. A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall. Only authorized traffic between the organization and the outside is allowed to pass through the firewall. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's

### 3.69 Information Systems Control and Audit

---

network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.

- **Encryption:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key. The more bits in the key, the stronger are the encryption algorithms. Two general approaches are used for encryption viz. private key and public key encryption.
- **Recording of Transaction Log:** An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
- **Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call-back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.

#### 3.9.10 Personal Computers Controls

Related risks are given as follows:

- Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
- Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.
- PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
- Segregation of duty is not possible, owing to limited number of staff.
- Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
- The operating staff may not be adequately trained.
- Weak access control: Most of the log-on procedures become active only at the booting of the computer from the hard drive.

The Security Measures that could be exercised to overcome these aforementioned risks are given as follows:

- Physically locking the system;
- Proper logging of equipment shifting must be done;
- Centralized purchase of hardware and software;
- Standards set for developing, testing and documenting;
- Uses of antimalware software;
- The use of personal computer and their peripheral must have controls; and
- Use of disc locks that prevent unauthorized access to the floppy disk or pen drive of a computer.

### 3.10 Controls over Data Integrity and Security

Before discussing the controls relating to Data Integrity, it is important to understand the concept of information classified. 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:

- **Top Secret:** Highly sensitive internal information 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 should be the highest possible.
- **Highly Confidential:** 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 banks, 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.
- **Proprietary:** 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 should be high.
- **Internal Use only:** 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 should controlled but normal.

### 3.71 Information Systems Control and Audit

---

- **Public Documents:** Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should minimal.

#### 3.10.1 Data Integrity

The organization has to decide about various data integrity controls implementation. The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through 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. The 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 design flaw. A user may assume that the visible output is the only system activity but there is possibility that erroneous data could infest the system. A person other than the designer or user should test the application. Again, this is critical if the service desk is outsourced to an application service provider. Release of customer information to such an entity must be controlled through contractual requirements with penalties if data is compromised.

There are six categories of integrity controls summarized in Table 3.10.1.

**Table 3.10.1: Data Integrity Controls**

Control Category	Threats/Risks	Controls
Source data control	Invalid, incomplete, or inaccurate source data input	Forms design; sequentially pre-numbered forms, turnaround documents; cancellation and storage of documents, review for appropriate authorization; segregation of duties, visual scanning; check-digit verification; and key verification.
Input validation routines	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 time; re-edit them, and prepare a summary error report.

<p><b>On-line data entry controls</b></p>	<p>Invalid or inaccurate transaction input entered through on-line terminals</p>	<p>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.</p>
<p><b>Data processing and storage controls</b></p>	<p>Inaccurate or incomplete data in computer-processed master files</p>	<p>Policies and procedures (governing the activities of data processing and storage personnel; data security and 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 (data wise administrators, data 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; review of user of computer output for completeness and accuracy, shredding of confidential output no longer needed; error and exception reports.</p>

### 3.73 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), parity checking; and message acknowledgement procedures (echo checks, trailer labels, numbered batches)
-----------------------------------	---	--

#### 3.10.2 Data Integrity Policies

Major data integrity policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **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.
- **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.

#### 3.10.3 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. Multiple levels of data security are necessary in an information system 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 while 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.

### 3.11 Cyber Frauds

With the advancements in the technology, cyber frauds are also increasing day-by-day across the world. One of the major reasons behind the rise of such frauds are:

- Failure of internal control system,
- Failure of organizations to update themselves to new set of risk, and
- Smart fraudsters: These are people who are able to target the weaknesses in system, lacunae's in internal controls, even before the organization realizes that such gaps are there.

All of the above are key ingredients to increased instances of cyber frauds. In India, the Information Technology Amendment Act, 2008 and amended in 2008 has specific sections dealing with cyber frauds. The same has been discussed under the regulatory issues of Chapter 7 of the Study Material. The discussion in this part is based on general nature of cyber frauds.

Fraud, as defined by SA 240 (Revised), on "The Auditor's responsibility to consider fraud and error in an audit of financial statements", defines fraud as "intentional misrepresentation of financial information by one or more individuals among employees, management, those charged with governance, or third parties." This definition is in context of financial information; same can be applied to any information used for decision making. Fraud has also been defined as "Intentional Error". Cyber Fraud shall mean frauds committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft. Other common forms may be monetary cyber frauds include non-delivery of paid products purchased through online auction etc.

On the basis of the functionality, these are of two types:

- **Pure Cyber Frauds:** Frauds, which exists only in cyber world. They are borne out of use of technology. For example: Website hacking.
- **Cyber Enabled Frauds:** Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

The fraudster may be from within the organization or from outside the organization. But, it has been observed that most of cyber frauds include more than one individual and one of the team members in many cases is a person within the organization.

### 3.11.1 Cyber Attacks

The following is a chart displaying major cyber-attacks during the year 2011:

Each of the above is discussed as follows:

- **Phishing:** It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.
- **Network Scanning:** It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.

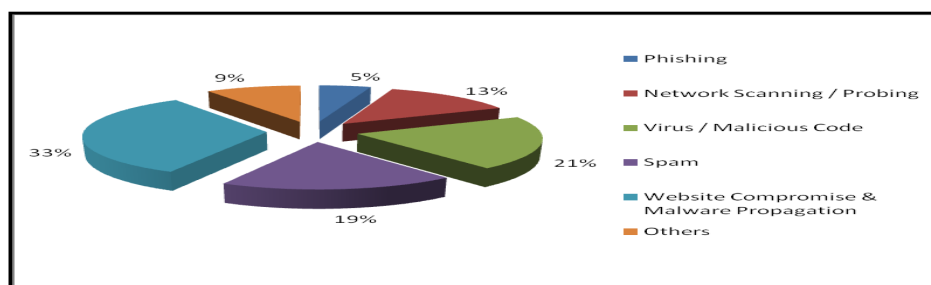


Fig. 3.11.1: Statistics of Cyber Attacks\*

- **Virus/Malicious Code:** As per Section 43 of the Information Technology Act, 2000, "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;
- **Spam:** E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as spam.
- **Website Compromise/Malware Propagation:** It includes website defacements. Hosting malware on websites in an unauthorized manner.
- **Others:** These are given as follows:
  - **Cracking:** Crackers are hackers with malicious intentions.
  - **Eavesdropping:** It refers to the listening of the private voice or data transmissions, often using a wiretap.
  - **E-mail Forgery:** Sending e-mail messages that look as if someone else sent it is

---

\* Source: <http://www.cert-in.org.in>

termed as E-mail forgery.

- **E-mail Threats:** Sending a threatening message to try and get recipient to do something that would make it possible to defraud him is termed as E-mail threats.
- **Scavenging:** This is gaining access to confidential information by searching corporate records.

### 3.11.2 Impact of Cyber Frauds on Enterprises

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- **Loss of credibility or Competitive Edge:** News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
- **Sabotage:** The above situation may lead to misuse of such information by enemy country.

### 3.11.3 Techniques to Commit Cyber Frauds

Following are the major techniques to commit cyber frauds:

- **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
- **Cracking:** Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
- **Data Diddling:** Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
- **Data Leakage:** It refers to the unauthorized copying of company data such as computer files.
- **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.

### 3.77 Information Systems Control and Audit

---

- **Internet Terrorism:** It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
- **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- **Masquerading or Impersonation:** In this case, perpetrator gains access to the system by pretending to be an authorized user.
- **Password Cracking:** Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
- **Piggybacking:** It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- **Scavenging or Dumpster Diving:** It refers to the gaining access to confidential information by searching corporate records.
- **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- **Trap Door:** In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

In spite of having various controls as well as countermeasures in place, cyber frauds are happening and increasing on a continuous basis. To overcome these frauds, there is an urgent need to conduct research in the related areas and come up with more appropriate security mechanisms, which can make the information systems more secure.

### 3.12 Summary

The chapter deals with Information System Security and its importance to an organization. The chapter defines the categories of information that may be considered sensitive and how same needs to be protected. In addition, the chapter also elaborates the concept of Information System Security Policy and the various components of the same. There is detailed discussion on each of the component of Information System Security Policy. It elaborates the steps to converting policies into Standards, Guidelines and Procedures.

The next part of chapter deals with controls and their types. The chapter elaborates the need for such controls. There is detailed discussion on the nature of controls and its implementation across organization. Failures to implement such controls and the resulting frauds have also been dealt in the chapter.

## Appendix-1

**Master Checklist on Logical Access Controls**

The following is an illustrative Checklist that could be used to review Logical Access Controls within application systems and databases.

No	Checkpoints
	User Access Management Policy and Procedure
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?
3.	Whether User IDs are in a unique format? <i>(Verify the naming conventions for the user IDs)</i>
4.	Whether invalid login attempts are monitored and User IDs are suspended on specific attempt? <i>(Verify the parameters set for unsuccessful login 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 guessing 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?

### 3.79 Information Systems Control and Audit

---

	<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>(On the desktop classified information should not be available, similarly no classified information should be available on the table unattended)</i>
9.	Whether the organisation restricted concurrent log- on? <i>(One user ID should not be allowed to login from 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 are 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 hashing algorithm of.)</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.
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.
<b>Maintenance of sensitive user accounts</b>	
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

**Appendix-2**

**Master Checklist for Physical and Environmental Security**

To ensure that IS assets are maintained in a secured manner within a controlled environment, the following checklist is given:

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:

### 3.81 Information Systems Control and Audit

---

	<ul style="list-style-type: none"><li>- Lay out of facilities</li><li>- Physical Security of the assets</li><li>- Physical 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 Information System 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 IS facility is accessed for information security related risks with respect to lighting, building orientation, signage and neighborhood characteristics are identified?
21.	Verify that surveillance systems are designed and operating properly?
22.	Ensure that physical access control procedures are comprehensive and being followed by security staff.
23.	Verify if the security controls in place are appropriate to prevent intrusion into sensitive IS facilities –data centre, communication hubs, emergency power services facilities?
24.	Review facility monitoring measures to ensure that alarm conditions are addressed promptly.
<b>Environmental Controls</b>	
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.	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 prevention instructions are clearly posted and fire alarm buttons clearly visible?

### 3.83 Information Systems Control and Audit

---

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 working condition.
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 to protect 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 of part inventories and vendor agreements are accurate and current and maintained as critical assets.

# 4

## Business Continuity Planning and Disaster Recovery Planning

---

### Learning Objectives

- To understand the concept of Business Continuity Management;
- To understand the key phases and components of a Business Continuity Plan,
- To understand the key aspects of BCP Implementation;
- To learn about Back-up and Disaster Recovery Planning; and
- To learn how to audit a BCP.

### Task Statements

- To design, develop, implement, test, maintain and audit all key phases and components of a Business Continuity Plan in an enterprise; and
- To conduct Risk assessment and Business Impact Assessment.

### Knowledge Statements

- To know the concepts and components of Business Continuity Management;
- To know the development of Business Continuity Plans, Disaster Recovery Plans; Emergency Plans etc; and
- To know the different phases and components of BCP.

### 4.1 Introduction

Today, the networked society exceeds the boundaries of the nations with increased dependency on supply chain management demanding regulatory compliance, security and privacy of data and above all, improvement in performance and availability of services on 24 x 7 basis. Meeting their demands in global economy requires an enterprise to be able to meet the challenges of ever increasing threats and risks. They should be able to not only withstand but suitably adapt the sudden disruptions due to infrastructure outage or human error, else it might impact not only revenue but also the image and brand, ultimately leading to the survival of the enterprise of all types and sizes, public and private.

Business Continuity Management (BCM), over the years has emerged a very effective management process to help enterprises to manage the disruption of all kinds, providing countermeasures to safeguard from the incident of disruption of all kinds. With the BCM

## 4.2 Information Systems Control and Audit

---

Process in place, enterprises are able to assess the potential threats and manage the consequences of the disruption, which could reduce or eliminate the losses that would have resulted.

In order to ensure effective implementation of BCM, the enterprise should conduct regular internal audits at planned intervals to conform to the compliance of Business Continuity Process in line with the policy and regulatory requirements for the enterprise. The findings of the internal audit should be reported to the top management for necessary corrective action and improvements and the management to provide adequate resources to ensure that necessary corrections and corrective actions are taken without undue delay to eliminate nonconformities and their cause. The internal auditing activities should be taken up by the independent group within the enterprises such as internal audit functions managed by Chartered Accountants etc. This would ensure objectivity and impartiality of the audit process engaging the professionals for these key activities.

This chapter provides further insight into the BCM Policy, BCM Processes of management, assessment, strategy development and implementation, testing and maintenance and trainings. This facilitates the understanding of the concept, planning, implementation and continuous improvements of BCPs.

### 4.2 Need of Business Continuity Management (BCM)

To meet the enterprise business objectives and ensure continuity of services and operations, an enterprise shall adapt and follow well-defined and time-tested plans and procedures, build redundancy in teams and infrastructure, manage a quick and efficient transition to the backup arrangement for business systems and services. Business continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities. Let us understand some key terms related to BCM.

- **Business Contingency:** A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.
- **BCP Process:** BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations. The purpose of BCP is to ensure that vital business functions (critical business operations) are recovered and operationalized within an acceptable timeframe. The purpose is to ensure continuity of business and not necessarily the continuity of all systems, computers or networks. The BCP identifies the critical functions of the enterprise and the resources required to support them. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and incident response so as to ensure that the proper procedures will be carried out to ensure the timely restoration of services.
- **Business Continuity Planning (BCP):** It refers to the ability of enterprises to recover from a disaster and continue operations with least impact. It is imperative that every

enterprise whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the enterprise. It is not enough that enterprise has a BCP but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the enterprise.

#### **4.2.1 BCP Manual**

An incident or disaster affecting critical business operations can strike at anytime. Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. The BCP is expected to provide:

- Reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.
- Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services to clients'.

The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liaisoning teams between the functional area(s) affected and other departments providing support services.

BCM is business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- Proactively improves an enterprise's resilience against the disruption of its ability to achieve its key objectives;
- Provides a rehearsed method of restoring an enterprise's ability to supply its key products and services to an agreed level within an agreed time after a disruption; and
- Delivers a proven capability to manage a business disruption and protect the enterprise's reputation and brand.

#### **4.2.2 Scope of Business Continuity**

Top management of the enterprise needs to define the scope of the BCM program by identifying the key products and services that support the enterprise's objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis. In case of an outsourced service or activity, the risk accountability remains with the enterprise and necessary controls and process should be in place to manage the risk from an outsourced service.

### 4.2.3 Advantage of Business Continuity

The advantages of BCM are that the enterprise:

- is able to proactively assess the threat scenario and potential risks;
- has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and
- is able to demonstrate a response through a process of regular testing and trainings.

### 4.3 BCM Policy

The main objective of BCP is to minimize/eliminate the loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction. This policy document is a high level document, which shall be the guide to make a systematic approach for disaster recovery, to bring about awareness among the persons in scope about the business continuity aspects and its importance and to test and review the business continuity planning for the enterprise in scope.

While developing the BCM policy, the enterprise should consider defining the scope, BCM principles, guidelines and minimum standards for the enterprise. They should refer any relevant standards, regulations or policies that have to be included or can be used as a benchmark. The objective of this policy is to provide a structure through which:

- Critical services and activities undertaken by the enterprise operation for the customer will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updation as required.
- Planning and management responsibility are assigned to a member of the relevant senior management team.

The BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability. The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability. The ongoing maintenance and management activities include embedding business continuity within the enterprise, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process market, technology or organizational structure.

## 4.4 Business Continuity Planning

Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an enterprise 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 otherwise 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 organizations, it is preferable for a firm's disaster recovery planner(s) to understand fully the risks to operations and the measures that can minimize the probabilities and consequences, and to formulate their disaster recovery plan accordingly.

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:* This is the operation's piece of business continuity planning.
- *Disaster Recovery Planning:* This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- *Crisis Management:* This is the overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization'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 organization 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

## 4.6 Information Systems Control and Audit

---

following components: Information, Technology, Telecommunication, Process, People, and Facilities.

### 4.4.1 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 organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and
- Identify critical lines of business and supporting functions.

Therefore, the goals of the business continuity plan should be to:

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

## 4.5 Developing a Business Continuity Plan

The methodology for developing a BCP can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organization. The methodology emphasizes on the following:

- Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- Obtaining commitment from appropriate management to support and participate in the effort;
- Defining recovery requirements from the perspective of business functions;
- Documenting the impact of an extended loss to operations and key business functions;
- Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;



- Selecting business continuity teams that ensure the proper balance required for plan development;
- Developing a business continuity plan that is understandable, easy to use and maintain; and
- 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 given as follows:

- (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
- (vii) Maintenance Program
- (viii) Initial Plan Testing and Plan Implementation

Each of these phases are described below:

- **Phase 1 – Pre-Planning Activities (Project Initiation):** This Phase is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to:
  - refine the scope of the project and the associated work program;
  - develop project schedules; and
  - identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase, a Steering Committee should be established. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing 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 project.
- **Phase 2 – Vulnerability Assessment and General Definition of Requirements:** Security and controls within an organization are continuing concern. It is preferable from

## 4.8 Information Systems Control and Audit

---

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 minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence.

This phase will include the following key tasks:

- A thorough Security Assessment of the computing 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.
- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- 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.
- Define the scope of the planning effort.
- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.
- Assemble Project Team and conduct awareness sessions.
- **Phase 3 – Business Impact Assessment (BIA):** A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:
  - identify critical systems, processes and functions;
  - assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
  - assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes 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.

- **Phase 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 analyzing alternative

recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, 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.

- **Phase 5 – Plan Development:** During 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 be developed during this phase.
- **Phase 6 – Testing/Exercising Program:** The plan 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.
- **Phase 7 – Maintenance Program:** Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. 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. Many recovery software products take this requirement into account.
- **Phase 8 – Initial Plan 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;
  - Analyzing test results; and
  - Modifying the plans as appropriate.

The approach taken to test the plans depends in large part, on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

## 4.6 Components of BCM Process

Components of BCM Process are given as follows (in Fig. 4.6.1):

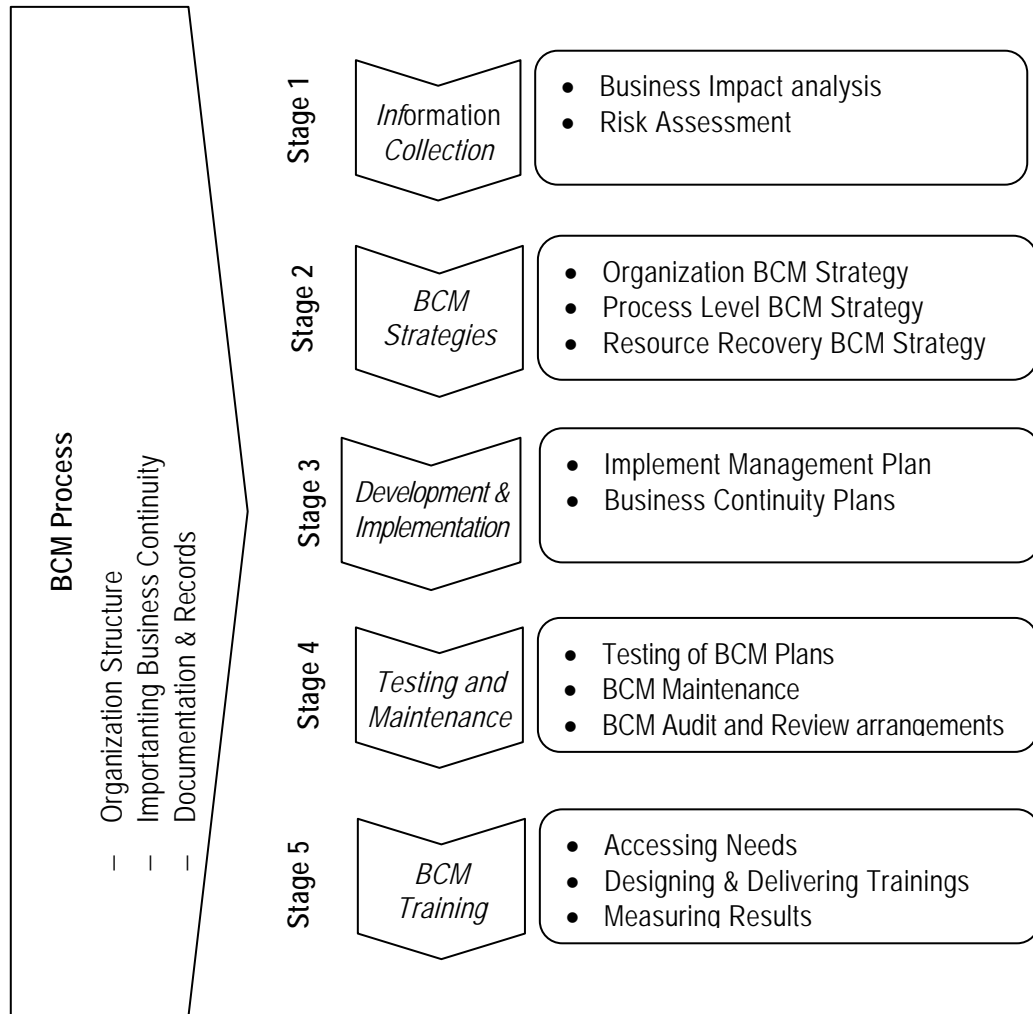


Fig 4.6.1: Components of BCM Process

- BCM – Process**  
 The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.
- BCM – Information Collection Process**  
 The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the

requirements that will determine the selection of appropriate BCM strategies in the next process.

- **BCM – Strategy Process**

Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.

- **BCM – Development and Implementation Process**

Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.

- **BCM – Testing and Maintenance Process**

BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.

- **BCM – Training Process**

Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

These components are explained below in detail.

## **4.7 Business Continuity Management Process**

A BCM process should be in place to address the policy and objectives as defined in the business continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity management. The BCM Processes are mapped as follows:

### **4.7.1 Organization Structure**

The organization should nominate a person or a team with appropriate seniority and authority to be accountable for BCM policy implementation and maintenance. It should clearly define the persons responsible for business continuity within the enterprise and responsibility.

### **4.7.2 Implementing Business Continuity in the Enterprise and Maintenance**

In establishing and implementing the BCM system in the organization, managers from each function on site represent their areas of the operation. These people are also responsible for the ongoing operation and maintenance of the system within their area of responsibility. Where training is required to enable as a colleague to effectively carry out their BCM

#### 4.12 Information Systems Control and Audit

---

responsibilities, this will be identified as part of the ongoing staff appraisal and training process.

Top management should appoint the Manager (BCM) role as being the role that is responsible for the BCM policy and its implementation. The Resource Planning Manager is supported by the Shift Leaders and Team Captains from each function, who are responsible for the ongoing implementation and maintenance of the BCM. The program should be communicated to all the stakeholders with appropriate training and testing. The enterprise may adopt any project management model for effective output.

In implementation, the major activities that should be carried out include:

- Defining the scope & context;
- Defining roles and responsibilities;
- Engaging and involving all stakeholders;
- Testing of program on regular basis;
- Maintaining the currency & appropriateness of business continuity program;
- Reviewing, reworking and updating the business continuity capability, risk assessments (RA) and business impact analysis (BIAs);
- Managing costs and benefits associated; and
- Convert policies and strategies into action.

##### 4.7.3 BCM Documentation and Records

All documents that form the BCM are subject to the document control and record control processes. The following documents (representative only) are classified as being part of the business continuity management system:

- The business continuity policy;
- The business continuity management system;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;

- Exercise schedule and results;
- Incident log; and
- Training program.

To provide evidence of the effective operation of the BCM, records demonstrating the operation should be retained for a minimum period of 1 year, in line with enterprise's policy. The nature of the record means that the retention is a statutory, regulatory or customer requirement, it will be retained for the amount of time dictated. These records include reference to all business interruptions and incidents, irrespective of the nature and length of disruption. This also includes general and detailed definition of requirements as described in developing a BCP. In this, a profile is developed by identifying resources required to support critical functions, which 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.

#### **4.8 BCM Information Collection Process**

In order to design an effective BCM, it is pertinent to understand the enterprise from all perspectives of interdependencies of its activities, external enterprises and including:

- enterprise's objectives, stakeholder obligations, statutory duties and the environment in which the enterprise operates;
- activities, assets and resources, including those outside the enterprise, that support the delivery of these products and services;
- impact and consequences over time of the failure of these activities, assets and resources; and
- Perceived threats that could disrupt the enterprise's key products and services and the critical activities, assets and resources that support them.

The pre-planning phase of Developing the BCP also involves collection of information. It enables us to refine the scope of BCP 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. Two other key deliverables of that 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.

The process used for the development of both Business Impact Analysis and the Risk Assessment is detailed below. The outputs from these processes are reviewed by top management and signed off as being an accurate representation of the operation at the time of their completion. Both the BIA and Risk Assessment will be reviewed as part of the annual BCM management review or following a change to the operation, its processes or associate risks. This review will ensure that the findings and the decisions made as a result of the findings are still accurate and relevant to the needs of the operation and its stakeholders.

### 4.8.1 Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services. 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. For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

- assess the impacts that would occur if the activity was disrupted over a period of time;
- identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
- Identify critical business processes;
- assess the minimum level at which the activity needs to be performed on its resumption;
- identify the length of time within which normal levels of operation need to be resumed; and
- Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

The enterprise should have a documented approach to conduct BIA. The enterprise should document its approach to assessing the impact of disruption and its findings and conclusions. The BIA Report should be presented to the Top Management. This report identifies critical service functions and the time frame 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. Developing the BCP also takes into account the BIA process.

### 4.8.2 Classification of Critical Activities

BCP leader and BCP team leaders in consultation with respective function owner shall carry out Business Impact Analysis for infrastructure and business transactions. BIA will result in categorization (like vital, desirable and essential) of infrastructure and business function following by disaster scenarios (Catastrophic, major, minor trivial) for various disaster causes (fire, flood, system failure etc.), which is given as follows:

- *Business Categorization (Vital/essential/desirable):* The parameters considered in deciding whether a function/service is Vital/Essential/Desirable are:
  - Loss of revenue;
  - Loss of reputation;
  - Decrease in customer satisfaction; and
  - Loss of productivity (man-hours).

These parameters shall be graded in a three-point scale 1-3 where,



- 1 = Low (L)
- 2 = Medium (M)
- 3 = High (H)

- *Disaster Scenarios (Major/minor/trivial/catastrophic):* The scenario of disaster shall be decided with the matrix given below:

The X-axis represents the Business impact of the infrastructure and business transaction as desirable (value=1), essential (value=2) or vital (value=3). The Y-axis represents the likelihood of occurrence of the disaster on a three point scale (1-3).

3 (minor)	6(Major)	9(Catastrophic)
2(Trivial)	4(Major)	6(Major)
1(Trivial)	2(Trivial)	3(Minor)

**Fig. 4.8.1: Business Impact [Desirable (1), Essential (2), Vital (3)]**

Identify all the mission critical processes for categorizing into Vital, Essential and Desirable and looking for the probable disasters as per the list attached.

#### 4.8.3 Risk Assessment

The risk assessment is assessment of the disruption to critical activities, which are supported by resources such as people, process, technology, information, infrastructure supplies and stakeholders. The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality. It is the decision of the enterprise to select a risk assessment approach, but it is important that it is suitable and appropriate to address all of the enterprise’s requirements. For ready reference

Specific threats may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.

Vulnerabilities might occur as weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience. The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist. This is similar to vulnerability assessment phase of developing a BCP.

Impacts might result from the exploitation of vulnerabilities by threats. As a result of the BIA and the risk assessment, the enterprise should identify measures that:

- reduce the likelihood of a disruption;
- shorten the period of disruption; and

## 4.16 Information Systems Control and Audit

---

- limit the impact of a disruption on the enterprise's key products and services.

These measures are known as loss mitigation and risk treatment. Loss mitigation strategies can be used in conjunction with other options, as not all risks can be prevented or reduced to an acceptable level. The enterprise might include one or more or all of the strategies for each critical activity.

### 4.9 BCM Strategy Process

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

The enterprise develops and documents a series of plans, which enable them to effectively manage an incident with impacts on the site operations and subsequently recover its critical activities and their supporting resources, within the timescales agreed with the customer. While some activities have been defined as non-critical, the actions required to recover these are also included in the business continuity plans as they assist in allowing the critical activities to operate in a more efficient and effective manner. The enterprise may adopt any strategy but it should take into account the implementation of appropriate measures to reduce the likelihood of incidents and/ or reduce the potential impact of those incidents and resilience and mitigation measures for both critical and non critical activities.

### 4.10 BCM Development and Implementation Process

The enterprise should have an exclusive organization structure, Incident Management Team / Crisis management team for an effective response and recovery from disruptions. In the event of any incident, there should be a structure to enable the enterprise to:

- confirm Impact of incident (nature and extent),
- control of the situation,
- contain the incident,
- communicate with stakeholders, and
- coordinate appropriate response.

#### 4.10.1 The Incident Management Plan (IMP)

To manage the initial phase of an incident, the crisis is handled by IMP. The IMP should have top management support with appropriate budget for development, maintenance and training. They should be flexible, feasible and relevant; be easy to read and understand; and provide the basis for managing all possible issues, including the stakeholder and external issues, facing the enterprise during an incidents.

#### 4.10.2 The Business Continuity Plan (BCP)

To recover or maintain its activities in the event of a disruption to a normal business operation, the BCP are invoked to support the critical activities required to deliver the enterprise's objectives. They may be invoked in whole or part and at any stage of the response to incident.

The recovery strategies may be two-tiered:

- Business: Logistics, accounting, human resources, etc; and
- Technical: Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).

The plan development phase also includes the implementation of changes to use 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 organization's recovery strategy needs to be developed for the recovery of the many business processes.

#### 4.11 BCM Testing and Maintenance Process

Various aspects of BCM Testing and Maintenance Process are given as follows:

##### 4.11.1 BCM Testing

A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become outdated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to be clearly defined in the BCP. A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation. Testing may be based on a predetermined outcome, e.g. plan and scope in advance; or allow the enterprise to develop innovative solutions.

An exercise program should lead to objective assurance that the BCP will work as anticipated when required. The BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.) and technology and telecommunications recovery, including the availability and relocation of staff. In addition, it might lead to the improvement of BCM capability by:

- Practicing the enterprise's ability to recover from an incident;
- Verifying that the BCP incorporates all enterprise critical activities and their dependencies and priorities;
- Highlighting assumptions, which need to be questioned;
- Instilling confidence amongst exercise participants;
- Raising awareness of business continuity throughout the enterprise by publicizing the exercise;

#### 4.18 Information Systems Control and Audit

---

- Validating the effectiveness and timeliness of restoration of critical activities; and
- Demonstrating competence of the primary response teams and their alternatives.

The frequency of testing should depend upon both the enterprise's needs, the environment in which it operates, and stakeholder requirements. However, the testing program should be flexible, taking into account the rate of change within the enterprise, and the outcome of previous one. The above exercise methods can be employed for individual plan components, and single and multiple plans. In case of Development of BCP, 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.
- These sources such as business processes, 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.

**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;
- Analyzing 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 organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

##### 4.11.2 BCM Maintenance

It is important to keep preparations including documentation, up-to-date. Contracts and agreements may also need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture. The BCM maintenance process demonstrate the documented evidence of the proactive management and governance of the enterprise's business continuity program; the key people who are to implement the BCM strategy and plans are trained and competent; the monitoring and control of the BCM risks faced by the enterprise; and the

evidence that material changes to the enterprise's structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise's business continuity and incident management plans.

Similarly, the maintenance tasks undertaken in Development of BCP are to:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- 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; and
- Implement version control procedures to ensure that the plan is maintained up-to-date.

#### **4.11.3 Reviewing BCM Arrangements**

An audit or self-assessment of the enterprise's BCM program should verify that:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the enterprise's objectives);
- The enterprise' BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
- The enterprise's BCM maintenance and exercising programs have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- The enterprise has an ongoing program for BCM training and awareness;
- BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- Change control processes are in place and operate effectively.

#### **4.12 BCM Training Process**

An enterprise with BCM uses training as a tool to initiate a culture of BCM in all the stakeholders by:

- Developing a BCM program more efficiently;

## 4.20 Information Systems Control and Audit

---

- Providing confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions;
- Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels; and
- Minimizing the likelihood and impact of disruptions

Development of a BCM culture is supported by:

- Leadership from senior personnel in the enterprise;
- Assignment of responsibilities;
- Awareness raising;
- Skills training; and
- Exercising plans.

### 4.12.1 Training, Awareness and Competency

While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined. These are consistent with the competencies required by the organization of the relevant role and are given as follows:

- Actively listens to others, their ideas, views and opinions;
- Provides support in difficult or challenging circumstances;
- Responds constructively to difficult circumstances;
- Adapts leadership style appropriately to match the circumstances;
- Promotes a positive culture of health, safety and the environment;
- Recognizes and acknowledges the contribution of colleagues;
- Encourages the taking of calculated risks;
- Encourages and actively responds to new ideas;
- Consults and involves team members to resolve problems;
- Demonstrates personal integrity; and
- Challenges established ways of doing things to identify improvement opportunities.

## 4.13 Types of Plans

There are various kinds of plans that need to be designed. They include the following:

### 4.13.1 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 e.g., 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 enterprise 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 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.

#### **4.13.2 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 organization'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 organization, 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.

#### **4.13.3 Recovery Plan**

The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan 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 organization, new members must be appointed immediately and briefed about their responsibilities.

### 4.13.4 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 organization 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 organization's ability to recover from a catastrophe.

### 4.14 Types of Back-ups

When the back-ups are taken of the system and data together, they are called total system's back-up. Various types of back-ups are given as follows:

- **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. One 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 probably includes 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 cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

#### 4.15 Alternate Processing Facility Arrangements

Security administrators should consider the following backup options:

- **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.
- **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.
- **Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the 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.
- **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

- how soon the site will be made available subsequent to a disaster;
- the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- the priority to be given to concurrent users of the site in the event of a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- the facilities and services the site provider agrees to make available; and
- 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.

## 4.16 Disaster Recovery Procedural Plan

The disaster recovery 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 jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning 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 organization, 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.
- 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.

#### **4.17 Audit of the BCP/DRP**

In a BCP Audit, the auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. BCP Auditor is expected to identify residual risks, which are not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit.

Sample list of BCP Audit steps are given below:

- (i) Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:
  - Identification and prioritization 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.
- (viii) Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.

#### 4.26 Information Systems Control and Audit

---

- (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 minimizing 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?
  - 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?
- (xix) *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?

- 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.

(xx) *Information Technology*

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization 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.

(xxi) *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?

#### 4.28 Information Systems Control and Audit

---

(xxii) Does the disaster recovery/ business resumption plan include the names and numbers of suppliers of essential equipment and other material?

(xxiii) 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.

(xxiv) 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 authorize activation of the plan should the need arise.

#### 4.18 Summary

In order to demonstrate responsiveness to business requirements and addressing the needs of all the stakeholders, it is imperative to establish the BCM process in any enterprise. The advantages of having an effective business continuity process are numerous but the most important factor is the brand value and the reputation of the enterprise. Therefore, the management has to have adequate resource provision in terms of budget, skilled manpower, technology etc. to establish BCM process and lead the industry sector by providing uninterrupted continuous 24x 7 operations to the external as well as internal customers.

BCM identifies itself as a management approach by focusing on aligning an enterprise with its customers through the execution of processes. It enables the enterprises to be more efficient and effective by becoming a process-based enterprise.

# 5

## Acquisition, Development and Implementation of Information Systems

---

### Learning Objectives

- To understand the modern business systems and business process design;
- To conceptualize a systematic approach to SDLC and review its phase wise activities, methods, tools, controls etc.;
- To understand the software procurement, RFP process, Evaluation of IT proposals etc.;
- To analyze the current system in view of understanding requirements;
- To compare different SDLC models and to be able select the most appropriate model for a particular project;
- To conceptualize the generic phases and associated activities of SDLC;
- To understand the importance of testing, implementation and maintenance; and
- To know the auditor's role in SDLC;

### Task Statements

- To demonstrate business process modeling;
- To select the system development method best suited for a project;
- To calculate the ROI for given projects;
- To organize the procurement as well as development of information systems, in case of particular business needs;
- To undertake feasibility study of the IS projects; and
- To manage the acquisition of hardware, software and other necessary infrastructure for establishing the requisite operating infrastructure.

### Knowledge Statements

- To know the business process modeling;
- To know the key consideration, while going for system development;
- To know various methods by which a system development can be undertaken;
- To know advantages and disadvantages of various system development models;
- To know different phases of SDLC and their related concepts; and
- To know the auditor's role in SDLC.

### 5.1 Introduction

Information systems play a vital role in the success of any functional system today. It may be reckoned as the symbiosis of IT hardware and software, in today's super highways of information infrastructure. Information systems serve many different purposes. Its functions may include the processing of business transactions to provide information needed to decide recurring issues, assisting senior officials with strategy formulations, and linking office information and corporate data etc. 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 computers 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 effectively and efficiently then deployment would be justified.

In the business context today, information systems are inevitable. Its deployment may be triggered by acquisition of already functional ready-to-use systems or by the development of customised solutions using requisite IT infrastructure, environment and support. System acquisition efforts are put in place due to many reasons, but primarily due to availability of such systems on affordable prices subject to satisfactory solution to the requisite tasks and functionalities. Another pressing need may be caused by stress in existing system. That is, the present system is not able to meet the requirements of system stakeholders and particularly, of its users. This makes it necessary to change/modify the system. To change or to modify depends on the intensity of stress. There are situations, which can be managed by slight modifications, but there may be situations, which may need complete overhaul. Secondly, case entity goes for system change. For example: Increased competition, pressure on profits, customer satisfaction being few reasons, which have forced many corporate to go for better systems. Many of them have shifted from traditional accounting packages to Enterprise Resource Planning Software.

Moreover, opportunity may be another reason for acquisition i.e. if management sees that there is scope for capitalising on a new business opportunity / venture, then management goes for system acquisition. Many companies implement new software's to capitalise in such opportunity. Effort for system development requires an understanding of the business process of the entity. In business, systems development refers to the process of examining a business situation in the prevailing context with the intent of improving it through better procedures and methods. The breaking point shall be business process design, in view of the feasibility of automation using affordable technical artefacts and to meet the goals.

### 5.2 Business Process Design

Business process design means structuring or restructuring the tasks, functionalities and activities for improvising a business system. Business Process Design is a critical step to understand the requirements of the system. Business Process Design needs a lot of intellectual capability from team of developers doing the same. Business process design involves a sequence of the steps described briefly in the following sections.



### 5.2.1 Present Process Documentation

In this step, the present business process is analyzed and documented. The key deliverable of this step includes the well-defined short-comings of the present processes and the overall business requirements. This step includes the following activities:

- Understanding the business and the objectives for which it exists;
- Documenting the existing business processes; and
- Analysis of the documented processes.

### 5.2.2 Proposed Process Documentation

This step is to design the new process requirements for the system. The design is based on the new system requirements and the changes proposed. The activities include the following:

- Understanding of the business processes necessary to achieve the business objectives;
- Designing the new processes; and
- Documentation of the new process, preferably using of CASE tools.

### 5.2.3 Implementation of New Process

This step is to implement largely the new as well as modified processes at the entity. The critical activities may include the following:

- Validating the new process;
- Implementing the new process; and
- Testing the new process.

It has been mentioned that system development effort is triggered in two basic situations, first due to stress and second due to opportunity. Business Process Design is largely based on nature of system i.e. whether it is typically integrated, automatic and manual. The idea of business process design has different implications when the same is being designed for integrated, automatic or manual system. Each nature of system needs a special design consideration, which may be understood by looking at the following case descriptions.

To understand these aforementioned facts in a more practical way, some case studies are given as follows:

**Case 1: Manual Billing System:** The billing clerk checks the price list of products before s/he bills the same to customer. S/he checks the approved price list of the products as is applicable on the date of billing, checks for discounts and bills the products to customer. In the above process, the key issue being that the billing clerk needs to possess, applicable and authorized price list with him. Business Process Design shall need to address the following critical issues:

- Availability of approved price lists with billing clerk.
- How it shall be ensured that the billing has been done on applicable rates only?
- How the approval is accorded to price lists?

## 5.4 Information Systems Control and Audit

---

- Whether the price list updating process is pre-defined or need based?
- How exceptions to listed price shall be documented?
- How the exceptions shall be submitted to management?

**Case 2: Automatic Billing System:** In this system, every bill is generated through system. System has in its database of approved price list. As soon as, the billing clerk selects the product from product lists, the system automatically picks up the price, as it is already available in data base. There is no option available with billing clerk to modify price at the time of billing. The key processes that need to be controlled include, ensuring the system price list is the approved price list. Business Process Design shall need to address the following issues:

- Availability of approved price lists in system.
- How it shall be ensured that the price lists in system cannot be modified?
- How the approval is accorded to price lists?
- Whether the price list updating process is pre-defined or need based?
- How the said price lists are updated in system?
- How the correctness of updates is validated?
- How exceptions, where the billed price is different from price in system authorized?
- How the exceptions to price reported to management?
- Does system provide a separate report for the same?

**Case 3: Integrated Systems:** Integrated system means a system, which has been tightly interfaced with the business processes of the entity. This shall require greater intellectual inputs to the process of business process modeling. The key issue to be addressed being the interface between the business process and the business objective. The issue to be addressed in addition to those discussed above shall include following:

- How the business objective change is built into business process change?
- How the business processes shall be documented?

Business Process Modeling is an important step for the process of system development. This step is important and critical for success of better system development. A off shoot of this process is the term Business Process Re-engineering. The key difference being, that in Business Process Re-engineering, the existing processes are fundamentally redefined rather than new processes being created, in the light of accommodating new environmental developments.

## 5.3 System Development

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 described briefly as follows:

- **System Analysis** is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.
- **System Design** is the process of planning and structuring 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 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, s/he needs to know more about the following:

- How does 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. S/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. S/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.

### 5.3.1 Achieving System Development Objectives

Achieving the objectives of the system development is essential but many times, such objectives are not achieved as desired. An analysis on 'why organizations fail to achieve their systems development objectives' reveals bottlenecks. Some of the most notable ones are described briefly as follows:

- (i) **User Related Issues:** It refers to those issues where user/customer is reckoned as the primary agent. Some of the aspects with regard to this problem are mentioned as follows:
  - **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information 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 purpose might change since the development process began.
  - **Resistance to Change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the

## 5.6 Information Systems Control and Audit

---

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 efforts to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to 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.
- (ii) **Developer Related Issues:** It refers to the issues and challenges with regard to the developers. Some of the critical bottlenecks are mentioned as follows:
- **Lack of Standard Project Management and System 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, system developers often lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do a little to help their development personnel stay technically sound, and more so a training plan and training budget do not exist.
- (iii) **Management Related Issues:** It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals. Some of such bottlenecks are mentioned as follows:
- **Lack of Senior Management Support and Involvement:** 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.
  - **Development of Strategic Systems:** Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.
- (iv) **New Technologies:** When an organization tries to create a competitive advantage by applying advance technologies, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.

In order to overcome these aforementioned issues, organizations must execute a well-planned systems development process efficiently and effectively. Accordingly, a sound system development team is inevitable.

### 5.3.2 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. Such committee usually consists of a group of key users of Information Systems services, those act 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 organization, systems designers take a lead role during the design, development and implementation stages. 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.

### 5.3.3 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.

An accountant can help in various related aspects during system development; some of them are as follows:

- (i) **Return on Investment (referred as ROI):** This defines the return, an entity shall earn on a particular investment i.e. capital expenditure. This financial data is a prime consideration for any capital expenditure entity decides to incur. The important data required for this analysis being the cost of project, the expected revenue/benefit for a given period. The analysis ideally needs to be done before the start of the development efforts for better decision making by management. For this analysis following data needs to be generated.
- (a) **Cost:** This includes estimates for typical costs involved in the development, which are given as follows:
- *Development Costs:* Development Costs for a computer based information system include costs of the system development process, like salaries of developers.
  - *Operating Costs:* Operating Costs of a computer based information system including hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.
  - *Intangible Costs:* Intangible Cost 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.

## 5.8 Information Systems Control and Audit

---

(b) **Benefits:** The benefits, which result from developing new or improved information systems that can be subdivided into tangible and intangible benefits. A post implementation analysis is also done to see how the system development effort has benefitted an organization. For example: A large oil company in public sector, few years back implemented an ERP system at a total cost of ₹ 100 crores. The calculated benefits from the project were ₹ 40 crores per annum. Above data gives an actual ROI of 40%, which is tremendous for any business. Same also tells the payback period is around 2.5 years.

(ii) **Computing Cost of IT Implementation and Cost Benefit Analysis:** For analysis of ROI, accountants need the costs and returns from the system development efforts. For correct generation of data, proper accounting needs to be done. Accountants shall be the person to whom management shall look for the purpose.

(iii) **Skills expected from an Accountant:** An accountant, being an expert in accounting field must possess skills to understand the system development efforts and nuances of the same. S/he is expected to have various key skills, including understanding of the business objectives, expert book keeper, and understanding of system development efforts etc.

## 5.4 Systems Development Methodology

A **System Development Methodology** is a formalized, standardized, well-organized and 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 as well as requisite functionalities.
- 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.

Since organizations vary significantly in the way they automate their business procedures, and each new type of system usually differs from others, 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 established as models and include Waterfall - Linear framework type, Prototyping-Iterative framework type, Incremental - Combination of linear and iterative framework type, Spiral - Combination linear and iterative framework type, Rapid Application Development (RAD) : Iterative Framework Type, and Agile Methodologies models; described one by one in the following sections:

#### 5.4.1 Waterfall Model

The waterfall approach is a traditional development approach in which each phase is carried in sequence or linear fashion. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release. In this traditional approach of system development, activities are performed in sequence. Fig. 5.4.1 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.

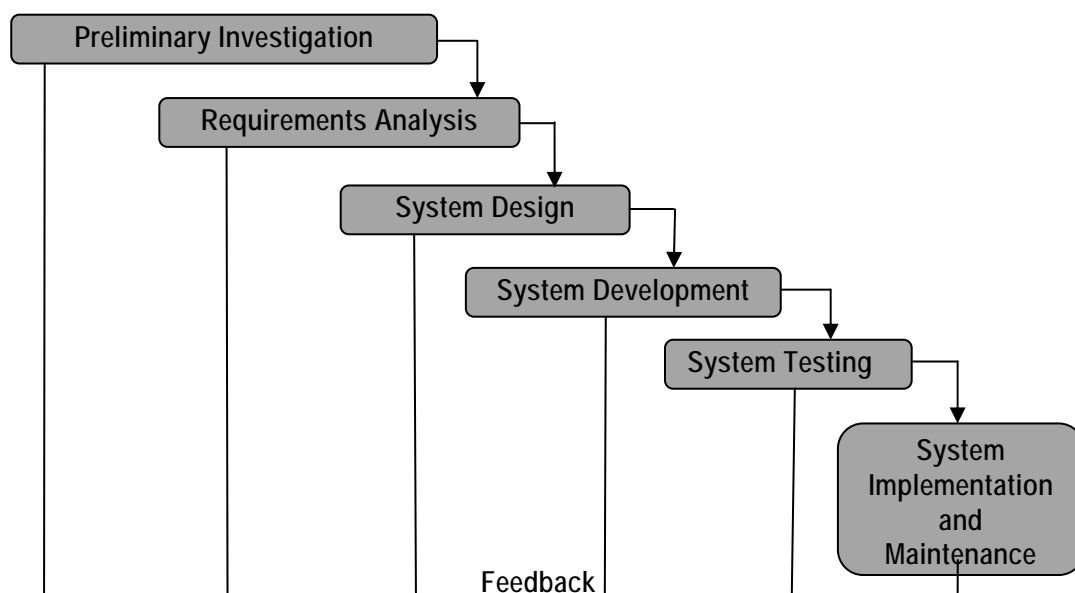


Fig. 5.4.1: Waterfall Approach

The characterizing features of this model have influenced the development community in big way. Some of the key characteristics are the following:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.

## 5.10 Information Systems Control and Audit

---

- 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.
- (a) **Strengths:** The fundamental strength of the waterfall model has made it quite popular and handy among the fraternity. Major strengths are given as follows:
  - It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
  - The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.
  - Progress of system development is measurable.
  - It enables to conserve resources.
- (b) **Weaknesses:** Though it is highly useful model, it suffers from various weaknesses too. Experts and practitioners identify a number of weaknesses including the following:
  - It is criticized to be inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
  - Project progresses forward, with only slight movement backward.
  - There is a little to iterate, which may be essential in situations.
  - It depends upon early identification and specification of requirements, even if the users may not be able to clearly define 'what they need early in the project'.
  - Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
  - Problems are often not discovered until system testing.
  - System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
  - It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.
  - It leads to excessive documentation, whose updation to assure integrity is an uphill task and often time-consuming.
  - Written specifications are often difficult for users to read and thoroughly appreciate.
  - It promotes the gap between users and developers with clear vision of responsibility.

### 5.4.2 The Prototyping Model

The traditional approach sometimes may take years to analyze, design and implement a system. More so, many a times we know a little about the system until and unless we go through its working phases, which are not available. In order to avoid such bottlenecks and overcome the issues, 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 modifying/replicating/expanding or even replacing it by a full-scale and fully operational system. As users work with the prototype, they learn about the system criticalities and make suggestions about the ways to manage it. These suggestions are then incorporated to improve the prototype, which is also used and evaluated. 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.

Prototyping can be viewed as a series of four steps, symbolically depicted in Fig. 5.4.2 wherein Implementation and Maintenance phases followed by full-blown developments take place once the prototype model is tested and found to be meet uses' requirements. The generic phases of this model are explained as follows:

- **Identify Information System Requirements:** In traditional approach, the system requirements are 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.
- **Develop the Initial Prototype:** The designers create an initial base model and give little or no consideration to internal controls, but instead emphasize 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.
- **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.

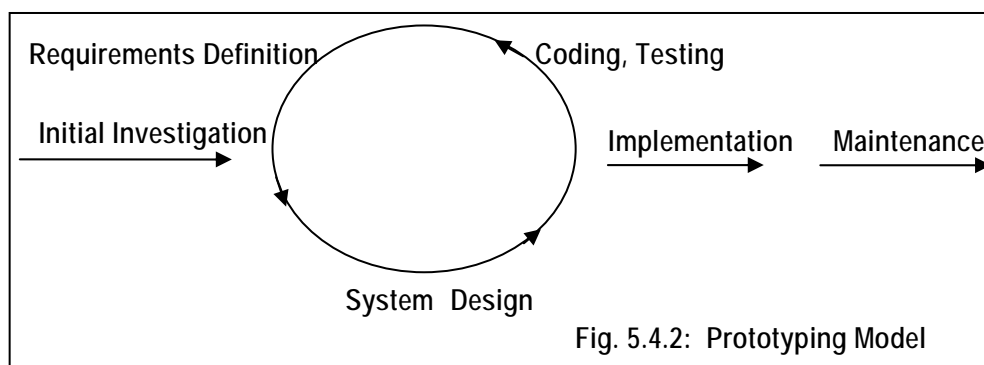


Fig. 5.4.2: Prototyping Model

## 5.12 Information Systems Control and Audit

---

- **Obtain User Signoff of the Approved Prototype:** 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.
- (a) **Strengths:** Some of its strengths identified by the experts and practitioners include the following:
  - It improves both user participation in system development and communication among project stakeholders.
  - It is 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.
  - Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
  - It helps to easily identify, confusing or difficult functions and missing functionality.
  - It enables to generate specifications for a production application.
  - It encourages innovation and flexible designs.
  - It provides for quick implementation of an incomplete, but functional, application.
  - It typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
  - A very short time period is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
  - 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.
- (b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:
  - Approval process and control are not strict.
  - 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.
  - Requirements may frequently change significantly.
  - Identification of non-functional elements is difficult to document.

- Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design with narrow focus that limits future system potential.
- Prototype may not have sufficient checks and balances incorporated.
- 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.
- 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.
- 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 weaknesses, 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.

#### 5.4.3 The Incremental Model

The Incremental 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. It is pictorially depicted in Fig. 5.4.3.

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 to ease the traumatic effect of introducing completely new system all at once. A few pertinent features are listed as follows:

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

## 5.14 Information Systems Control and Audit

---

- 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 (i.e. Working system).

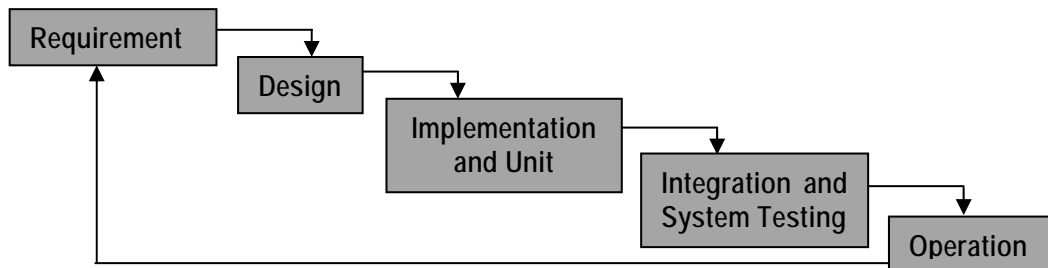


Fig. 5.4.3: Incremental Model

- (a) **Strengths:** Some of its strengths identified by the experts and practitioners include the following:
- Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
  - 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.
  - Stakeholders can be given concrete evidence of project status throughout the life cycle.
  - It is more flexible and less costly to change scope and requirements.
  - It helps to mitigate integration and architectural risks earlier in the project.
  - It allows the delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
  - Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organization is negatively impacted.
- (b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:
- 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.
  - Each phase of an iteration is rigid and do not overlap each other.
  - Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
  - Since some modules will be completed much earlier than others, well-defined interfaces are required.
  - It is difficult to demonstrate early success to management.

#### 5.4.4 Spiral Model

The Spiral model is a software development process combining elements of both design and prototyping-in-stages. It tries to combine advantages of top-down and bottom-up concepts. It combines the features of the prototyping model and the waterfall model (given in Fig. 5.4.4). The spiral model is intended for large, expensive and complicated projects. 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. A list of pertinent characterizing features includes the following:

- 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.
- 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.
- 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.
- A second prototype is evolved by a fourfold procedure by 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; and constructing and testing the second prototype.

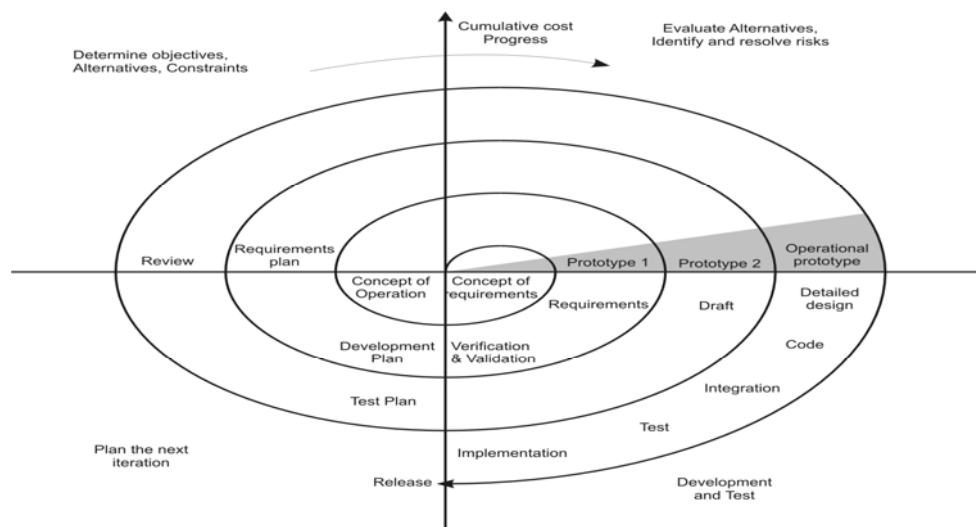


Fig. 5.4.4: Spiral Model

## 5.16 Information Systems Control and Audit

---

(a) **Strengths:** Some of its strengths identified by the experts and practitioners include the following:

- It enhances the risk avoidance.
- It is useful in helping for optimal development of a given software iteration based on project risk.
- It 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.

(b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:

- It is challenging to determine the exact composition of development methodologies to use for each iteration around the Spiral.
- It may prove highly customized to each project, and thus is quite complex and limits reusability.
- A skilled and experienced project manager is required to determine how to apply it to any given project.
- No established controls exist for moving from one cycle to another cycle. Without controls, each cycle may generate more work for the next cycle.
- There are no firm deadlines, cycles continue with no clear termination condition leading to, inherent risk of not meeting budget or schedule.

### 5.4.5 Rapid Application Development (RAD) Model

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. Key features include the following:

- Key objective is fast development and delivery of a high quality system at a relatively low investment cost,
- Attempts to reduce inherent project risk by breaking a project into smaller segments and providing more ease-of-change during the development process.
- 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.

- Key emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.
  - 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.
  - 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.
  - Active user involvement is imperative.
  - Iteratively produces production software, as opposed to a throwaway prototype.
  - Produces documentation necessary to facilitate future development and maintenance.
  - Standard systems analysis and design techniques can be fitted into this framework.
- (a) **Strengths:** Some of the strengths identified by the experts and practitioners include the following:
- The operational version of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks.
  - Because RAD produces systems more quickly and to a business focus, this approach tends to produce systems at lower cost.
  - Quick initial reviews are possible.
  - Constant integration isolates problems and encourages customer feedback.
  - It 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.
  - It concentrates on essential system elements from user viewpoint.
  - It provides for the ability to rapidly change system design as demanded by users.
  - It leads to a tighter fit between user requirements and system specifications.
- (b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:
- Fast speed and lower cost may affect adversely the system quality.
  - The project may end up with more requirements than needed (gold-plating).
  - Potential for feature creep where more and more features are added to the system over the course of development.

## 5.18 Information Systems Control and Audit

---

- It may lead to inconsistent designs within and across systems.
- It may call for violation of programming standards related to inconsistent naming conventions and inconsistent documentation,
- It may call for lack of attention to later system administration needs built into system.
- Formal reviews and audits are more difficult to implement than for a complete system.
- Tendency for difficult problems to be pushed to the future to demonstrate early success to management.
- Since some modules will be completed much earlier than others, well-defined interfaces are required.

### 5.4.6 Agile Model

This is an organized set of software development methodologies based on the *iterative and incremental* development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle. Agile Manifesto is based on following 12 features:

- Customer satisfaction by rapid delivery of useful software;
  - Welcome changing requirements, even late in development;
  - Working software is delivered frequently (weeks rather than months);
  - Working software is the principal measure of progress;
  - Sustainable development, able to maintain a constant pace;
  - Close, daily co-operation between business people and developers;
  - Face-to-face conversation is the best form of communication (co-location);
  - Projects are built around motivated individuals, who should be trusted;
  - Continuous attention to technical excellence and good design;
  - Simplicity;
  - Self-organizing teams; and
  - Regular adaptation to changing circumstances.
- (a) **Strengths:** Some of the strengths identified by the experts and practitioners include the following:
- Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.
  - The team does not have to invest time and efforts and finally find that by the time



they delivered the product, the requirement of the customer has changed.

- Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
- The documentation is crisp and to the point to save time.
- The end result is generally the high quality software in least possible time duration and satisfied customer.

(b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle.
- There is lack of emphasis on necessary designing and documentation.
- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
- Agile requires more re-work and due to the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
- The project can easily get taken off track if the customer representative is not clear about the final outcome.
- Agile lacks the attention to outside integration.

## 5.5 System Development Life Cycle (SDLC)

The System Development Life Cycle provides system designers and developers to follow a sequence of activities. It consists of a generic sequence 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, the processes 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 logical phase 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 given as follows:

- Better planning and control by project managers;
- Compliance to prescribed standards ensuring better quality;

## 5.20 Information Systems Control and Audit

---

- Documentation that SDLC stresses on is an important measure of communication and control; and
- 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:

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

Some of the shortcomings and anticipated risks associated with the SDLC are as follows:

- The development team may find it cumbersome.
- The users may find that the end product is not visible for a long time.
- The rigidity of the approach may prolong the duration of many projects.
- 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 as a set of activities that analysts, designers and users carry out to develop and implement an information system. In most of the business situations, these activities are 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 5.5.1 describes the activities of all the phases involved in the System Development Life Cycle.

**Table 5.5.1: System Development Life Cycle**

PHASE	PHASE NAME	NATURE OF ACTIVITY
1.	Preliminary Investigation	Determining and evaluating the strategic feasibility of the system and ensure that the solution fits the business strategy.
2.	Systems Requirements Analysis	Analyzing the typical system requirements, in view of its functionalities, deliverables etc.
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 Acquisition	Acquisition of Operating infrastructure including hardware, software and services.
5.	Systems Development	Developing the system as per the system designed in view of its adequate implementation to lead to fulfillment of requirements to the satisfaction of all the stakeholders.
6.	Systems Testing	Requisite testing to ensure the valid and reliable implementations.
7.	Systems Implementation	Operationalization of the developed system for the acceptance by management and user before migration of the system to the live environment and data conversion from legacy system to the new system.
8.	Post Implementation Review and Maintenance	Continuous evaluation of the system as it functions in the live environment and its updation / maintenance.

### 5.5.1 Preliminary Investigation

It is predominantly aimed 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. The deliverable of the preliminary investigation includes a report including feasibility study observations.

A preliminary investigation is normally initiated by some sort of system request. The steps involved in the preliminary investigation phase are Identification of Problem, Identification of objectives, Delineation of scope, and Feasibility Study. Thereby, it largely enables the requirements engineer to tackle the issues and Feasibility Study for the following:

- Determine whether the solution is as per the business strategy;
- Determine whether the existing system can rectify the situation without a major modification;
- Define the time frame for which the solution is required;
- Determine the approximate cost to develop the system; and
- Determine whether the vendor product offers a solution to the problem.

**(i) Identification of Problem:** The first step in an application development is to define the problem clearly and precisely, which is done only after the critical study of the existing system and 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

## 5.22 Information Systems Control and Audit

---

manager might want access to specific new information that s/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 perform 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 feasibility. 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; and
- Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.

**(ii) Identification of Objectives:** After the identification of the problem, it is easy to work out and precisely specify 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, one of the objectives was 'to introduce a system wherein intending passengers could book a ticket from source to destination, faster than in real-time'.

**(iii) Delineation of Scope:** The scope of a solution defines its typical boundaries. It should be clear and comprehensible to the user management stating the extent and '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 and proves quite handy. The typical scope determination may be performed on the following dimensions:

- **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 and probability of failure-free operations. The reliability required for an application depends on its criticality and the user profile.

Moreover, while eliciting information to delineate the scope, few aspects needs to be kept in mind:

- Different users may 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 be met with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle it may have 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 weightage too. These factors are 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 factor like the economic benefits that entail.

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

- **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, an analyst may try to know how does the inventory department operates and who are the managers and supervisors. Analysts can usually

## 5.24 Information Systems Control and Audit

---

learn these details by examining organization charts and studying written operating procedures.

- **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.

(iv) **Feasibility Study:** After possible solution options are identified, project feasibility i.e. 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 described briefly as follows:

- **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?

The detailed description of each dimension is given as follows:

(a) **Technical Feasibility:** It may try to answer, whether implementation of the project viable using current technology? 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 inquiries, 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?

Some of the technical issues to be considered are given in the Table 5.5.2 below.

Table 5.5.2: Technical Issues

Design Considerations	Design Alternatives
Communications Channel configuration	Point to point, multidrop, or line sharing
Communications Channel	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

- (b) **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.
- (c) **Economic Feasibility:** 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:
- The cost of conducting a full systems investigation;

## 5.26 Information Systems Control and Audit

---

- The cost of hardware and software for the class of applications being considered;
- The benefits in the form of reduced costs or fewer costly errors; and
- The cost if nothing changes (i.e. the proposed system is not developed).

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

- (d) **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.
- (e) **Resources Feasibility:** This focuses on human resources. Implementing sophisticated software solutions becomes difficult at specific locations because of the reluctance of skilled personnel to move to such locations.
- (f) **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, may include the following:
- 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 is to be implemented. In general, the greater the requirements for change in the user environment in which the system will be installed, greater is the risk of implementation failure.

- (g) **Behavioral Feasibility:** It refers to the systems, which is to 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.
- (h) **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 is liable to violate the local legal requirements, should also be rejected. For example, a revised system should comply with all applicable statutes about financial and statutory reporting requirements, as well as the company's contractual obligations.



(v) **Reporting Results to Management:** After the analyst articulates the problem, defines the same along with its scope, s/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 covering letter of intent 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 may get 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.

(vi) **Internal Control Aspects:** Management implements proper internal control to ensure business objectives. As defined in section 217(2AA), Companies Act, 1956, Directors are responsible to have proper internal control for a company. In terms of system development, controls need to be well in place during the development of system. In systems, it is not possible to put in place controls post development. A better understanding of controls during planning and effective implementation of those controls shall help to achieve the above stated objectives.

For validating control aspects in system, entity may have an internal audit team. Few large software developers engage outside experts for the same. To check controls internally or through external auditor depends on size and nature of entities of the business. The same is also dependent upon management's attitude. Review by external consultant is more independent. External consultant may bring his/her expertise to entity. The flip side is that external consultant may be costly; secrecy is also a fact to consider. However, the key control queries regarding various aspects at this stage may include the following:

- Whether problem definition is proper?
- Whether all feasibility studies have been properly done?
- Whether results of feasibility studies have been documented?
- Whether management report submitted reflects the outcome of feasibility studies done?

### 5.5.2 System Requirements Analysis

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 objectives are performed in this phase in order to generate the deliverable, Systems Requirements Specification (SRS):

- 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;

## 5.28 Information Systems Control and Audit

---

- To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

In order to accomplish the aforementioned objectives, a series of steps are taken. Such steps result in process, assuring appropriate systems requirements analysis. A generic set of process are described as follows:

**(i) Fact Finding:** 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 services to customers. To assess these needs, the analysts often interact extensively with people, who will be benefited from the system in order to determine 'what are their actual requirements'. Various fact-finding techniques/tools are used by the system analyst for determining these needs/requirements are briefly discussed below:

- **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.
- **Questionnaires:** Users and managers are asked to complete questionnaire about the information systems 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.
- **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide system developers with a larger picture of the problems and opportunities. Interviews also give analyst the opportunity to observe and record first-hand user reaction and to probe for further information.
- **Observation:** In general and particularly 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.

**(ii) 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 that should be intensive in order to fully understand the present system and its related problems. The following areas should be studied in depth:

- **Reviewing Historical Aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts enable to identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts 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 equipment and techniques.
- **Analyzing 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 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, s/he will be able to determine how these inputs fit into the framework of the present system.
- **Reviewing Data Files:** 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.
- **Reviewing 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. S/he must review the types of data communication equipment 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.
- **Analyzing Outputs:** The outputs or reports should be scrutinized carefully by the system

### 5.30 Information Systems Control and Audit

---

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 is it kept on file, etc. must be investigated. Often, many reports are a carry-over from earlier days and have little relevance to current operations. Attempts should be made to eliminate all such reports in the new system.

- **Reviewing Internal Controls:** A detailed investigation of the present information system is not complete until internal control mechanism 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.
- **Modeling the Existing 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 processes must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps to disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- **Undertaking Overall Analysis of the Existing 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 costs-benefits of each of these must be investigated thoroughly.

**(iii) System Analysis of Proposed Systems:** After a thorough analysis of each functional area of the present information system, 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 should be in conformity with the project's objectives articulated and in accordance with the following:

- Outputs are produced with great emphasis on timely managerial reports that utilize the management by exception' principle.
- Databases are maintained with great accent on online processing capabilities.
- Input data is 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, utilize data communications as, when and where deemed appropriate.
- Work volumes and timings are 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.

**(iv) 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 primarily for the following:

- To conceptualize, clarify, document and communicate the activities and resources involved in the organization and its information systems;
- To analyze present business operations, management decision making and information processing activities of the organization; and
- To 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 specification or representations can be classified into four categories based on the systems features. These are described briefly as follows:

- **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.
- **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. It documents the flows among different display screens generated by alternative end user responses to menus and prompts.
- **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

## 5.32 Information Systems Control and Audit

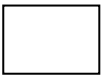



input/output or storage media of a system.

- **Detailed System Processes:** These tools are used to help the programmer to 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.

It is clear from the foregoing description that a number of CASE tools are in use for typical representation, specifications and system modeling. A set of the prominent tools have been already mentioned categorically and some are being described in detail as follows:

- Structured English:** Structured English, also known as Program Design Language (PDL), 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. A better structured, universal and precise tool is referred to as pseudo code.
- Flowcharts:** Flowcharting is a pictorial representation technique that can be used by analysts to represent the inputs, outputs and processes of a business process. 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.
- 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 5.5.3. These four symbols are combined to show how data are processed.

**Table 5.5.3: Data Flow Diagram Symbols**

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.

- (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.
- (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, s/he is liable to miss some of the branches. The four parts of the decision table are given as follows:
- **Condition Stub** – This comprehensively lists the comparisons or conditions;
  - **Action Stub** – This comprehensively lists the actions to be taken along various program branches;
  - **Condition entries** – This list in its various columns the possible permutations of answer to the questions in the conditions stub); and
  - **Action entries** – This lists in its columns corresponding to the condition entries the actions contingent upon the set of answers to questions of that column.
- (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 5.5.4 illustrates the use of a system component matrix to document the basic components of a sales processing and analysis system in an organization.

## 5.34 Information Systems Control and Audit

Table 5.5.4: A System Component Matrix

Information system Activities	Hardware Resources		Software Resources		People Resources		Data Resources	Information Products
	Machines	Media	Programs	Procedures	Specialists	Users		
Input	POS Terminals	Bar tags, Mag Stripe Cards	Data Entry program	Data Entry procedures		Sales clerks customers	Customer data, product data	Data entry displays
Processing	Mainframe Computer		Sales processing program, sales analysis program	Sales transaction procedures	Computer operators	Sales clerks managers	Customer inventory and sales databases	Processing status displays
Output	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
Storage	Magnetic Disk Drives	Magnetic disk packs	Database management system program		Computer operators		Customer, inventory and sales databases	
Control	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

- (h) **Data Dictionary:** A data dictionary 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 record in the data dictionary. Similarly, when new computer programs are created that access data items in existing files, the data dictionary is updated to indicate the data items the 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. 5.5.5 shows a sample record from a generic data dictionary, which is basically a file about data. Each file record contains information about one data field used in other files or metadata of the system.



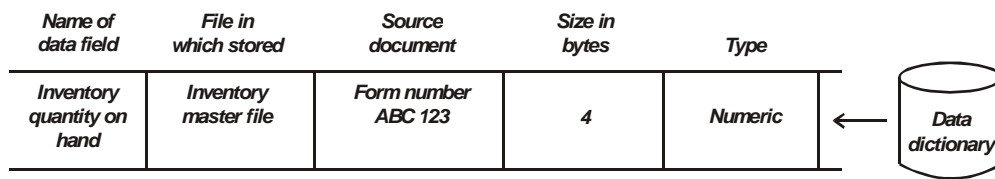


Fig. 5.5.5: Example of Data Dictionary

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help to 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 participates 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) **User Interface Layout and Forms:** Several type layout forms for both soft and hard copy are used to model input/output components of an automated information system. Some of the prominent and inevitable ones are described briefly as follows:
- **Layout form and Screen Generator:** These are for printed report used to format or “paint” the desired layouts and contact without having to enter complex formatting information. Fig. 5.5.6 shows a Layout screen for the design of 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.

<b>Customer Order Report</b>				
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. 5.5.6: Layout screen for the design of a display for a customer order report

(v) **Systems Specification:** At the end of the analysis phase, the systems analyst prepares a document called **Systems Requirement Specifications (SRS)**. A well documented SRS may normally contain the following sections:

- **Introduction:** Goals, Objectives, software context, Scope and Environment of the computer-based system.
- **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.
- **Appendices:** Data flow/Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review:** 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, the user should sign the document. This is a technical requirement of the contract between users and development team/organization.

(vi) **Roles Involved in SDLC:** A variety of tasks during the SDLC are performed by special teams/committees/individuals based on requisite expertise as well as skills. Some of the generic roles are described as follows:

- (a) **Steering Committee:** It is a special high power committee of experts to accord approvals for go-ahead and implementations. Some of the functions of Steering Committee are given as follows:
- To provide overall directions 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; and
  - To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

- (b) **Project Manager:** A project manager is normally responsible for more than one project and liaising with the client or the affected functions. S/he is responsible for delivery of the project deliverables within the time/budget and periodically reviews the progress of the project with the project leader and his/her team.
- (c) **Project Leader:** The project leader is dedicated to a project, who has to ensure its completion and fulfillment of objectives. S/he reviews the project status more frequently than a Project Manager and the entire project team reports to him/her.
- (d) **Systems Analyst / Business Analyst:** The systems analysts' main responsibility is to conduct interviews with users and understand their requirements. S/he is a link between the users and the designers/programmers, who convert the users' requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.
- (e) **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.
- (f) **Programmer/Developers:** 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, they also test the program for debugging activity to assure correctness and reliability
- (g) **Database Administrator:** 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.
- (h) **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.
- (i) **Testers:** Testers are a junior level quality assurance personnel attached to a project, who test programs and subprograms as per the plan given by the module / project leaders and prepare test reports.
- (j) **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.

## 5.38 Information Systems Control and Audit

---

(k) **IS Auditor:** As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. S/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.

(vii) **Internal Controls:** Requirements phase is the most important phases of SDLC. The issue of controls is very important here also. Some of the key control aspects at this stage may be taken care by the following queries:

- Whether present system analysis has been properly done?
- Whether appropriate domain, were expert was engaged?
- Whether all user requirements of proposed system have been considered?
- Whether SRS document has been properly made and vetted by Users, Domain Experts, System Analysts?

### 5.5.3 System Designing

After the completion of requirements analysis for a system, systems designing activity takes place for the most feasible and optimal alternative, which is selected by management. The objective is to design an Information System that best satisfies the users/managerial requirements. It describes the parts of the system and their interaction. It sets out how the system shall be implemented using the chosen hardware, software and network facilities. It also specifies the program and the database specifications and the security plans and further specifies the change control mechanism to prevent uncontrolled entry of new requirements.

The key and generic 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.

Design phase documents/deliverables include 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 guides the programmers about 'what the system should do and how to implement'. 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 activities includes Architectural Design; Design of the Data / Information Flow; Design of the Database; Design of the User-interface; Physical Design; and Design and acquisition of the hardware/system software platform', which are described briefly as follows:

- (a) **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; functions 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. 5.5.7. 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.

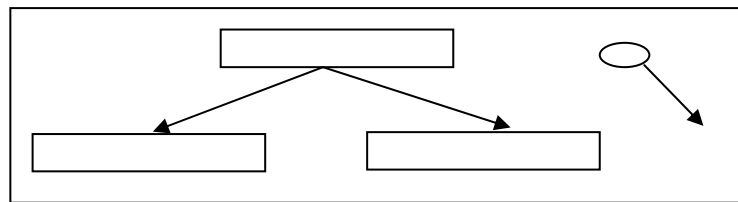


Fig. 5.5.7: Functional Decomposition Tool

- (b) **Design of Data/Information flow:** The design of the data and information flow 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).
- (c) **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 design of the database involves four major activities, which are shown in Table 5.5.5.

Table 5.5.5: Major Activities in Database Designing

Design Activity	Explanation
Conceptual Modeling	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.
Data Modeling	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.
Storage Structure Design	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.

#### 5.40 Information Systems Control and Audit

<b>Physical Design</b>	<b>Layout</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.
------------------------	---------------	--

- (d) **User Interface Design:** It 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.

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 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. The output from an information system should accomplish one or more of the following objectives including to convey information about past activities, current status or projections of the future, signal important events, opportunities, problems or warnings, trigger an action, and confirmation of an action.

Important factors in Input/Output design are listed in Table 5.5.6, which should be considered by the system analyst while designing user input/ output forms.

**Table 5.5.6: Factors affecting Input / Output Form Designs**

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	Data needs to be inputted to computer	A sales manager, may be requiring a

	need outputs, which may be required on a regular, periodic basis - perhaps daily, weekly, monthly, at the of quarter or annually.	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.	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.
<b>Format</b>	Input format refers to the manner in which data are physically arranged. Output format refers to the arrangement referring to data output on a printed report or in a display screen.	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.).	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.
<b>Media</b>	Input-output medium refers to the physical device used for input, storage or output.	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, keyboards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.	A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape/disk and voice output.
<b>Form</b>	Form refers to the way the information is	Forms are pre-printed papers that require people to fill in	The form of the output should be decided keeping in

## 5.42 Information Systems Control and Audit

	inputted in the input form and the content is presented to users in various output forms - quantitative, non-quantitative, text, graphics, video and audio.	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.	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.
<b>Input Volume/ Output Volume</b>	Input volume refers to the amount of data that has to be entered in the computer system at any one time. The amount of data output required at any one time is known as output volume.	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.	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.

- (e) **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.

Some of the generic design principles being applied to develop the design of typical information systems include the following:



- 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, with high cohesion and low coupling.

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

- (f) **System's Operating Platform:** In some cases, the new system requires an operating platform including hardware, network 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 for requisite provisions. 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.
- (g) **Internal Design Controls:** From internal control point of view, this phase is also an important phase as all internal controls are placed in system during this phase. The key control aspects at this stage include the following:
- Whether management reports of stage I and stage II, were referred by System Designer?
  - Whether all control aspects have been properly covered?
  - Whether controls put in place in system, appear in the documentation done at this stage?
  - Whether a separate review of design document has been done by internal auditor?

#### 5.5.4 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 operating infrastructure including hardware, software

#### 5.44 Information Systems Control and Audit

---

and services. Such acquisitions are highly technical and cannot be taken easily and for granted. Thereby, technical specifications, standards etc. come to rescue.

**(a) Acquisition Standards:** Management should establish acquisition standards that address the security and reliability issues as per current state-of-the-art development standards. Acquisition standards should focus on the following:

- 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;
- Invitations-to-tender soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software;
- Request-for-proposals soliciting bids when acquiring off-the-shelf or third-party developed software; and
- Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

**(b) 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. A sub-committee of experts under the steering committee, referred to as 'System Acquisition Committee' is constituted. The sub-committee is mandated to ensure timely and effective completion of this stage.

The next aspect is call for Request For Proposal (RFP) from vendors. This stage is one of the most critical phases for system acquisition; as well defined RFP leads to better acquisition. RFP, means asking vendors to submit proposals for the requirements mentioned. RFP process is the initiation of final stages for implementation. The requirements analysis and design phase have been completed, before starting of this phase. The following considerations are valid for both acquisition of hardware and software:

- **Vendor Selection:** This step is a critical step for success of process of acquisition of systems. It is necessary to remember that vendor selection is to be done prior to sending RFP. The result of this process is that 'RFP are sent only to selected vendors'. For vendor selection, following things are kept in mind including the background and location advantage of the vendor, the financial stability of vendor, the market feedback of vendor performance, in terms of price, services etc.
- **Geographical Location of Vendor:** The issue to look for whether the vendor has local support persons. Otherwise, the proposals submitted by vendor not as per RFP requirements need to be rejected, with no further discussion on such rejected proposals. This stage may be referred to as 'technical validation', that is to check the proposals submitted by vendors, are technically complying with RFP requirements.

- **Presentation by Selected Vendors:** All vendors, whose proposals are accepted after "technical validation", are allowed to make presentation to the System Acquisition Team. The team evaluates the vendor's proposals by using techniques.
- **Evaluation of Users Feedback:** The best way to understand the vendor systems is to analyze the feedback from present users. Present users can provide valuable feedback on system, operations, problems, vendor response to support calls.

Besides these, some specific considerations for hardware and software acquisition are described as follows:

- The benchmark tests to be done for proposed machine. For hardware's, there are specified standard benchmark tests defined based on the nature of hardware. These need to be applied to proposed equipment.
- Software considerations that can be current applications programs or new programs that have been designed to represent planned processing needs.
- The benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer.
- The benchmarking problems would then comprise long jobs, short jobs, printing jobs, disk jobs, mathematical problems, input and output loads etc., in proportion typical of the job mix.
- If the job is truly represented by the selected benchmarking problems, then this approach can provide a realistic and tangible basis for comparing all vendors' proposals.
- Tests should enable buyer to effectively evaluate cross performance of various systems in terms of hardware performance (CPU and input/output units), compiler language and operating system capabilities, diagnostic messages, ability to deal with certain types of data structures and effectiveness of software utilities.
- Benchmarking problems, however, suffer from a couple of disadvantages. It takes considerable time and efforts to select problems representative of the job mix which itself must be precisely defined. It also requires the existence of operational hardware, software and services of systems. Nevertheless, this approach is very popular because it can test the functioning of vendors' proposal. The manager can extrapolate in the light of the results of benchmarking problems, the performance of the vendors' proposals on the entire job mix.

(c) **Other Acquisition Aspects and Practices:** On addition to the above, there are several other acquisition aspects and practices also, which are given as follows:

(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

## 5.46 Information Systems Control and Audit

---

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 is 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 usage 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 rights. 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 system;
- The Maintainability of each proposed system;
- The Compatibility of each proposed system with Existing Systems; and
- Vendor Support.

**(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 given as follows:

- **Checklists:** It is the most simple and 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 and Software.

- 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. Table 5.5.7 illustrates a Point Scoring Analysis list.

Table 5.5.7: 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
<b>Totals</b>	123	94	106	85

- Public Evaluation Reports:** Several consultancy as well as independent 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, reports would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts.
- Benchmarking Problems related Vendor's Solutions:** Benchmarking problems related to vendors' proposals are accomplished by sample programs that represent at least a

part of the buyer's primary work load and include considerations and can be current applications that have been designed to represent planned processing needs. That is, benchmarking problems are oriented towards testing whether a solution offered by the vendor meets the requirements of the job on hand of the buyer.

- **Testing 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 judgment can be made. It must be borne in mind, however that various capabilities to be tested would have to be assigned relative weightage.

### 5.5.5 System Development : Programming Techniques and Languages

This phase is supposed to convert the design specifications into a functional system under the planned operating system environments. Application programs are written, tested and documented, conduct system testing. Finally it results into a fully functional and documented system. A good coded application and programs should have the following characteristics:

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data, subsequently could result in the failure of a program after some time.
- **Robustness:** It refers to the applications' strength to uphold its operations in adverse situations by 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 per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

Other related aspects of this phase are given as follows:

- (a) **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, interoperability, compatibility, efficient utilization of resources and least processing time.

(b) **Programming Language:** Application programs are coded in the form of statements or instructions and the same is converted by the compiler to object code for the computer to understand and execute. The programming languages commonly used are given as follows :

- High level general purpose programming languages such as COBOL and C;
- Object oriented languages such as C++, JAVA etc.;
- Scripting language such as JAVAScript, VBScript; and
- Decision Support or Logic Programming languages such as LISP and PROLOG.

The choice of a programming language may depend on various pertinent parameters. In general, language selection may be made 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.

(c) **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:

- Giving input the source program to the compiler,
- Letting the compiler to find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as input to the compiler.

(d) **Testing the Programs:** 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 of all the possible exceptions. The test plan should require the execution of all standard processing logic based on chosen testing strategy/techniques. 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 finding the faults and debugging.

(e) **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 both internal and external documentation in order to ensure

## 5.50 Information Systems Control and Audit

---

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.

- (f) **Program Maintenance:** The requirements of business data processing applications are subject to periodic change. This calls for modification of various programs. There are usually separate categories of programmers called maintenance programmers, who are entrusted with this task.

### 5.5.6 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 with a minimum amount of efforts. 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/facets of Testing are described as follows.

(i) **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 component of the program and show that they 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. Such typical tests are described as follows:

- **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 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.

In terms of techniques, Unit Testing is classified as Static Analysis Testing and Dynamic Testing. Such typical testing techniques are elaborated as follows:

- (a) **Static Testing:** Static Analysis Tests are conducted on source programs and do not normally require executions in operating conditions. Typical static analysis techniques include the following:
- **Desk Check:** This is done by the programmer him/herself. S/he checks for logical syntax errors, and deviation from coding standards.
  - **Structured Walk Through:** The application developer leads other programmers to scan through the text of the program and explanation to uncover errors.
  - **Code Inspection:** The program is reviewed by a formal committee. Review is done with formal checklists.
- (b) **Dynamic Analysis Testing:** Such testing is normally conducted through execution of programs in operating conditions. Typical techniques for dynamic testing and analysis include the following:
- **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 typical inputs including simple, extreme, valid and invalid input-cases and executes to uncover errors. There is no knowledge of the test object's internal structure.  
  
This method of test design is applicable to all levels of software testing i.e. 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:** It 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:** It 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.

**(ii) 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 validity of 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 two manners:

- **Bottom-up Integration:** It 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:** It 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 into 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 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 or any modification made in the software, it 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 faults. The data used for the regression tests should be the same as the data used in the original test.

**(iii) System Testing:** It 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 liable to be properly performed, in actual failures
- **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, availability authentication, authorization, 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.

(iv) **Final Acceptance Testing:** It 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 policy, methodology and prescriptions.
- **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 described as follows:
  - **Alpha Testing:** This is the first stage, often performed by the users within the organization by the developers, to improve and ensure the quality/functionality as per users satisfaction.
  - **Beta Testing:** This is the second stage, generally performed after the deployment of the system. It is performed by the external users, during the real life execution of the project. It normally involves sending the product outside the development environment for real world exposure and receives feedback for analysis and modifications, if any.

## 5.54 Information Systems Control and Audit

---

(v) **Internal Testing Controls:** There are several controls that can be exercised internally to assure the testing phase quality and efficiency. Though it varies from one organization to another, some of the generic key control aspects appear to be addressed by the responses to following queries:

- Whether the test-suite prepared by the testers includes the actual business scenarios?
- Whether test data used covers all possible aspects of system?
- Whether CASE tools like 'Test Data Generators' have been used?
- Whether test results have been documented?
- Whether test have been performed in their correct order?
- Whether modifications needed based on test results have been done?
- Whether modifications made have been properly authorized and documented?

### 5.5.7 System Implementation

In order to finally deploy or implement the new system in the real operating environment, several activities are undertaken. In terms of the output of the phase, a fully functional as well as documented system is a prerequisite. Moreover, many other issues including defect removal, maintenances, reengineering etc. may also be in place to assure the desirable quality control of the system in its true operational environment. Some of the generic key activities involved in System Implementation include the following:

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

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. Some of the generic activities involved in system implementation stage are described briefly 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:

- **Site Preparation:** An appropriate location/ambiance as prescribed and the typical

equipment must be availed to provide an operating environment for the equipment that will meet the vendor's temperature, humidity and dust control specifications etc.

- **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 operating environment may be desirable to prove end to end connectivity.
  - **Equipment Checkout:** The equipment must be turned on for testing under normal operating conditions. Though the routine 'diagnostic tests' should be run by the vendor, the implementation in-house team should devise and run extensive tests of its own to ensure that equipment functionalities in actual working conditions.
- (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. Such training structure should be highly formalized and be based business process executions with actual data.
- (iii) **System Change-Over Strategies:** Conversion or changeover is the process of changing over or shifting over from the old system (may be the manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover, as it may put many resources/assets/operations at risk. The Four types of popular implementation strategies are described as follows:
- **Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Fig 5.5.8 (i) 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.

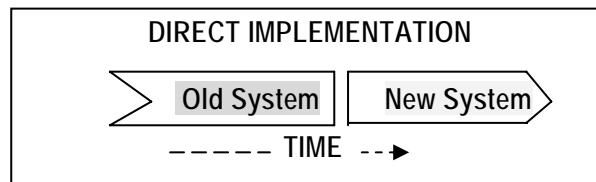


Fig. 5.5.8 (i): Direct Changeover

- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and used by employees whilst other files continue to be used on

the old system i.e. the new is brought in stages (phases). If a 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. 5.5.8(ii).

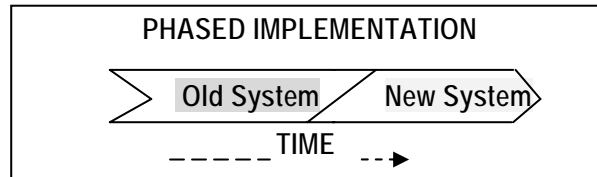


Fig. 5.5.8 (ii): Phased Changeover

- **Pilot Changeover:** 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. 5.5.8 (iii) depicts Pilot Implementation.

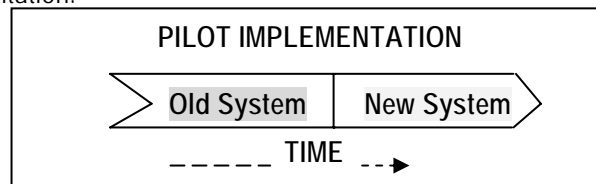


Fig. 5.5.8 (iii): Pilot Changeover

- **Parallel Changeover:** 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. 5.5.8 (iv) shows parallel implementation.

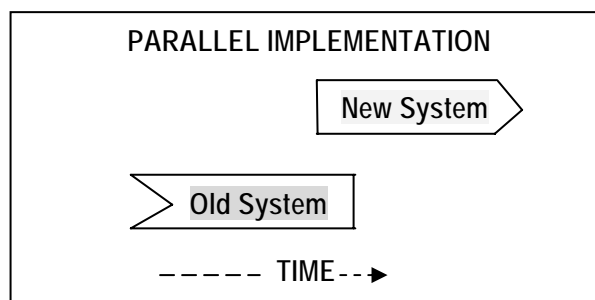


Fig. 5.5.8 (iv): Parallel Changeover

- (iv) Such requisite changeover or Conversion includes all those activities, which must be completed to successfully convert from the previous system to the new information system. Fundamentally these technical activities can be classified as follows:

- **Procedure Conversion:** Operating procedures should be carefully completed with sufficient-enough documentation for the new system. It 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.
- **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.
- **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, matching and balancing the total results of both systems.
- **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, 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 period/month should provide sufficient computer time to handle all required processing.

#### 5.5.8 Post Implementation Review and Systems Maintenance

In order to assess, review and assure the complete working solution, a number of activities may be planned. As no phase may be assured to be perfect, errors are liable to occur. Therefore, a well-formalized review must be undertaken including some of the systems maintenance activities, such as adding new data elements, modifying reports, adding new reports; and changing calculations. As the deliverable of this phase, a well written document stating observations, modifications, controls, scope of further improvements etc. may be prepared. Such aspects may also be availed in the form of responses to following queries:

- 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?

(i) **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. Typical evaluations include the following:

- **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 record 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.
- **Operational Evaluation:** The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties. It tries to answer the questions related to functional aspects of the system. Such an 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 or generates. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operational evaluations. The objective of an information system is to provide information to a considerable extent 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.



(ii) **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 at regular intervals. Most of the information systems require at least some modification after development. The need for modification arises from a failure to anticipate/capture all the requirements during system analysis/design and/or from changing organizational requirements. Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting 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 during the executions. 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 the 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 with the 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.

## 5.6 Operation Manuals

It is typical user's guide, also commonly known as Operations Manual. Moreover, it may be a technical communication document intended to give assistance to people using a particular

## 5.60 Information Systems Control and Audit

---

system. It is usually written by technical writers, although user guides are written by programmers, product or project managers, or other technical staff, particularly in smaller companies. These are most commonly associated with electronic goods, computer hardware and software. The section of an operation manual will 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 generic operations manual could be as shown in Table 5.6.1:

**Table 5.6.1: Sample Format of Operations Manual**

<p>1.0 General Information</p> <p>1.1 System Overview</p> <p>1.2 Project References</p> <p>1.3 Authorized Use Permission</p> <p>1.4 Points of Contact</p> <p>1.4.1 Information</p> <p>1.4.2 Coordination</p> <p>1.4.3 Help Desk</p> <p>1.5 Organization of the Manual</p> <p>1.6 Acronyms and Abbreviations</p> <p>2.0 System Operations Overview</p> <p>2.1 System Operations</p> <p>2.2 Software Inventory</p> <p>2.3 Information Inventory</p> <p>2.3.1 Resource Inventory</p> <p>2.3.2 Report Inventory</p> <p>2.4 Operational Inventory</p> <p>2.5 Processing Overview</p> <p>2.5.1 System Restrictions</p> <p>2.5.2 Waivers of Operational Standards</p> <p>2.5.3 Interfaces with Other Systems</p> <p>2.6 Communications Overview</p> <p>2.7 Security</p>	<p>3.0 Run Description</p> <p>3.1 Run Inventory</p> <p>3.2 Run Description</p> <p>*3.2.x [Run Identifier]</p> <p>3.2.x.1 Run Interrupt Checkpoints</p> <p>3.2.x.2 Set-Up and Diagnostic Procedures</p> <p>3.2.x.3 Error Messages</p> <p>3.2.x.4 Restart / Recovery Procedures</p> <p>* 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>
--	--

## 5.7 Auditors' Role in SDLC

The audit of systems under development can have three main objectives. It is primarily aimed to provide an opinion on the efficiency, effectiveness, and economy of project management. An auditor's role is to assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored; and the effectiveness of controls being enacted for the management of the system's operation.

In order to achieve these goals, an auditor has to attend project and steering committee meetings and examine project control documentation and conducting interviews. This is to ensure 'what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved. For addressing the second objective, the auditor can examine system documentation such as functional specifications to arrive at an opinion on controls. The auditor's opinion will be based on the degree to which the system satisfies the general control objectives that any information system should meet. A list of such objectives should be provided to the auditor. The auditor should provide a list of the standard controls, over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria.

An Auditor may adapt a rating system such as on a scale of 1 to 10 in order to give rating to the various phases of SDLC. While rating a Feasibility Study, an auditor can review Feasibility Study Report and different work products of this study phase. An interview with personnel, who have conducted this feasibility study, can be conducted. Depending on the content and quality of the Feasibility Study report and interviews, an auditor can arrive at a rating between 1 to 10 (10 being best). After deriving such a rating for all the phases, the auditor can form his/her overall opinion about the SDLC phases.

Moreover, in order to audit technical work products (such as database design or physical design), auditor may opt to include a technical experts to seek his/her opinion on the technical aspects of SDLC. However, auditor will have to give control objectives, directives and in general, validate the opinion expressed by technical experts. Some of the control considerations for an auditor include the following:

- Documented policy and procedures;
- Established Project team with all infrastructure and facilities ;
- Developers/ IT managers are trained on the procedures ;
- Appropriate approvals are being taken at identified mile-stones;
- Development is carried over as per standards, functional specifications;
- Separate test environment for development/ test/ production / test plans;
- Design norms and naming conventions are as per standards and are adhered to;
- Business owners testing and approval before system going live;
- Version control on programs;
- Source Code is properly secured;

## 5.62 Information Systems Control and Audit

---

- Adequate audit trails are provided in system; and
- Appropriateness of methodologies selected.

Further, Post-Implementation Review is performed to determine whether the system adequately meets earlier identified business requirements and needs (in feasibility studies or Requirements Specifications). Auditors should be able to determine if the expected benefits of the new system are realized and whether users are satisfied with the new system. In post implementation review, auditors need to review which of the SDLC phases have not met desired objectives and whether any corrective actions were taken. If there are differences between expectations and actual results, auditors need to determine the reasons for the same. Such discrepancies may be due to incomplete user requirements or any other shortcoming. Such reasons can help auditors to evaluate the current situation and offer guidelines for future projects.

In order to formalize the auditors' role and practices, a master checklist may be prepared. Such checklists may prove handy and highly beneficial to ensure an appropriate acquisition and / or development of information systems including software, and to maintain the information systems in an appropriate manner. The following sample checklist may be used by the IS Auditors for this purpose:

S. No.	Checkpoints	Status
1.	Whether information system acquisition and / or development policy and procedure documented?	
2.	Whether system acquisition and / or development policy and procedure approved by the management?	
3.	Whether the policy and procedure cover the following: <ul style="list-style-type: none"> <li>• Problems faced in the existing system and need for replacement</li> <li>• Functionality of new IS</li> <li>• Security needs</li> <li>• Regulatory compliance</li> <li>• Acceptance Criteria</li> <li>• Proposed roles and responsibilities</li> <li>• Transition/ Migration to new IS</li> <li>• Interfaces with legacy systems</li> <li>• Post implementation review</li> <li>• Maintenance arrangements.</li> </ul>	
4.	Whether policy and procedure documents are communicated / available to the respective users?	
5.	Whether policy and procedure documents are reviewed and updated at regular intervals?	
6.	Whether the organization has evaluated requirement and functionalities of proposed IS? <i>(Verify the requirements analysis conducted at three levels viz. process level, application level and organization level. Verify the site visit</i>	

	<i>reports and other customer references obtained with respect to functionalities of proposed IS).</i>	
7.	Whether the organization carried out feasibility study in respect of the following <ul style="list-style-type: none"> <li>• Financial feasibility</li> <li>• Operational feasibility</li> <li>• Technical feasibility</li> </ul>	
8.	Whether the selection of vendor and acquisition terms considers the following: <ul style="list-style-type: none"> <li>• Evaluation of alternative vendors</li> <li>• Specification on service levels and deliverables</li> <li>• Penalty for delays</li> <li>• Escrow mechanism for Source codes</li> <li>• Customization</li> <li>• Upgrades</li> <li>• Regulatory Compliance</li> <li>• Support and maintenance.</li> </ul>	
9.	Whether the organization has identified and assigned roles in development activities to appropriate stakeholders? <i>(Verify the assigned roles should be on "need to know" and "need to basis". and duties of developers and operators are segregated).</i>	
10.	Whether the organization has a separate development, test and production environments?	
11.	Whether the IS developed plan is prepared and approved by the management? <i>(Verify that IS development plan to include:</i> <ul style="list-style-type: none"> <li>• <i>Input data elements,</i></li> <li>• <i>Validations controls viz. Field/ Transactions/ File with appropriate error reporting</i></li> <li>• <i>Process workflow</i></li> <li>• <i>data classifications with security are in place, viz. Read only for users, Read/ Write for authorized persons</i></li> <li>• <i>Output).</i></li> </ul>	
12.	Whether the testing of IS includes: <ul style="list-style-type: none"> <li>• Confirms the compliance to functional requirements</li> <li>• Confirms the compatibility with IS infrastructure</li> <li>• Identifies bugs and errors and addresses them by analyzing root causes</li> </ul> Escalating functionality issues at appropriate levels.	
13.	Whether the adequate documentation for: <ul style="list-style-type: none"> <li>• Preserving test results for future reference</li> </ul>	

## 5.64 Information Systems Control and Audit

	<ul style="list-style-type: none"> <li>• Preparation of manuals like systems manual, installation manual, user manual</li> <li>• Obtaining user sign off / acceptance</li> </ul>	
14.	<p>Whether the implementation covers the following?</p> <ul style="list-style-type: none"> <li>• User Departments' involvement and their role</li> <li>• User Training</li> <li>• Acceptance Testing</li> <li>• Role of Vendor and period of Support</li> <li>• Required IS Infrastructure plan</li> <li>• Risk involved and actions required to mitigate the risks</li> <li>• Migration plan</li> </ul>	
15.	<p>If the development activities are outsourced, are the outsourcing activities evaluated based on the following practices:</p> <ul style="list-style-type: none"> <li>• What is the objective behind Outsourcing?</li> <li>• What are the in-house capabilities in performing the job?</li> <li>• What is the economic viability?</li> <li>• What are the in-house infrastructure deficiencies and the time factor involved?</li> <li>• What are the Risks and security concerns?</li> <li>• What are the outsourcing arrangement and fall back method?</li> <li>• What are arrangements for obtaining the source code for the software?</li> <li>• Reviewing the capability and quality of software development activities by visit to vendor's premises?</li> <li>• Review of progress of IS development at periodic intervals.</li> </ul>	
16.	<p>Whether the organization carried out a post implementation review of new IS?</p>	
17.	<p>Whether a process exists for measuring vendors' performance against the agreed service levels?</p>	
18.	<p>Whether the post implementation review results are documented?</p>	

## 5.8 Summary

The objective of the chapter is to describe the key issues for the system development process. The core issues dealt in the chapter include the RFP process and its evaluation. Chapter also helps to understand the concepts of ROI in terms of investments made in systems. Afterwards, the chapter discusses various methods of developments. It establishes a link between the need of business and the methods adopted to develop the system. It elaborates various advantages and disadvantages of system development.

The chapter explains the key considerations for selecting the method of development. Other methods for the development e.g. Waterfall, Prototyping, Incremental, Spiral, Rapid Application Development (RAD) and Agile Methodologies have also been discussed. Once a method of

development has been selected, the chapter elaborates the steps within each method development. It lists various teams and functions at each stage of system development. Detailed discussion on the System Development Life Cycle (SDLC) is also provided in the chapter. Accordingly, various stages for development of system development life cycle have been discussed. In addition, CASE tools used during development of the system including flowchart, data flow diagram have also been discussed.

# 6

## Auditing of Information Systems

---

### Learning Objectives

- To understand Information Systems Audit, its need, methodology and related standards;
- To know about IS Audit planning, performing an IS audit and best practices;
- To discuss different types of IS audit and assurance engagements;
- To have an overview of continuous auditing;
- To review General Controls and Application Controls; and
- To understand review of controls at various levels/layers such as: Parameters, user creation, granting of access rights, input, processing and output controls.

### Task Statements

- To apply appropriate audit technique/s in a specified audit situation; and
- To make proper documentation relating to IS Audit.

### Knowledge Statements

- To know the importance of audit in an IS environment;
- To know the approaches to be adopted for an IS Audit; and
- To know various types of controls, related concepts and their audit.

### 6.1 Introduction

Information Systems have become an integral part of our day-to-day life. From morning till evening, all humans interact with systems, in one form or another. The increased usage of technology has its pitfalls. Organizations need to rely more on technology for their day-to-day jobs, e.g. management decision making and all business related activities. As the usage of technology and information system is increasing, associated risk with technology is also imposing several threats to the information systems.

More and more use of technology and the increased instances has made it imperative for organizations to place proper controls. Controls can be classified based on nature say, preventive, detective and corrective or based on some other parameters like physical, logical or environmental. More classifications are also possible like based on the asset they protect; the detail discussion has already been done in Chapter 3 of the study material. In the same



chapter, there is detailed discussion on the risk associated with non-implementation of controls or improper implementation.

It is also clear that compliance is an important audit procedure undertaken by auditor to evaluate the nature, timing and extent of other audit procedures. As a part of compliance, an auditor evaluates the existence effectiveness and continued effectiveness of internal controls. The chapter highlights the same audit procedures in terms of performing systems audit for an organization. System audit, in today's environment shall precede any financial audit. The chapter discusses the need and method of doing an Information System Audit (IS Audit). In addition, the chapter also discusses various standards for IS Audit and the methodology for conducting an IS Audit in detail.

## 6.2 Controls and Audit

As discussed earlier, a Control is a system that prevents, detects or corrects unlawful events. Various controls are adapted as per requirement and accordingly, their audit become necessary. The details of controls have already been discussed in Chapter 3 of the Study Material.

### 6.2.1 Need for Audit of Information Systems

Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 6.2.1.

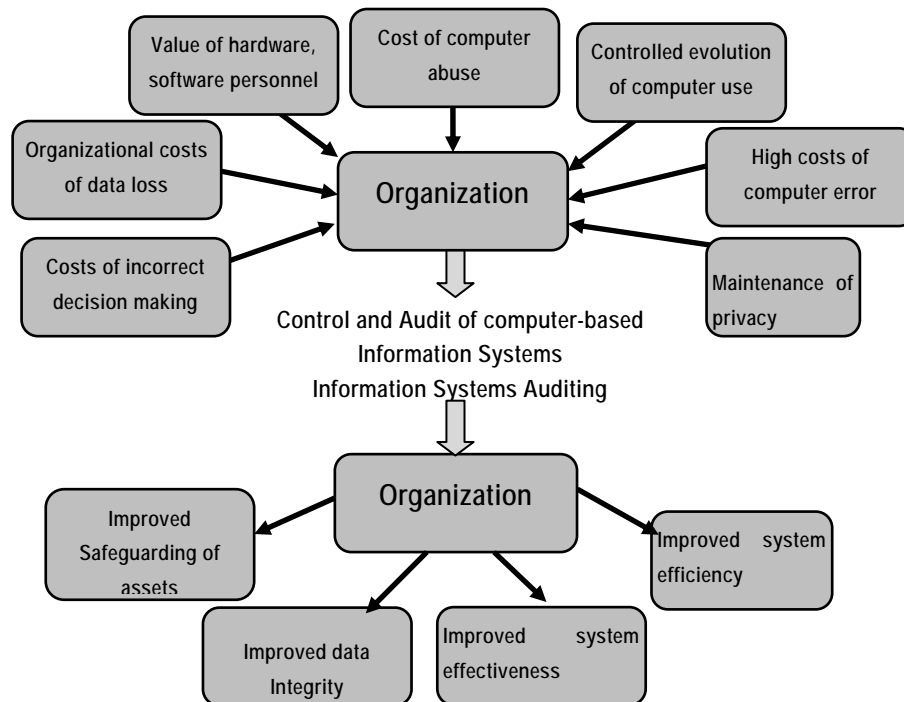


Fig. 6.2.1: Impact of Controls and Audit influencing an Organization

### 6.3 Information Systems Control and Audit

---

Let us now discuss these reasons in details:

- **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.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **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.
- **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.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

**Information Systems Auditing:** It 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 effectiveness and efficiency both. This enables organizations to better achieve four major objectives that are as follows:

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
- **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- **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.

### 6.2.2 Effect of Computers on Audit

To cope up with the new technology usage in an enterprise, the auditor should be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria. Two basic functions carried out to examine these changes are:

- Changes to Evidence Collection; and
- Changes to Evidence Evaluation.

These are discussed as follows:

**(i) Changes to Evidence Collection:** Existence of an audit trail is a key financial audit requirement; since without an audit trail, the 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 transactions on the computer system. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.
- **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.
- **Non-availability of 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 availability of printed 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 an 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.

## 6.5 Information Systems Control and Audit

---

- **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's strength and weakness throughout the system.

- **System generated transactions:** Financial systems may have the ability to initiate, approve and record financial transactions.
- **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. *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)
- **Systemic 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 systemic problem, the computer may have processed hundreds or thousands of similar transactions incorrectly

### 6.2.3 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 to meet each of the internal control objectives 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. The same is shown in Fig. 6.2.2.

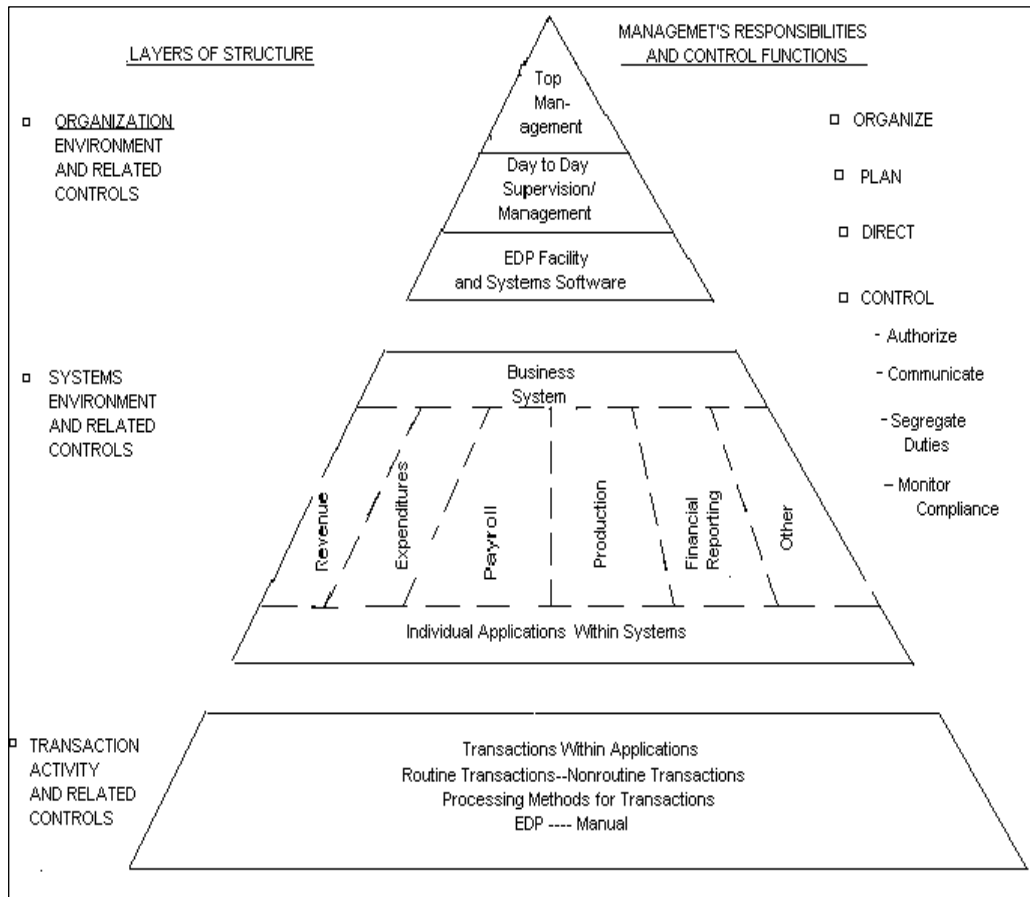


Fig. 6.2.2: Structure of the Control Environment

### 6.3 The IS Audit

The IS Audit of an Information System environment may include one or both of the following:

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

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer program and the data processing environment as a whole.

## 6.7 Information Systems Control and Audit

---

### 6.3.1 Skill set 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 to be with an IS auditor include:

- Sound knowledge of business operations, practices and compliance requirements;
- Should possess the requisite professional technical qualification and certifications;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policy and procedural 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.

### 6.3.2 Functions of IS Auditor

IS Auditor often is the assessor of business risk, as it relates to the use of IT, to management. The auditor 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. IS Auditors review risks relating to IT systems and processes; some of them are:

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

### 6.3.3 Categories of Information Systems Audits

Information Systems Audits has been categorized into five types:

- (i) **Systems and Application:** 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 (end point device), server, and on the network connecting the clients and servers.

#### 6.3.4 Steps in Information System Audit

Different audit organizations go about IS auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into six stages as shown in Fig. 6.3.1.

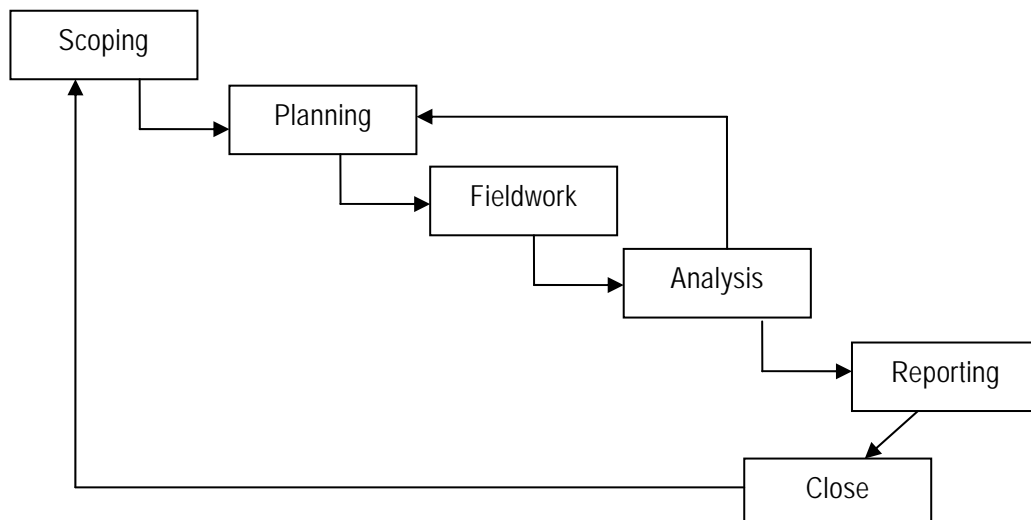


Fig. 6.3.1: Steps in IS Audit process

- (i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. 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.
- (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.

## 6.9 Information Systems Control and Audit

---

- (iii) **Fieldwork:** Gathering evidence by interviewing staff and managers, reviewing documents, and 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, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.
- (v) **Reporting:** Reporting to the management is done after analysis of evidence gathered and analyzed
- (vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

Analysis and reporting may 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 used for reviewing security parameters, and the basic security management functions that are built-in to modern systems can help with log analysis, reviewing user access rights etc.

Secondly, after accepting an engagement, the pre-audit survey is more important, as in this survey auditor has official access to client records and data. The purpose of this survey shall help auditor to assess the audit schedules, audit team size, and audit team components.

### 6.3.5 Audit Standards and Best Practices

IS auditors need guidance and a 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 conflict. The auditor needs guidance on how:

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

The Institute of Chartered Accountants of India has issued various Standards on Auditing 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 details are available in the Auditing paper of CA Course Curriculum. In addition to these Standards, there are certain guidelines, which 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, which are given as follows:

- (i) **ISACA (Information Systems Audit and Control Association):** ISACA 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):** This is a framework containing good business practices relating to information technology. The details are given in Chapter 1 of the Study Material.

(ii) **ISO 27001:** ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS). An ISMS is a systematic approach to manage Information security in an IS environment It encompasses people and, processes. ISO 27001 defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is safe to say that this standard is the foundation of information security management. It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

Many Indian IT companies have taken this certification, including INFOSYS, TCS, WIPRO. Companies getting themselves certified by as ISO 27001, are better competitor's to those not certified. Companies certified generate a greater client assurance. It removes the dependency from individuals and put reliance on processes. The details of this standard are given in chapter 7 of the Study Material.

(iii) **Internal Audit Standards:** 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 various information technology associated risks and recommended practices.

(iv) **Standards on Internal Audit issued by ICAI:** The Institute of Chartered Accountants of India (ICAI) has issued various standards; the details are given in the Study Material of Auditing paper. The standards issued by the ICAI highlight the process to be adopted by internal auditor in specific situation.

(v) **ITIL:** The Information Technology Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement. The details are given in the Chapter 7 of the Study Material.

## 6.4 Performing IS Audit

An IS Auditor uses the equivalent concepts of materiality (in financial audits) and significance (in performance audits) to plan both effective and efficient audit procedures. Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures. The underlying principle is that the auditor is not required to spend resources on items of little importance; that is, those that would not affect the judgment or conduct of a reasonable user of the audit report, in light of surrounding circumstances. On the basis of this principle, the auditor may determine that some areas of the IS controls audit (e.g., specific systems) are not material or significant, and therefore warrant little or no audit attention.

Materiality and significance include both quantitative and qualitative factors in relation to the subject matter of the audit. Even though a system may process transactions that are quantitatively immaterial or insignificant, the system may contain sensitive information or provide an access path to other systems that contain information that is sensitive or otherwise material or significant. For example, an application that provides public information via a website, if improperly configured, may expose internal network resources, including sensitive systems, to unauthorized access.

Planning occurs throughout the audit as an iterative process. (For example, based on findings from the testing phase, the auditor may change the planned audit approach, including the design of specific tests.) However, planning activities are concentrated in the planning phase, during which the objectives are to obtain an understanding of the entity and its operations, including its internal control, identify significant issues, assess risk, and design the nature, extent, and timing of audit procedures. To accomplish this, the methodology presented here is a guidance to help the auditor to perform IS Audit.

The auditor must address many considerations that cover the nature, timing, and extent of testing. The auditor must devise an auditing testing plan and a testing methodology to determine whether the previously identified controls are effective. The auditor also tests whether the end-user applications are producing valid and accurate information. For microcomputers, several manual and automated methods are available to test for erroneous data. An initial step is to browse the directories of the PCs in which the end-user-developed application resides. Any irregularities in files should be investigated. Depending on the nature of the audit, computer-assisted techniques could also be used to audit the application.

The auditor should also conduct several tests with both valid and invalid data to test the ability and extent of error detection, correction, and prevention within the application. In addition, the auditor should look for controls such as input balancing and record or hash totals to ensure that the end user reconciles any differences between input and output. The intensity and extent of the testing should be related to the sensitivity and importance of the application. The auditor should be cautious of too much testing and limit his/her tests to controls that cover all the key risk exposures and possible error types. The key audit concern is that the testing should reveal any type of exposure of sensitive data and that the information produced by the application is valid, intact, and correct. One should test the critical controls, processes, and

apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.

Secondly, we may test the critical controls, processes, and apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation. Validation of the information obtained is prescribed by the auditor's work program. Again, this work program is the organized, written, and pre-planned approach to the study of the IT department. It calls for validation in several ways, which are as follows:

- Asking different personnel the same question and comparing the answers;
- Asking the same question in different ways at different times;
- Comparing checklist answers to work papers, programs, documentation, tests, or other verifiable results;
- Comparing checklist answers to observations and actual system results; and
- Conducting mini-studies of critical phases of the operation.

Such an intensive program allows an auditor to become informed about the operation in a short time. Programs are run on the computer to test and authenticate application programs that are run in normal processing. The audit team selects one of the many Generalized Audit Software (GAS) packages such as Microsoft Access or Excel, IDEA, or ACL and determines what changes are necessary to run the software at the installation. The auditor is to use one of these software's to do sampling, data extraction, exception reporting, summarize and foot totals, and other tasks to perform in-depth analysis and reporting capability.

Various steps are given as follows:

#### **6.4.1 Basic Plan**

Planning is one of the primary and important phases in an Information System Audit, which ensures that the audit is performed in an effective manner. Planning takes more significance in case of Information Systems Audit since the audit risks are significantly impacted by inherent risk. Hence, for the audit efforts to be successful, a good audit plan is a critical success factor. Planning develops the annual audit schedule to perform the individual audits. It includes budgets of time and costs, and state priorities according to organizational goals and policies. The objective of audit planning is to optimize the use of audit resources.

Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work is completed expeditiously. Planning also assists in proper assignment of work to assistants and in coordination of the work done by other auditors and experts. Important points are given as follows:

- The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.
- Obtaining knowledge of the business is an important part of planning the work. The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.

## 6.13 Information Systems Control and Audit

---

- The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel. The overall audit plan and the audit program; however, remains the auditor's responsibility.
- The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the auditor.
- The audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a onetime activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many times changes in conditions or circumstances or unexpected findings during the course of audit require changes in the audit procedures and methodology initially planned. Hence, an auditor is expected to modify the audit plan as warranted by the circumstances.

The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change management procedure. Every change should be recorded with reason for change.

### 6.4.2 Preliminary Review

The extent of audit effort is dictated by the degree of risk of assessment, which is critical to the effectiveness of the audit effort. Amongst the critical factors affecting the risk is the appropriate assessment of the control environment. The preliminary review of audit environment enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

The following are some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review.

- (i) **Knowledge of the Business:** Related aspects are given as follows:
- General economic factors and industry conditions affecting the entity's business,
  - Nature of Business, its products & services,
  - General exposure to business,
  - Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
  - Level of competence of the Top management and IT Management, and
  - Finally, Set up and organization of IT department.

- (ii) **Understanding the Technology:** An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:
- Analysis of business processes and level of automation,
  - Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
  - Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
  - Studying network diagrams to understand physical and logical network connectivity,
  - Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
  - Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
  - And finally, Studying Information Technology policies, standards, guidelines and procedures.
- (iii) **Understanding Internal Control Systems:** For gaining understanding of Internal Controls emphasis to be placed on compliance and substantive testing.
- (iv) **Legal Considerations and Audit Standards:** Related points are given as follows:
- The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
  - The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
  - The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization. Sometimes, this may also include restrictions on the use of certain types of technologies e.g. freeware, shareware etc.
  - The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.
- (v) **Risk Assessment and Materiality:** Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. It implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence. Risk assessment allows the auditor to determine the scope of the audit and assess the

## 6.15 Information Systems Control and Audit

---

level of audit risk and error risk (the risk of errors occurring in the area being audited). Additionally, risk assessment will aid in planning decisions such as:

- The nature, extent, and timing of audit procedures.
- The areas or business functions to be audited.
- The amount of time and resources to be allocated to an audit

The steps that can be followed for a risk-based approach to make an audit plan are given as follows:

- Inventory the information systems in use in the organization and categorize them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- Assess what risks affect these systems and the severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Risks that affect a system and taken into consideration at the time of assessment can be differentiated as inherent risks, control risks and detection risks. These factors directly impact upon the extent of audit risk which can be defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit. At this stage, the auditor needs to:

- Assess the expected inherent, control and detection risk and identify significant audit areas.
- Set materiality levels for audit purposes.
- Assess the possibility of potential vulnerabilities, including the experience of past periods, or fraud.

Risks are categorized as follows:

- **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same.

Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional

judgment on the part of an auditor.

- **Control Risk:** Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.
- **Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

## 6.5 IS Audit and Audit Evidence

According to SA-230, Audit Documentation refers to the record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached (terms such as "working papers" or "work papers" are also sometimes used). The objects of an auditor's working papers are to record and demonstrate the audit work from one year to another. Evidences are also necessary for the following purposes:

- Means of controlling current audit work;
- Evidence of audit work performed;
- Schedules supporting or additional item in the accounts; and
- Information about the business being audited, including the recent history.

In IS environment, the critical issue is that evidences are not available in physical form, but are in electronic form.

### 6.5.1 Inherent Limitations of Audit

To be able to prepare proper report, auditor needs documented evidences. The problem of documents not available in physical form has been highlighted at many places. Following is list of actions that auditor needs to take to address the problems:

- Use of special audit techniques, referred to as Computer Assisted Audit Techniques, for documenting evidences. Elaborated under this part, later on.
- Audit timing can be so planned that auditor is able to validate transactions as they occur in system.

## 6.17 Information Systems Control and Audit

---

Auditor shall form his/her opinion based on above processes. As per (SA 200) "Overall Objectives of An Independent Auditor and Conduct of An Audit in Accordance With Standards of Auditing", any opinion formed by the auditor is subject to inherent limitations of an audit, which include:

- The nature of financial reporting;
- The nature of audit procedures;
- The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
- The matter of difficulty, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.
- Fraud, particularly fraud involving senior management or collusion.
- The existence and completeness of related party relationships and transactions.
- The occurrence of non-compliance with laws and regulations.
- Future events or conditions that may cause an entity to cease to continue as a going concern.

### 6.5.2 Provisions relating to Digital Evidences

As per Indian Evidence Act, 1872, "Evidence" means and includes:

- (i) All statements, which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;
- (ii) All documents produced for the inspection of the Court, such documents are called documentary evidence.

Documentary Evidence also includes 'Electronic Records'. The Information Technology Act, 2000 provides the legal recognition of electronic records and electronic signature through its various sections. The said Act also highlights Electronic Governance and accordingly, digital evidences are recognized legally. The details of related regulatory issues have been given in the Chapter 7 of the Study Material.

### 6.5.3 Concurrent or Continuous Audit

Today, organizations produce information on a real-time, online basis. Real-time recordings need real-time auditing to provide continuous assurance about the quality of the data that is continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the client's events and the auditor's assurance services thereon. Errors in a computerized 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 them are described below:

- (i) **Snapshots:** Tracing a transaction in a computerized 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 utilized 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 to locate the snapshot points based on materiality of transactions when the snapshot will be captured and 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 recognize 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 recognize 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 recognize 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 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. 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** - Organizations have to adhere to the policies, procedures and standards of the organization 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 an 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:

- 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;
- Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;
- 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
- 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 given 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 analyzed 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.

## 6.21 Information Systems Control and Audit

---

- **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.

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 organization 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.
- (v) **Audit Hooks:** There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

### 6.5.4 Audit Trail

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 authorized data) and achieve objectives effectively and efficiently from the perspective of users of the system from within and outside the organization.

(i) **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:

- **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.
- **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.
- **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. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(ii) **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.

## 6.6 Audit and Evaluation Techniques for Physical and Environmental Controls

In this section we shall concentrate majorly on the controls of Physical, Logical, environmental Controls.

Auditing of these controls is discussed as follows:

### 6.6.1 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:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **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.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

### 6.6.2 Audit of Environmental Controls

Related aspects are given as follows:

(a) **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 should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should take into account while conducting his/her audit is given below:

(b) **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.

- 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.
- (c) **Audit of Environmental Controls:** Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify:
- The IPF (Infrastructure Planning and Facilities) 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, firefighting equipment and refilling date of fire extinguishers;
  - Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;
  - 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; and
  - Identify undesired activities such as smoking, consumption of eatables etc.
- (d) **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. The following Table 6.6.1 presents a brief idea about the same.

**Table 6.6.1: Documentation of Auditing of Environmental Controls**

Control Activities	Control Techniques	Audit Procedures
Safeguards against the risks of heating, ventilation and air-conditioning	• Identify systems that provide constant temperature and humidity levels within the	• Review a heating, ventilation and air-conditioning design to verify proper functioning within

6.25 Information Systems Control and Audit

systems.	organization.	an organization.
<b>Control of radio emissions affect on computer systems.</b>	<ul style="list-style-type: none"> <li>• Evaluate electronic shielding to control radio emissions that affect the computer systems.</li> </ul>	<ul style="list-style-type: none"> <li>• Review any shielding strategies against interference or unauthorized access through emissions.</li> </ul>
<b>Establish adequate interior security based on risk</b>	<ul style="list-style-type: none"> <li>• Critical systems have emergency power supplies for alarm systems; monitoring devices, exit lighting, communication systems.</li> </ul>	<ul style="list-style-type: none"> <li>• Verify critical systems (alarm systems, monitoring devices, and entry control systems) have emergency power supplies.</li> <li>• Identify back -up systems and procedures and determine the frequency of testing. Review test results.</li> </ul>
<b>Adequately protect against emerging threats, based on risk.</b>	<ul style="list-style-type: none"> <li>• Appropriate plans and controls such as shelter in place or for a potential CBR attack(chemical, biological and radioactive attack)</li> <li>• Restricting public access and protect critical entry points-air intake vents, protective grills and roofs.</li> </ul>	<ul style="list-style-type: none"> <li>• Interview officials, review planning documents and related test results.</li> <li>• Observe and document the controls in place to mitigate emerging threats.</li> <li>• Observe location of these devices and identify security measures implemented.</li> <li>• Verify the controls existence and intrusion detection sensors.</li> </ul>
<b>Adequate environmental controls have been implemented</b>	<ul style="list-style-type: none"> <li>• Fire detection and suppression devices are installed and working.(smoke detectors, fire extinguishers and sprinkle systems)</li> <li>• Controls are implemented to mitigate disasters, such as floods, earthquakes.</li> <li>• Redundancy exists in critical systems like,</li> </ul>	<ul style="list-style-type: none"> <li>• Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, emergency power off switches, air -ventilation apparatus and other emergency devices.</li> <li>• Determine that humidity, temperature and voltage are controlled within the accepted levels.</li> <li>• Check cabling, plumbing, room ceiling smoke detectors, water</li> </ul>



	<p>uninterrupted power supply, air cooling system, and backup generators</p> <ul style="list-style-type: none"> <li>• Humidity, temperature, and voltage control are maintained and acceptable levels</li> <li>• Emergency lighting, power outages and evacuation routes are appropriately located.</li> </ul>	<p>detectors on the floor are installed and in working properly.</p>
<p><b>Staff have been trained to react to emergencies</b></p>	<ul style="list-style-type: none"> <li>• Operational and support personnel are trained and understand emergency procedures.</li> <li>• Emergency procedures are documented and periodically tested-incident plan, inspection plan and maintenance plan.</li> </ul>	<ul style="list-style-type: none"> <li>• Interview security personnel to ensure their awareness and responsibilities.</li> <li>• Review training records and documentation. Determine the scope and adequacy of training.</li> <li>• Review test policies, documentation and know-how of operational staff.</li> <li>• Review incident handling procedures and maintenance and inspection plan.</li> </ul>

Further, we may again recall that below mentioned are the General Controls that have been discussed in detail in Chapter - 3 of the study material.

- (i) Organizational Controls
- (ii) Operating System Controls;
- (iii) Management Controls;
- (iv) Financial Controls;
- (v) BCP Controls;
- (vi) Operating System Controls;
- (vii) Data Management Controls;
- (viii) System Development Controls;
- (ix) Computer Centre Security Controls;
- (x) Internet & Intranet Controls; and
- (xi) Personal Computers Controls.

## 6.7 Application Controls and their Audit Trails

Application Controls and their categories have been explained in detail in Chapter 3 of the Study material. We may however again provide an overview of the same here as shown in Table 6.7.1.

Table 6.7.1: Application Controls and Audit Trail

<i>Controls</i>	<i>Scope</i>
<u><i>Boundary Controls</i></u>	<i>Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.</i>
<u><i>Input Controls</i></u>	<i>Responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.</i>
<u><i>Communication Controls</i></u>	<i>Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.</i>
<u><i>Processing Controls</i></u>	<i>Responsible for computing, sorting, classifying and summarizing data. 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.</i>
<u><i>Output Controls</i></u>	<i>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.</i>
<u><i>Database Controls</i></u>	<i>Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.</i>

### 6.7.1 Audit Trail Controls

Two types of audit trails that should exist in each subsystem.

- An Accounting Audit Trail to maintain a record of events within the subsystem; and
- An Operations Audit Trail to maintain a record of the resource consumption associated with each event in the subsystem.

We shall now discuss Audit Trails for Application Controls in detail.

### 6.7.2 Boundary Controls

This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.

- *Identity of the would-be user of the system;*
- *Authentication information supplied;*
- *Resources requested;*
- *Action privileges requested;*
- *Terminal Identifier;*
- *Start and Finish Time;*
- *Number of Sign-on attempts;*
- *Resources provided/denied; and*

Accounting Audit Trail

- *Action privileges allowed/denied.*

Operations Audit Trail

- *Resource usage from log-on to log-out time.*
- *Log of Resource consumption.*

### 6.7.3 Input Controls

*This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.*

Accounting Audit Trail

- *The identity of the person(organization) who was the source of the data;*
- *The identity of the person(organization) who entered the data into the system;*
- *The time and date when the data was captured;*
- *The identifier of the physical device used to enter the data into the system;*
- *The account or record to be updated by the transaction;*
- *The standing data to be updated by the transaction;*
- *The details of the transaction; and*
- *The number of the physical or logical batch to which the transaction belongs.*

Operations Audit Trail

- *Time to key in a source document or an instrument at a terminal;*
- *Number of read errors made by an optical scanning device;*
- *Number of keying errors identified during verification;*
- *Frequency with which an instruction in a command language is used; and*

- *Time taken to invoke an instruction using a light pen versus a mouse.*

#### 6.7.4 Communication Controls

*This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.*

##### Accounting Audit Trail

- *Unique identifier of the source/sink node;*
- *Unique identifier of each node in the network that traverses the message; Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched;*
- *Time and date at which the message was received by the sink node;*
- *Time and date at which node in the network was traversed by the message; and*
- *Message sequence number; and the image of the message received at each node traversed in the network.*

##### Operations Audit Trail

- *Number of messages that have traversed each link and each node;*
- *Queue lengths at each node; Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors;*
- *Log of system restarts; and*
- *Message transit times between nodes and at nodes.*

#### 6.7.5 Processing Controls

*The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.*

##### Accounting Audit Trail

- *To trace and replicate the processing performed on a data item.*
- *Triggered transactions to monitor input data entry, intermediate results and output data values.*

##### Operations Audit Trail

- *A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.*
- *A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.*

### 6.7.5 Database Controls

*The audit trail maintains the chronology of events that occur either to the database definition or the database itself.*

#### Accounting Audit Trail

- *To attach a unique time stamp to all transactions,*
- *To attach beforeimages and afterimages of the data item on which a transaction is applied to the audit trail; and*
- *Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.*

#### Operations Audit Trail

- *To maintain a chronology of resource consumption events that affects the database definition or the database.*

### 6.7.6 Output Controls

*The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.*

#### Accounting Audit Trail

- *What output was presented to users;*
- *Who received the output;*
- *When the output was received; and*
- *What actions were taken with the output?*

#### Operations Audit Trail

- *To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.*

## 6.8 Audit of Application Security Controls

There are many aspects to the application controls that are reviewed as a part of any application audit and the same has already been discussed in the earlier sections but out of these, application security is one of the most important controls that are why the same is discussed separately. The objective of this exercise is to establish whether the application security controls are operating effectively to protect the confidentiality, integrity and availability of information. Application security is concerned with maintaining these aforementioned attributes of the information. The result of lacunae in application security may lead to security related frauds that may give rise to financial and reputation losses.

### 6.8.1 Approach to Application Security Audit

Application security audit is being looked from the usage perspective. A layered approach is used based on the functions and approach of each layer. Layered approach is based on the activities being undertaken at various levels of management, namely supervisory, tactical and strategic. The approach is in line with management structure which follows top-down approach. For this, auditors need to have a clear understanding of the following.

- Business process for which the application has been designed;
- The source of data input to and output from the application;
- The various interfaces of the application under audit with other applications;
- The various methods that may be used to login to application, other than normal user-id and passwords that are being used, including the design used for such controls;
- The roles, descriptions, user profiles and user groups that can be created in an application; and
- The policy of the organization for user access and supporting standards.

As discussed earlier, there are various layers, which are shown in the Fig. 6.8.1 and discussed as follows:

- **Operational Layer:** The basic layer, where user access decision are generally put in place.
- **Tactical Layer:** The next is management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- **Strategic Layer:** This is the layer used by TOP management. It includes the overall information security governance, security awareness, supporting information security policies and standards, and the overarching an application security perspective.

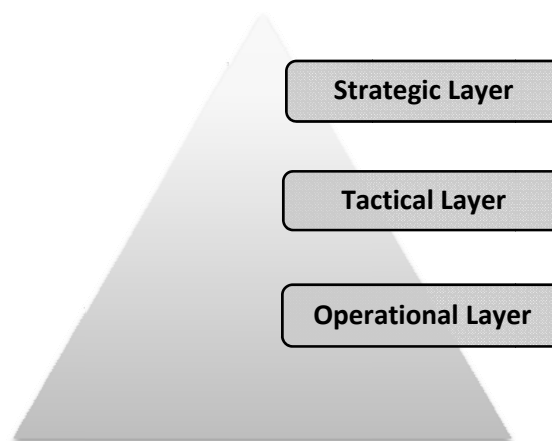


Fig. 6.8.1: Application Security Layer

### 6.8.2 Understanding the Layers and Related Audit Issues

In this section, various aspects relating to each aforementioned layer have been discussed.

(i) **Operational Layer:** The operational layer audit issues include:

- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities. Auditor needs to always ensure the use of unique user IDs, and these need to be traceable to individual for whom created. In case, guest IDs are used then test of same should also be there. Likewise, vendor accounts and third-party accounts should be reviewed. In essence, users and applications should be uniquely identifiable.
- **Password Controls:** In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum. Auditor needs to check whether there are applications where password controls are weak. In case such instances are found, then auditor may look for compensating controls against such issues.
- **Segregation of Duties:** As frauds due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases. As defined earlier, Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals. Example to illustrate:
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher in system, must not have right to authorize payments.
  - Maker must not be checker.

Auditor needs to check that there is no violation of above principle. Any violation may have serious repercussions, the same need to be immediately communicated to those charged with governance.

(ii) **Tactical Layer:** At the tactical layer, security administration is put in place. This includes:

- Timely updates to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
- **IT Risk Management:** This function is another important function performed, it includes the following activities:
  - Assessing risk over key application controls;
  - Conducting a regular security awareness programme on application user;

### 6.33 Information Systems Control and Audit

---

- Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;
- Reviewing application patches before deployment and regularly monitoring critical application logs;
- Monitoring peripheral security in terms of updating antivirus software;

An auditor should understand the risk associated with each application and obtain a report on periodic risk assessment on the application or self-assessment/compliance reports on the application.

- **Interface Security:** This relates to application interfaced with another application in an organization. An auditor needs to understand that data flow to and from the application. Security of the interfaced data is also important, especially when unencrypted methods of transmission are used for data transmission.
  - **Audit Logging and Monitoring:** Regular monitoring the audit logs is required. The same is not possible for all transactions, so must be done on an exception reporting basis.
- (iii) **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

One of the key responsibilities of the IT risk management function is to promote ongoing security awareness to the organization's users. Security metrics are now becoming popular to gauge the performance of the security management function. These are often good indicators of the security health of an organization. Auditor needs to check whether all these aforementioned guidelines have been properly framed and are they capable of achieving the business objectives sought from the application under audit.

Based on the key controls described previously, the risk assessment of failure/weakness in the operating effectiveness of the key application security controls shall be made and acted upon by auditor.

## 6.9 Summary

In the chapter, there has been a detailed discussion on Information System Audit, its need and the method of performing the same. Chapter outlines the losses that an organization may face, incase, it does not get it audited. The chapter also discusses the impact of computers on audit and audit procedures adopted. Afterwards, the chapter discusses the steps to perform an Information system audit. The idea of pre-audit survey and planning of an audit for effective execution of an audit has also been elaborated in the chapter.



The chapter discusses various auditing standards that an auditor can use for performing a systems audit. Chapter elaborates the standards issued by ISACA, ISO 27001 and Standards issued by ICAI. In addition, the chapter also elaborates concept of risk assessment, documentation to be done by an Information Systems Auditor (ISA). In addition, the chapter also provides a detailed discussion on Continuous Auditing. Finally, there is a detailed discussion on various types of controls, including specialized application security controls.

## Information Technology Regulatory Issues

### Learning Objectives

- To learn the key provisions of IT Act 2000 along with amendments and its objectives;
- To understand related definitions and specific provisions;
- To understand systems audit requirements by various agencies; and
- To get an overview of Cyber Forensic and Cyber Fraud Investigations.

### Task Statements

- To understand the key provisions of IT Act and Rules as relevant for assurance and assessing impact of the non-compliance;
- To identify risk to an entity in terms of technology being used;
- To understand scope of cyber forensics/cyber fraud investigation; and
- To outline the requirements of other statutes regarding systems audit.

### Knowledge Statements

- To know the specific sections of IT Act & its Rules as relevant for assurance: Electronic Contracting, digital signatures, cyber offences, etc;
- To know the need for systems audit as per various regulatory bodies such as: RBI, SEBI, IRDA; and
- To know the concepts of Cyber Forensic/Cyber Fraud Investigation.

### 7.1 The IT Act and its Objectives

The Information Technology Act was enacted on 17th May 2000 primarily to provide legal recognition for electronic transactions and facilitate e-commerce. India became the 12th nation in the world to adopt cyber laws by passing the Act. When the Information Technology Act, 2000 was introduced, it was the first information technology legislation introduced in India. The IT Act is based on Model law on e-commerce adopted by UNCITRAL (United Nations Commission on International Trade) of United Nations organization.

The IT Act was amended by passing of the Information Technology (Amendment) Act 2008 (Effective from October 27, 2009). The amended Act casts responsibility on body corporate to protect sensitive personal information (Sec. 43A). It recognizes and punishes offences by companies and individual (employee) actions (Sec. 43, 66 to 66F, 67..) such as sending offensive messages using electronic medium or using body corporate's IT for unacceptable

purposes, stealing computer resources, unauthorized access to computer resources, identity theft/cheating by personating using computer, violation of privacy, cyber terrorism, offences using computer and publishing or transmitting obscene material. It also provides for extensive powers for police and statutory authorities. The amended Act is expected to create a paradigm shift in data protection and privacy regime in India as it provides for establishing a self-regulation framework for maintenance of reasonable security practices and procedures for protecting "sensitive personal data or information". It also has provisions for adjudication related to data protection and privacy (civil liabilities) and provides for criminal prosecution vis-à-vis data protection and privacy.

The following rules have been issued for IT Act 2008:

- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
- Information Technology (Intermediaries guidelines) Rules, 2011.
- Information Technology (Electronic Service Delivery) Rules, 2011.

The Information Technology Act, 2000 was enacted 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.

The provisions of the Information Technology Act 2000 and the amendments of 2008 are simple to understand and most of these are self-explanatory. As an auditor, it is important to understand the key provisions of the IT Act as it impacts other compliances and provides the basis for other compliances. For example, when tax audit is being performed and the client accounts are maintained in a computer, it is important for the auditor to know specific provisions and the impact of the data being maintained in electronic form. Further, if audit is being done as per Companies Act, then specific aspects of internal controls and risk management are to be reviewed by auditor.

In modern enterprises, most of the critical information is input, processed and stored in computers even in case of small and medium enterprises. Hence, the regulatory provisions and impact of this data being available electronically, the risks of it being misused and regulatory provisions of such non-compliance has to be understood and also communicated to the client to mitigate the control weaknesses and ensure compliance. It is advisable for students to understand provisions of the IT Act. In this chapter, the key provisions are reproduced with brief explanations as required.

The Objectives of the Act are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data

### 7.3 Information Systems Control and Audit

---

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; and
- 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.

The IT Act extends to whole of India and also applies to any offence or contravention there under committed outside India by any person {section 1 (2)} read with Section 75. The Act applies to offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.

Some of the key Issues of electronic information impacting enterprises and auditors are:

- **Authenticity:** How do we implement a system that ensures that transactions are genuine and authorized?
- **Reliability:** How do we rely on the information, which does not have physical documents?
- **Accessibility:** How do we gain access and authenticate this information, which is digital form?

A good understanding of the provisions of IT Act will provide answer to these issues.

### 7.2 Key Definitions

As enterprises increasingly use digital signature technologies to support e-commerce, legal issues such as non-repudiation, online contracts and protection of intellectual property have become more common. The IT Act provides various definitions of different technological terms; some of the key definitions are given below:

- (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.
- (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) "**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;

## 7.5 Information Systems Control and Audit

---

- (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.
  - (na) "**Cyber Cafe**" 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) "**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.
- (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) "**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) "**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;

- (w) "**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 thereunder;
- (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;

## 7.7 Information Systems Control and Audit

---

- (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.

## 7.3 [Chapter-II] Digital Signature and Electronic Signature

This chapter of IT Act 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 anybody 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. The provisions of this section are 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**

- (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".

**7.4 [Chapter III] Electronic Governance**

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] 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

## 7.9 Information Systems Control and Audit

---

(b) accessible so as to be usable for a subsequent reference.

### **[Section 5] Legal recognition of Electronic Signatures**

Where any law requires that any information or matter shall be authenticated by affixing the signature or any document shall 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 electronic 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] Use of Electronic Records and Electronic Signatures 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).

#### **Explanation –**

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 license 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.

**[Section 6A] Delivery of services by Service Provider**

- (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 setup, 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 firm 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 such 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] 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, if -
  - (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:

PROVIDED that 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.

## 7.11 Information Systems Control and Audit

---

- (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.

### ***[Section 7A] Audit of Documents, etc. maintained 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.

### ***[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:

PROVIDED that 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.

### ***[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***

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.

### ***[Section 10A] Validity of contracts formed through electronic means***

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.

## 7.5 [Chapter V] Secure Electronic Records and Secure Electronic Signatures

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] 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] Secure Electronic Signature**

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] Security Procedures and Practices**

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.

## 7.6 [Chapter IX] Penalties, Compensation and Adjudication

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] Penalty and Compensation for damage to computer, computer system, etc.**

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;
- (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;

### 7.13 Information Systems Control and Audit

---

- (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;
- (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,

he shall be liable to pay damages by way of compensation to the person so affected.

#### 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 formalized 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.

**[Section 43A] Compensation for failure to protect data**

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.

**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;
- (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 thereunder 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 therefor 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] 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.

## 7.7 [Chapter XI] Offences

Apart from giving recognition to electronic contracts, the IT Act identifies certain acts as "Computer Crimes" and provides penalties for these offences. It is necessary for every user to Internet and other proprietary networks to avoid inadvertently committing any action, which can be termed as a "Computer Crime". The Act lists common crimes that can be perpetrated in the electronic society and specifies penalty. The Computer crimes that are recognized by the Act could affect:

- Hackers
- Digital Contract parties
- The Digital IC users
- Netizen
- Web Site owners/Content creators
- Software professionals
- Auditors
- Certifying authorities web hosting firms

Chapter XI deals with offences under the IT Act. Auditors need to have good understanding of various provisions of this section so as to review compliance as required.

### **[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 programme, computer commands, design and layout and program analysis of computer resource in any form.

### **[Section 66] Computer Related Offences**

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 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 (45 of 1860);



- (b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

**[Section 66A] Punishment for sending offensive messages through communication service, etc.**

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 makes by making use of such computer resource or a communication device; or
- (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, 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 66B] Punishment for dishonestly receiving stolen computer resource or communication device**

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**

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**

Whoever, by means of any communication device or computer resource cheats by personating, 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**

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

## 7.17 Information Systems Control and Audit

---

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 authorization 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.

**[Section 67] Punishment for publishing or transmitting obscene material in electronic form**

Whoever publishes or transmits or causes to be published or transmitted 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 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form**

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.

**[Section 67B] 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

## 7.19 Information Systems Control and Audit

---

- (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 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 bona fide 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 67C] 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] Power of the Controller to give directions***

- (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 thereunder.
- (2) Any person who intentionally or knowingly 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 with both.

### ***[Section 69] Powers to issue directions for interception or monitoring or decryption of any information through any computer resource***

- (1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so 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 generated, transmitted, received or stored in 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, 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 imprisonment for a term which may extend to seven years and shall also be liable to fine.

***[Section 69A] 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 officers 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-section (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 shall 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, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

## 7.21 Information Systems Control and Audit

---

- (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorised 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] Protected system**

- (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.

### **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.

- (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.

### **[Section 70A] National nodal agency**

- (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 70B] 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 whitepapers 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] 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] Penalty for 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 pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, 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.

***[Section 72A] Punishment for Disclosure of information in breach of lawful contract***

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] Penalty for publishing Electronic Signature Certificate false in certain particulars***

- (1) No person shall publish an 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] Publication for fraudulent purpose***

Whoever knowingly creates, publishes or otherwise makes available an 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] Act to apply for offences 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] 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:

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 authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:

- Designate a Cyber Law Compliance Officer as required.
- Conduct regular training of relevant employees on Cyber Law Compliance.
- Implement strict procedures in HR policy for non-compliance.
- Implement authentication procedures as suggested in law.
- Implement policy and procedures for data retention as suggested.
- Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.
- Implement applicable standards of data privacy on collection, retention, access, deletion etc.
- Implement reporting mechanism for compliance with cyber laws.

## **7.8 [Chapter XII] Intermediaries not to be liable in Certain Cases**

Chapter XII contains section 79.

***[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 made available or hosted by him.

## 7.25 Information Systems Control and Audit

---

- (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 hosted; 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.
- (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;
  - (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 purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

## **7.9 [CHAPTER XIIA] Examiner of Electronic Evidence**

### ***[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 purposes 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.

## 7.10 [Chapter XIII] Miscellaneous

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 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 (2 of 1974) 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.

### ***[Section 81A] Application of the Act to electronic cheque and truncated cheque***

- (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

## 7.27 Information Systems Control and Audit

---

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 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 84B] Punishment for abetment of offence***

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 84C] Punishment for attempt to commit offences***

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 thereunder 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:

PROVIDED that 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.

**7.11 Requirements of Various Authorities for System Controls & Audit**

Under this part, requirements by various statutory bodies' vis-à-vis system and audit requirements have been put including that of IRDA, RBI and SEBI. It is important to note that these are just illustrative and not comprehensive.

**7.11.1 Requirements of IRDA for System Controls & Audit**

The **Insurance Regulatory and Development Authority of India (IRDA)** is the apex body overseeing the insurance business in India. It protects the interests of the policyholders, regulates, promotes and ensures orderly growth of the insurance in India.

Information System Audit has a significant role to play in the emerging Insurance Sector. Information System Audit aims at providing assurance in respect of Confidentiality, Availability and Integrity for Information systems. It also looks at their efficiency, effectiveness and responsiveness. It focuses on compliance with laws and regulations, which are given as follows:

**(i) System Audit:** These are as follows:

- All insurers shall have their systems and process audited at least once in three years by a CA firm.
- In doing so, the current internal or concurrent or statutory auditor is not eligible for appointment.
- CA firm must be having a minimum of 3-4 years experience of IT systems of banks or mutual funds or insurance companies.

**(ii) Preliminaries**

Before proceeding with the audit, the auditor is expected to obtain the following information at the audit location:

- Location(s) from where Investment activity is conducted.
- IT Applications used to manage the Insurer's Investment Portfolio.
- Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/utilities (describe).
- Are systems and applications hosted at a central location or hosted at different office?

## 7.29 Information Systems Control and Audit

---

- Previous Audit reports and open issues / details of unresolved issues from:
  - Internal Audit,
  - Statutory Audit, and
  - IRDA Inspection / Audit.
- Internal circulars and guidelines of the Insurer.
- Standard Operating Procedures (SOP).
- List of new Products/funds introduced during the period under review along with IRDA approvals for the same.
- Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.
- IRDA Correspondence files, circulars and notifications issued by IRDA.
- IT Security Policy.
- Business Continuity Plans.
- Network Security Reports pertaining to IT Assets.

(iii) **System Controls:** These are as follows:

- There should be Electronic transfer of Data without manual intervention. All Systems should be seamlessly integrated. Audit Trail required at every Data entry point. Procedures for reviewing and maintaining audit trail should be implemented.
- The auditor should comment on the audit trail maintained in the system for various activities. The auditor should review the FOS, MOS and BOS and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.
- Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.

### 7.11.2 Requirements of RBI for System Controls & Audit

The **Reserve Bank of India (RBI)** is India's central banking institution, which formulates the monetary policy with regard to the Indian rupee. The Bank was constituted for the need of following:

- To regulate the issue of banknotes,
- To maintain reserves with a view to securing monetary stability, and
- To operate the credit and currency system of the country to its advantage.

IS audits are gaining importance as key processes are automated or enabled by technology. The Reserve Bank of India (RBI) has been at the forefront of recognizing and promoting IS Audit internally and across all the stakeholders including financial institutions.

RBI has been proactive in providing guidelines on key areas of IT implementation by using global best practices. They have constituted various expert committees who review existing and future technology and related risks and provide guidelines, which are issued by all stakeholders.

Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the IT related risks are managed. Sample areas of review covered by IS Audit assignments are given here.

(i) **System Controls:** These are given as follows:

- Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design. System person would only make modifications/improvements to programs and the operating persons would only use such programs without having the right to make any modifications.
- Contingency plans/procedures in case of failure of system should be introduced/tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
- An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.
- In order to bring about uniformity of software used by various branches/offices there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the view-point of control and for its implementation in other branches in order to maintain uniformity.
- Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.
- There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
- With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

(ii) **System Audit:** Relevant points are given as follows:

- In this regard, banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions. Where the bank leverages external resources for conducting IS Audit on areas where skills are lacking, the responsibility and

### 7.31 Information Systems Control and Audit

---

accountability for such external IS Audits still remain with the IS Audit Head and CAE.

- Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent and exercise due professional care.
- The IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function.
- Additionally, to ensure independence for the IS Auditors, Banks should make sure that:
  - Auditors have access to information and applications, and
  - Auditors have the right to conduct independent data inspection and analysis.
- *Competence:* IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training. As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by a bank. They should be competent audit professionals with sufficient and relevant experience. Qualifications such as Certified Information Systems Auditor (CISA, offered by ISACA), Information Systems Audit (ISA, offered by ICAI), or Certified Information Systems Security Professional (CISSP, offered by ISC2), along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.
- IT Governance, information security governance related aspects, critical IT general controls such as data centre controls and processes and critical business applications/systems having financial/compliance implications, including regulatory reporting, risk management, customer access (delivery channels) and MIS systems, needs to be subjected to IS Audit at least once a year (or more frequently, if warranted by the risk assessment).
- IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, anti-malware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy and or testing.
- IS Auditors should review the following additional areas that are critical and high risk such as:
  - IT Governance and information security governance structures and practices implemented by the Bank.



- Testing the controls on new development systems before implementing them in live environment.
  - A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that:
    - Controls in existing application are not diluted, while migrating data to the new application
    - Controls are designed and implemented to meet requirements of a bank's policies and procedures, apart from regulatory and legal requirements
    - Functionality offered by the application is used to meet appropriate control objectives
- A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively. Periodic review of application controls should be a part of an IS audit scope, in order to detect the impact of application changes on controls. This should be coupled with review of underlying environment–operating system, database, middleware, etc. – as weaknesses in the underlying environment can negate the effectiveness of controls at the application layer. Due care should be taken to ensure that IS Auditors have access only to the test environment for performing the procedures and data used for testing should be, as far as practical, be a replica of live environment.
- Detailed audit of SDLC process to confirm that security features are incorporated into a new system, or while modifying an existing system, should be carried out.
- A review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system, and a review of data migration from legacy systems to the new system where applicable should be followed.
- IS Auditors may validate IT risks (identified by business teams) before launching a product or service. Review by IS Auditor may enable the business teams to incorporate additional controls, if required, in the system before the launch.
- When IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for the organization, they should discuss the matter with appropriate level of management. If the IS Auditors are not in agreement with the decision, regarding residual risk, IS Auditors and Senior Management should report the matter to the Board (or Audit Committee) for resolution.

In addition, RBI has an inspection wing, which does inspection of banking and non-banking financial institutions. As part of the audit, one of the critical aspects, which have been reviewed, are scope, coverage, frequency and report of system audit. If system audit has not

### 7.33 Information Systems Control and Audit

---

been done, it is considered as non-compliance and reported to the senior management for compliance. In the case of branch statutory audit, the LFAR has specific questions pertaining to IT areas such as Security/BCP etc., which need to be reviewed by the statutory auditors. Although very limited, these can also be considered as key areas of IS Audit.

#### 7.11.3 Requirements of SEBI for System Controls & Audit

The **Securities and Exchange Board of India (SEBI)** is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market:

- The issuers of securities,
- The investors, and
- The market intermediaries.

Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders.

(i) **Systems Audit:** SEBI had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

- The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.
- Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.
- Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.
- The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report
- Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.
- The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit. Sample areas of review covered by IS Audit assignments are given here.

(ii) **Audit Report Norms:** These are given as follows:

- The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories and the system audit report along with comments of Stock Exchanges / Depositories should be communicated to SEBI.
- The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it). For each section, auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed.

(iii) **Auditor Selection Norms:** There are various norms for selection of Auditors, which are given as follows:

- Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
- The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC)<sup>2</sup>.
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

(iv) **System Controls:** These are given as follows:

- Further, along with the audit report, Stock Exchanges/Depositories are advised to submit a declaration from the MD/CEO certifying the security and integrity of their IT Systems.
- A proper audit trail for upload/modifications/downloads of KYC data to be maintained

Department of Electronics & IT, Ministry of Communication and IT, Government of India, maintains a panel of systems auditors, which are used by government enterprises for

getting system audit done. This provides information on scope of different types of systems audit which is used as reference by auditee firms for getting systems audit done.

### 7.12 Cyber Forensic and Cyber Fraud Investigation

Cyber forensics is one of the latest scientific techniques that have emerged due to the effect of increasing computer frauds. To understand the term better, an understanding of the independent words will be useful. Cyber, means on 'The Net' that is online. Forensics is a scientific method of investigation and analysis techniques to gather, process, interpret, and to use evidence to provide a conclusive description of activities in a way that is suitable for presentation in a court of law. Considering 'Cyber' and 'Investigation' together will lead us to conclude that 'Cyber Investigation' is an investigation method gathering digital evidences to be produced in court of law.

Court rulings and amendments to cyber laws now permit courts to rely upon digital evidences. As electronic evidences can be created through use of technology, cyber forensics emphasizes the use of special methods to gather evidences, so that these electronic evidences stand the rigours/scrutiny when presented in a court of law.

To ensure that the above objectives are achieved, the experts of the fields use standard processes and globally accept methods so that same result shall always be obtained if the same evidences are checked by another expert, that is why cyber forensic experts follow standard methods for investigation.

Increasing frauds across the cyber space, the sheer size, speed and value of the frauds has surprised the law keeper's. Fraudsters are always on the look-out to misuse any loop hole or weaknesses in the computer systems. Cyber Frauds across the world as withdrawal of an amount equal to USD45 Million, by using ATM cards of banks, sent shock waves across the IT security agencies. There is an increasing demand for experts in the field of cyber forensics. The IT Act under Section 43A and Section 65 to 67B lists various types of cyber-crimes and specifies penalty for them. For example, section 65 has already been discussed in earlier sections.

Keeping the importance of the same in view, the Institute of Chartered Accountants of India, New Delhi, has also launched a post qualification course on the above subject by the name "Certificate Course on Forensic Accounting and Fraud Detection." This post qualification course can be taken by a qualified CA.

### 7.13 Security Standards

Information security is essential in the day-to-day operations of enterprises. Breaches in information security can lead to a substantial impact within the enterprise through, for example, financial or operational damages. In addition, the enterprise can be exposed to external impacts such as reputational or legal risk, which can jeopardize customer or employee relations or even endanger the survival of the enterprise. COBIT 5 for Information security published by ISACA, USA highlights the needs for enterprises to ensure required level of security is implemented. The ever-increasing need for the enterprise to implement security is highlighted here:

- Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions;
- Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services;
- Comply with the growing number of relevant laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance; and
- Achieve all of the above while containing the cost of IT services and technology protection.

Considering the importance of security, Government of India recently published the National Cyber Security Policy 2013 with the vision: **“To build a secure and resilient cyberspace for citizens, business and Government”** and the mission **“To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation”**.

The policy document highlights the need for security in the cyberspace and outlines that cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-states actors. Cyber-attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms of any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets.

Large-scale cyber incidents may overwhelm the government, public and private’s sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identify theft, phishing, social engineering, activism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, supply chain attacks, data leakage etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence to secure cyber space. Major objectives of this policy are given as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of T all sectors of the economy;

### 7.37 Information Systems Control and Audit

---

- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, & people);
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;
- To enhance and create National and Sectorial level 24\*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution and crisis management through effective predicative, protective, response and recovery actions;
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources;
- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, and pilot development of secure ICT products/processes in general and specifically for addressing National Security requirements;
- To improve visibility of the integrity of Information & Communication Technology products & services and establishing infrastructure for testing & validation of security of such products;
- To create a workforce of 500,000 professional skilled in cyber security in the next 5 years through capacity building, skill development and training;
- To provide fiscal benefits to businesses for adoption of standard security practices and processes;
- To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft;
- To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention;
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;
- To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace and
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Based on the key aspects of National Cyber Security Policy 2013, we can understand that Chartered Accountants in their role as accountants and auditors have another important role

to play in ensuring compliance of security and also pro-actively provide assurance on the state of IT security in an enterprise.

There are many standards on IT security issued by various stakeholders such as regulators, professional organizations and technology providers. It is important to remember that each standard has a specific purpose and perspective, which has to be understood before implementation. Some of the most relevant and used standards and frameworks in the security space are given below for information. These are only illustrative and not comprehensive.

### 7.13.1 ISO 27001

Information security is not just about anti-virus software, implementing the latest firewall or locking down the laptops or web servers. The overall approach to information security should be strategic as well as operational, and different security initiatives should be prioritized, integrated and cross-referenced to ensure overall effectiveness.

ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC)) defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is safe to say that this standard is the foundation of Information Security Management. ISO 27001 is for information security; the same thing that ISO 9001 is for quality – it is a standard written by the world's best experts in the field of information security and aims to provide a methodology for the implementation of information security in an organization. It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the best possible way in the organization.

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks. It is a systematic approach to managing confidential or sensitive information so that it remains secure (which means Available, Confidential and with its Integrity intact). The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts. It encompasses people, processes and IT systems. An Information Security Management System helps us to coordinate all our security efforts – both electronic and physical – coherently, consistently and cost-effectively.

Given the importance of ISO 27001, many legislatures have taken this standard as a basis for drawing up different regulations in the field of personal data protection, protection of confidential information, protection of information systems, management of operational risks in financial institutions, etc.

How the standard works?

ISO 27001 requires that management:

- systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

History

ISO/IEC 27001 is derived from The British Standard BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by BSI in 2002, explicitly incorporating Deming's PDCA process concept, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It was extensively revised in 2013, bringing it into line with the other ISO certified management systems standards and dropping the PDCA concept.

- (a) ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, was an Information Security Management System (ISMS) standard published in October 2005 by ISO/IEC. Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information Security Management Systems – Requirements. It was superseded, in 2013, by ISO/IEC 27001:2013.

**The Plan-Do-Check-Act (PDCA) cycle**

ISO 27001 prescribes 'How to manage information security through a system of information security management'. Such a management system consists of four phases that should be continuously implemented in order to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information.

The PDCA cyclic process is shown in the Fig. 7.13.1 and is explained below:

- **The Plan Phase (Establishing the ISMS)** – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- **The Do Phase (Implementing and Working of ISMS)** – This phase includes carrying out everything that was planned during the previous phase.
- **The Check Phase (Monitoring and Review of the ISMS)** – The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.

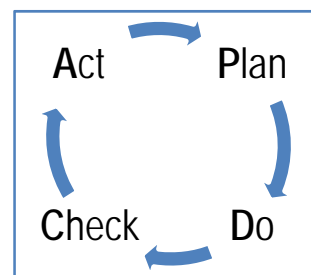


Fig. 7.13.1: PDCA Cycle



- The Act Phase (Update and Improvement of the ISMS) – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

- (b) *ISO/IEC 27001:2013 is the first revision of ISO/IEC 27001 that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization. It is an information security standard that was published on 25<sup>th</sup> September 2013. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. ISO 27001:2013 does not put so much emphasis on this cycle.*

#### Structure

*In the new structure, the Processing Approach, used in ISO27001:2005, and which houses the PDCA model, was eliminated. The reason for this is that the requirement is for continual improvement and PDCA is just one approach to meeting that requirement. There are other approaches, and organizations are now free to use them if they wish. The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.*

*27001:2013 has ten short clauses, plus a long Annex, which covers the following:*

*Clause 1: Scope*

*Clause 2: Normative references*

*Clause 3: Terms and Definitions*

*Clause 4: Context of the organization*

*Clause 5: Leadership*

*Clause 6: Planning*

*Clause 7: Support*

*Clause 8: Operation*

*Clause 9: Performance evaluation*

*Clause 10: Improvement*

*Annex A: List of controls and their objectives*

*ISO/IEC 27001:2013 specifies 114 controls in 14 groups (A.5 to A.18), in contrast to 133 controls in 11 groups in the old standard. A brief mention about the groups and their controls are mentioned below:*

- *A.5: Information security policy (2 controls)*

## 7.41 Information Systems Control and Audit

---

- *A.6: Organization of information security (7 controls)*
- *A.7: Human resource security (6 controls that are applied before, during, or after employment)*
- *A.8: Asset management (10 controls)*
- *A.9: Access control (14 controls)*
- *A.10: Cryptography (2 controls)*
- *A.11: Physical and environmental security (15 controls)*
- *A.12: Operations security (14 controls)*
- *A.13: Communications security (7 controls)*
- *A.14: Information systems acquisition, development and maintenance (13 controls)*
- *A.15: Relationship with external parties (5 controls)*
- *A.16: Information security incident management (7 controls)*
- *A.17: Information security in business continuity management (4 controls)*
- *A.18: Compliance with legal and contractual requirements (8 controls)*

### Changes from the 2005 standard

*The new standard puts more emphasis on measuring and evaluating how well an organization's ISMS is performing, and there is a new section on outsourcing, which reflects the fact that many organizations rely on third parties to provide some aspects of IT. It does not emphasize the PDCA cycle that 27001:2005 did. Other continuous improvement processes like Six Sigma's DMAIC method can be implemented. More attention is paid to the organizational context of information security, and risk assessment has changed. Overall, 27001:2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO 20000, and it has more in common with them.*

*A couple of the major changes to the standard are:*

- *Annex A has been revised and restructured; there are now 114 controls under 14 categories rather than the previous 133 controls under 11 categories.*
- *The Plan-Do-Check-Act Cycle (PDCA) is no longer mandated.*

### Benefits of ISO 27001

The key benefits of ISO 27001 are given as follows:

- It can act as the extension of the current quality system to include security.
- It provides an opportunity to identify and manage risks to key information and systems assets.
- Provides confidence and assurance to trading partners and clients; acts as a marketing tool.

- Allows an independent review and assurance to you on information security practices.

A company may adopt ISO 27001 for the following reasons:

- It is suitable for protecting critical and sensitive information.
- It provides a holistic, risk-based approach to secure information and compliance.
- Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
- Demonstrates security status according to internationally accepted criteria.
- Creates a market differentiation due to prestige, image and external goodwill.
- If a company is certified once, it is accepted globally.

### 7.13.2 Standard on Auditing (SA) 402

Audit Considerations Relating to an Entity using Service Organization, Standard on Auditing (SA) 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24, "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002. The revised Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor.

This SA is effective for audits of financial statements w.e.f. April 1, 2010. Details of this standard are discussed in the Study Material of Advance Auditing paper at Final level of CA Course Curriculum.

### 7.13.3 Information Technology Infrastructure Library (ITIL)

The **IT Infrastructure Library (ITIL)** is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

Although the UK Government originally created the ITIL, it has rapidly been adopted across the world as the standard for best practice in the provision of information technology services. As IT services become more closely aligned and integrated with the business, ITIL assists in establishing a business management approach and discipline to IT Service Management, stressing the complementary aspects of running IT like a business. Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. The core of Service Management is transforming resources into valuable services.

ITIL V3 represents an important change in best practice approach, transforming ITIL from

## 7.43 Information Systems Control and Audit

---

providing a good service to being the most innovative and best in class. At the same time, the interface between old and new approaches is seamless, making adoption simple for those experienced in ITIL V2. ITIL V3 makes the link between ITIL's best practice and business benefits both clearer and stronger. Based on a core of five titles, the changes in ITIL V3 reflect the way IT Service Management has matured over the past decades and change the relationship between IT and business. Whereas previously ITIL worked to align Service Management with business strategy, ITIL V3 integrates into a single lifecycle, and well depicted in Fig. 7.13.2.

This release of ITIL V3 brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set.

- **Service Strategy:** This provides guidance on clarification and prioritization of service-provider investments in services;
- **Service Design:** This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;
- **Service Transition:** This relates to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than Business As Usual (BAU);
- **Service Operation:** This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs), and
- **Continual Service Improvement:** This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.

**Details of the ITIL Framework:** Details of these aforementioned volumes are given as follows:

I. **Service Strategy:** The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers. The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

- ***IT Service Generation:*** *IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.*

- **Service Portfolio Management:** *IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.*
- **Financial Management:** *Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.*
- **Demand Management:** *Demand management is a planning methodology used to manage and forecast the demand of products and services.*
- **Business Relationship Management:** *Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.*

II. **Service Design:** Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.

The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets. Service Design is not limited to new services and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services, taking into account the continuity of services, conformance to standards and regulations and achievement of service levels. It also provides guidance on the development of design capabilities for service management.

- **Service Catalogue Management:** *Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers. Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.*
- **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 is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be; liaising with availability management, capacity management, incident management and problem management.*
- **Availability Management:** *Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost. The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations. Availability management addresses many IT component abilities like reliability, maintainability,*

*serviceability, resilience and security to perform at an agreed level over a period of time.*

- **Capacity Management:** *Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include application sizing; workload management; demand management; modelling; capacity planning; resource management and performance management.*
- **IT Service Continuity Management:** *IT Service Continuity Management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.*
- **Information Security Management:** *A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.*
- **Supplier Management:** *The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements. Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination.*

III. **Service Transition:** Service Transition provides guidance on the service design and implementation ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively. Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation. It provides guidance on the support mechanism on transferring the control of services between customers and service providers. The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations. Guidance is provided on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation, whilst controlling the risks of failure and disruption. It combines the processes in Release, Program and Risk Management and sets them in the practical context of Service Management.

- **Service Transition Planning and Support:** *The service transition planning and support process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes. The service transition planning and support process must incorporate the service design and operational requirements within the transition planning.*
- **Change management and Evaluation:** *This aims to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is an event that results in a new status of one or more configuration items (CIs), and which is*

*approved by management, is cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.*

- **Service Asset and Configuration Management:** *Service Asset and Configuration Management is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships. Configuration management is the management and traceability of every aspect of a configuration from beginning to end.*
- **Release and Deployment Management:** *Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which functions as intended when introduced into existing infrastructure.*
- **Service Validation and Testing:** *The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.*
- **Knowledge Management:** *Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organisational knowledge. It refers to a multi-disciplined approach to achieving organisational objectives by making the best use of knowledge.*

**IV. Service Operation:** Service Operation provides guidance on the management of a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

- **Functions:** The major functions are as follows:
  - **Service Desk:** *The service desk is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage. Tasks include handling incidents and requests, and providing an interface for other ITSM processes. Features include Single Point of Contact (SPOC); Single Point of Entry and Exit; easier for customers and streamlined communication channel.*
  - **Application management:** *ITIL application management 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.*
  - **IT Operations:** *IT Operations primarily work from documented processes and procedures and should be concerned with a number of specific sub-processes, such as: output management, job scheduling, backup and restore, network monitoring/management, system monitoring/ management, database monitoring/management storage monitoring/management.*

## 7.47 Information Systems Control and Audit

- **IT Technical Support:** *IT technical support provides a number of specialist functions: research and evaluation, market intelligence, proof of concept and pilot engineering, specialist technical expertise, and creation of documentation.*
- **Incident Management:** *Incident management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.*
- **Request fulfillment:** *Request fulfillment (or request management) focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.*
- **Event Management:** *An event may indicate that something is not functioning correctly, leading to an incident being logged. Event management generates and detects notifications, while monitoring checks the status of components even when no events are occurring.*

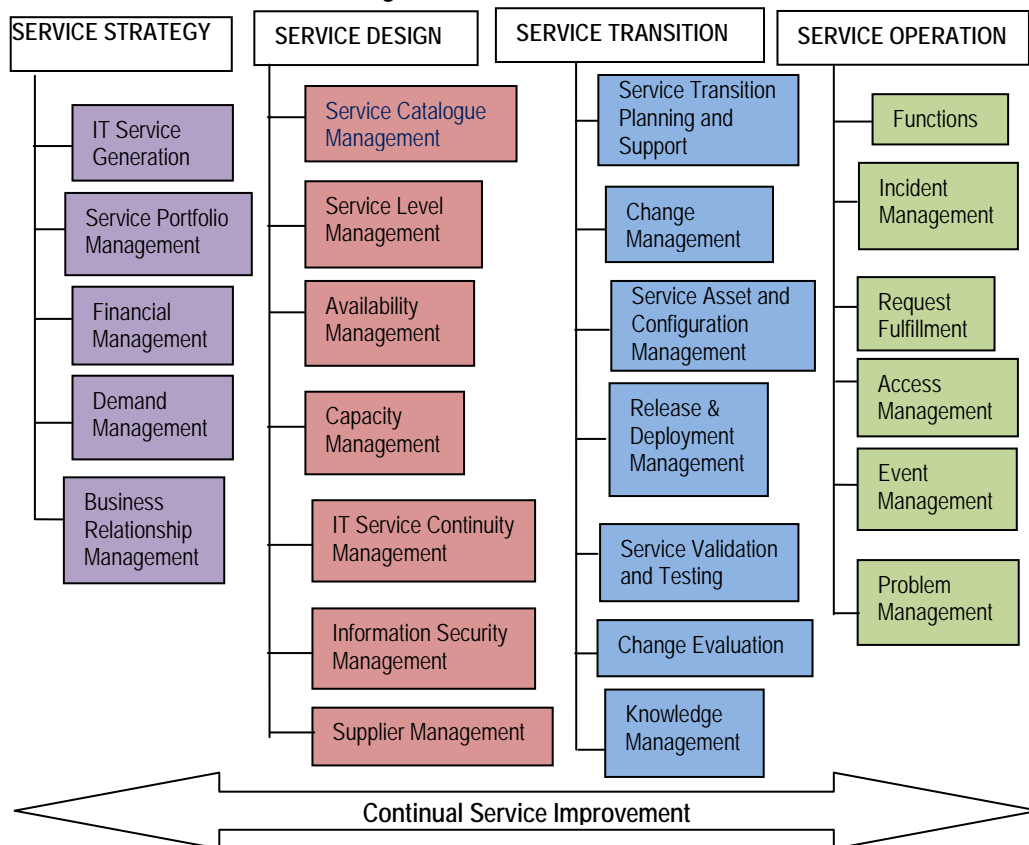


Fig. 7.13.2: ITIL V3

V. **Continual Service Improvement:** Continual Service Improvement provides guidance on the measurement of service performance through the service life-cycle, suggesting



improvements to ensure that a service delivers the maximum benefit. This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services. It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.

It provides guidance on linking improvement efforts and outcomes with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT Service Management processes.

### **7.14 Summary**

The chapter discusses the legal issues relating to Information technology. Chapter elaborates the important provisions of the Information Technology Act, 2000. The chapter also puts the importance of adoption of such a law for growth of e-commerce. The chapter further goes to highlight the requirements regarding system audit/disclosure by other statutes and governing bodies like RBI, SEBI and IRDA. The latter part of the chapter discussed the key aspects of National Cyber Security Policy 2013 and further elaborates various security and related certification standards used by various bodies across the world.

## Emerging Technologies

### Learning Objectives

- To introduce the emerging technologies, their perspectives and other imperatives;
- To understand the paradigm of cloud computing, its goals and utilities in today's computing scenarios;
- To inculcate the concepts of mobile computing, its goals and applications;
- To discuss the application of emerging technologies;
- To sensitize about the emerging issues and the concept of green IT and related security issues; and
- To know the concept of BYOD and Web 2.0 technologies and related challenges.

### Task Statements

- To understand various emerging technologies; and
- To suitably adopt the same in enterprises.

### Knowledge Statements

- To know the concept of cloud computing and mobile computing;
- To know about Green IT and related security issues; and
- To know the concept of BYOD & Web 2.0.

### 8.1 Introduction

Recently, emerging technologies are seen to be having enormous potential to meet the global challenges. One of the high-potential technologies is considered to be informatics. It is expected to revolutionize the value-additions to the huge information component, which is growing exponentially. Technological innovations in the field of storage, mining and services may be the key to address emerging challenges. Though a number of other advance technologies include synthetic biology, Nano-scale design, systems biology, wireless networks, ICT-enhanced educational systems etc. ICT appears to be spearheading all such developments at one or the other levels. In order to add some flavour to address the challenges, some of the technologies, which have recently emerged and are being rapidly adapted include cloud, grid mobile, and green computing.

## 8.2 Cloud Computing

Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. The Internet is commonly visualized as clouds; hence the term “cloud computing” for computation done through the Internet. With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides these, databases in cloud may be highly dynamic and scalable. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is *Google Apps* where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. This model of IT enabled services enables anytime access to a shared pool of applications and resources. These applications and resources can be accessed using a simple front-end interface such as a Web browser, and as a result enabling users to access the resources from any client device including notebooks, desktops and mobile devices.

Cloud computing provides the facility to access shared resources and common infrastructure offering *services on demand over the network* to perform operations that meet changing business needs (shown in Fig. 8.2.1). The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications ‘on the cloud’, which entails virtualization of resources that maintains and manages itself.

With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software. Cloud computing is of particular benefit to small and medium-sized business systems, who wish to completely outsource their data-centre infrastructure; or large companies, who wish to get peak load capacity without incurring the higher cost of building larger data centres internally. In both the instances, service consumers use ‘*what they need on the Internet*’ and *pay only for ‘what they use’*.



Fig. 8.2.1: Clod Computing Scenario\*

\* Source: [www.ibm.com](http://www.ibm.com)

## 8.3 Information Systems Control and Audit

---

The service consumer may no longer be required to pay for a PC, use an application from the PC, or purchase a specific software version that's configured for smart phones, PDAs, and other devices. The consumers may not own the infrastructure, software, or platform in the cloud based schemes, leading to lower upfronts, capital, and operating expenses. End users may not need to care about how servers and networks are maintained in the cloud, and can access multiple servers anywhere on the globe without knowing 'which ones and where they are located'.

### 8.2.1 Cloud vs Grid Computing

Cloud computing evolved from grid computing and provides on-demand resource provisioning. Grid computing may or may not be in the cloud paradigm depending on what type of users are using it. If the users are systems administrators and integrators, they care 'how things are maintained in the cloud'. They upgrade, install, and virtualized servers and applications. If the users are consumers, they do not care 'how things are run in the system'.

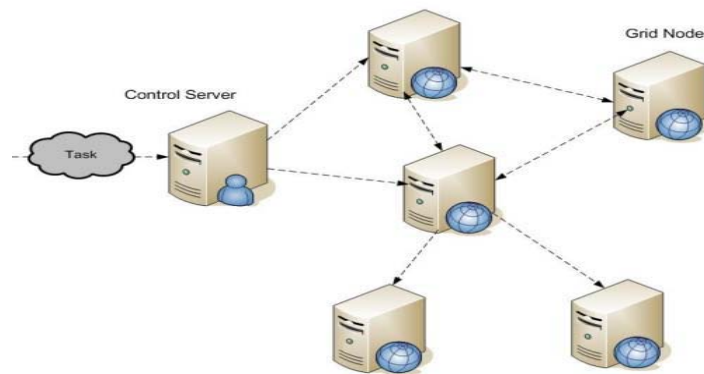


Fig. 8.2.2: Grid Computing Scenario\*

Grid computing requires the use of software that can divide and carve out pieces of a program as one large system image to several thousand computers. One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail (as shown in Fig. 8.2.2). This is alleviated if that component has a failover component on another node, but problems can still arise if components rely on other pieces of software to accomplish one or more grid computing tasks. Large system images and associated hardware to operate and maintain them, can contribute to large capital and operating expenses. Some pertinent similarities and differences are highlighted as follows:

- Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services. CPU and network bandwidth is allocated and de-allocated on demand. The system's storage capacity goes up and down

---

\* Source: [www.ibm.com](http://www.ibm.com)

depending on the number of users, instances, and the amount of data transferred at a given time.

- Both computing types involve multitenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances. Sharing resources among a large pool of users assists in reducing infrastructure costs and peak load capacity. Cloud and grid computing provide Service-Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for receiving data not in stipulated time.
- While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

### 8.2.2 Goals of Cloud Computing

The core goals of utilizing a cloud-based IT ecosystem are to pool available resources together into a highly efficient infrastructure whose costs are aligned with what resources are actually used but to the services accessible and available from anywhere at any time. However, the infrastructure can be quickly and easily scaled as an organization's business requirements evolve. To meet the requirements, some of the pertinent objectives in order to achieve the goals are as follows:

- To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;
- To access services and data from anywhere at any time;
- To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- To consolidate IT infrastructure into a more integrated and manageable environment;
- To reduce costs related to IT energy/power consumption;
- To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- To enable rapidly provision resources as needed.

### 8.2.3 Cloud Computing Architecture

The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves into multiple cloud components communicating with each other over a loose coupling mechanism, such as a messaging

## 8.5 Information Systems Control and Audit

---

queue. Elastic provisioning implies intelligence in the use of tight or loose coupling of cloud resources, services, middleware, and software components.

In the context of cloud computing, protection depends on having the Right Architecture for the Right Application (RARA). Organizations must understand the individual requirements of their applications, and if already using a cloud platform, understand the corresponding cloud architecture. A cloud computing architecture consists of a front end and a back end. They connect to each other through a network, usually the Internet. The front end is the side, the computer user sees and interacts through, and the back end is the "cloud" section of the system, truly facilitating the services, depicted in Fig. 8.2.3, which is given as follows:

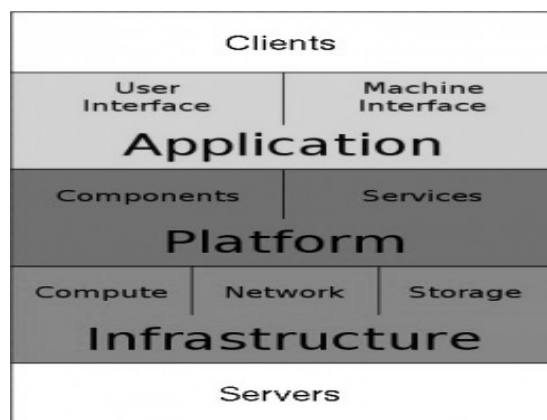


Fig. 8.2.3: Cloud Computing Architecture\*

The details are given as follow:

- **Front End Architecture:** The front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.
- **Back End Architecture:** Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

A central server is established to be used for administering the whole system. It is also used for monitoring client's demand as well as traffic to ensure that everything of system runs

---

\*Source: [www.synergy.gs](http://www.synergy.gs)

without any problem. There are some set of rules, technically referred as protocols, are followed by this server and it uses a special type of software known as middleware. Middleware allows computers that are connected on networks to communicate with each other. If any cloud computing service provider has many customers, then there's likely to be very high demand for huge storage space. Many companies that are service providers need hundreds of storage devices. The cloud computing system must have a redundant back-up system of all the data of its client's.

#### 8.2.4 Cloud Computing Environment

The cloud computing environment can consist of multiple types of clouds based on their deployment and usage. Such typical Cloud computing environments, catering to special requirements, are briefly described as follows (given in Fig. 8.2.4).

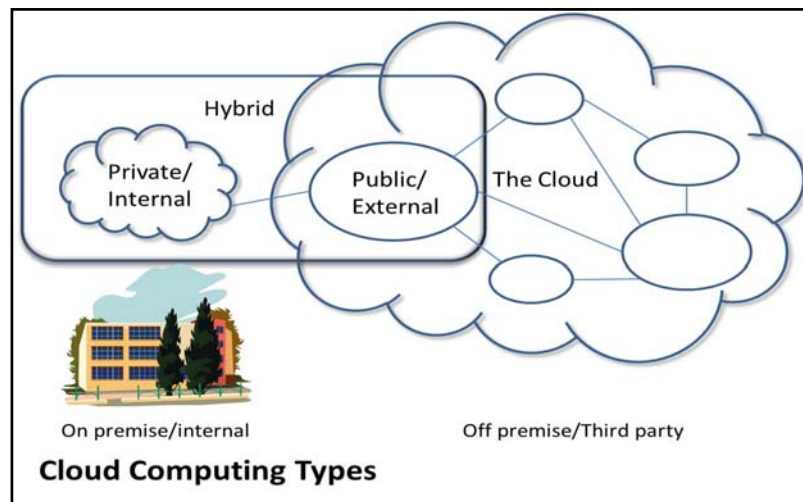


Fig. 8.2.4: Types of Cloud Computing\*

- (a) **Public Clouds:** This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.

The Advantages of public cloud include the following:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.

\*Source: [www.synergy.gs](http://www.synergy.gs)

## 8.7 Information Systems Control and Audit

---

Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.

(b) **Private Clouds:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization. The advantages of private clouds include the following:

- They improve average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.
- High levels of automation is largely responsible for reducing operations costs and administrative overheads

Moreover, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently.

(c) **Hybrid Clouds:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

### 8.2.5 Cloud Computing Models

Cloud computing service providers offer their services on the lines of several fundamental models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Where IaaS is the most basic and each higher model abstracts from the details of the lower models. These are pictorially presented in Fig. 8.2.5. In 2012, Network as a Service (NaaS) and Communication as a Service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models.

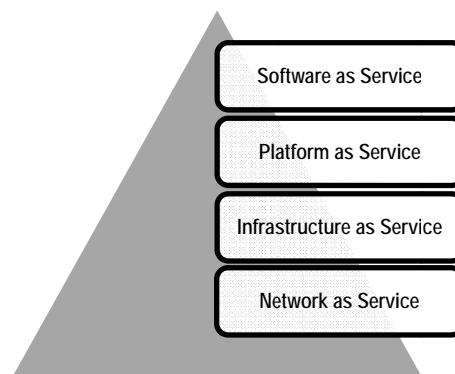


Fig. 8.2.5: Cloud Computing Service Models



- (a) **Infrastructure as a Service (IaaS):** IaaS providers offer computers, more often virtual machines and other resources as service. It provides the infrastructure / storage required to host the services ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure. Examples of IaaS providers include: Amazon EC2, Azure Services Platform, Dyn DNS, Google Compute Engine, HP Cloud, il and etc.
- (b) **Platform as a Service (PaaS):** Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of acquiring and managing the underlying hardware /software layers. In PaaS, one can make applications and software's on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want. All the development tools are provided. Some of examples of PAAS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard etc.
- (c) **Software as a Service (SaaS):** SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.
- (d) **Network as a Service (NaaS):** It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services. NaaS involves optimization of resource allocation by considering network and computing resources as a whole. Some of the examples are: Virtual Private Network, Mobile Network Virtualization etc.
- (e) **Communication as a Service (CaaS):** CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates the large capital investments. Examples are: Voice over IP (VoIP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.

### 8.2.6 Characteristics of Cloud Computing

Cloud computing, typically entails few very important characteristics apart from the popular essentials of the computing paradigms. Few of them are given as follows:

- **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
- **Agility:** The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).

## 8.9 Information Systems Control and Audit

---

- **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
- **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
- **Services in Pay-Per-Use Mode:** SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
- **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- **Performance:** It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Maintenance:** The cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places.

### 8.2.7 Issues relating to Cloud Computing

In spite of its many benefits, as mentioned above, cloud computing also has certain issues. Businesses, especially smaller ones, need to be aware of the same before adapting this technology. Major issues are shown in Fig. 8.2.6 and discussed as follows:

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.
- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be

affected temporarily or permanently, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which lead to data loss and access issues with multiple Web 2.0 services.

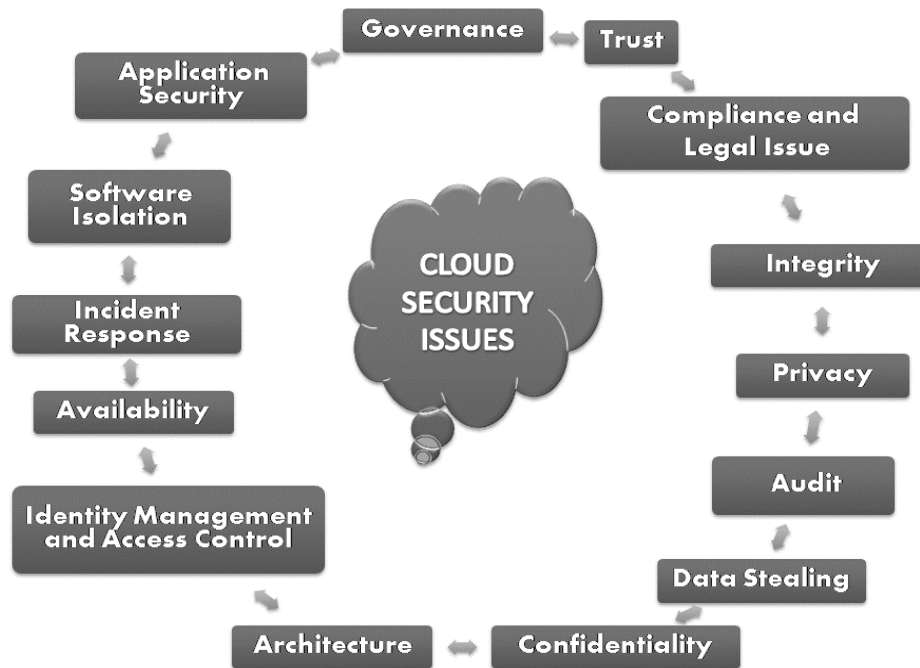


Fig. 8.2.6: Issues in Cloud Security

- **Governance:** Due to the lack of control over the employees and services, it creates problems relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization. The organization gains computational resources as capital expenditures. These actions should be looked by the organization under governance through legal regulation, policies, privacy and security. Auditing and risk management programs are some way to verify the policy, which can shift the risk landscape.
- **Trust:** Deployment model provided a trust to the Cloud environment. An organization has direct control over security aspects as well as the federal agencies even have responsibility to protect the information system from the risk. Trust is an important issue in Cloud. Various clients' oriented studies reveal that Cloud has still failed to build trust between the client and service provider. Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.
- **Legal Issues and Compliance:** There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. One of the major

## 8.11 Information Systems Control and Audit

---

troubles with laws is that they vary from place to place, and users have no assurance of where the data is located physically. There is a need to understand various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements. An approach to monitor and compliance that helps to prepare Cloud Service Provider (CSP) and users to address emerging requirements and the evolution of Cloud models. To achieve efficiency, risk management, and compliance, CSPs need to implement an internal control monitoring function coupled with external audit process. To increase the comfort of Cloud activities, Cloud user define control requirements, internal control monitoring processes, examine applicable external audit reports, and accomplish their responsibilities as CSP users. It is the responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way.

- **Privacy:** Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity. The Cloud should be designed in such a way that it decreases the privacy risk.
- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'. Its security is stronger than the one built in software and application. But, still it consumes more time, insistent across customers, pricy and motivational debilitate for everyone. The context of use of Cloud, time consuming audits seriously detains a key gain of Cloud agility.
- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing. Some of the Cloud providers do not use their own server, instead. They use server/s from other service providers. In that case, there is a probability that the data is less secure and is more prone to the loss from external server. If the external server is shut down due to any legal problem, financial crisis, natural disaster, and fire creates loss for the user. In that case, data protection is an important mechanism to secure the data. Back up policies such as Continuous Data Protection (CDP) should be implemented in order to avoid issues with data recovery in case of a sudden attack.
- **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.
- **Identity Management and Access control:** The key critical success factor for Cloud providers is to have a robust federated identity management architecture and strategy internal in the organization. Using Cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with Cloud providers. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a

public Cloud and extending or changing the existing framework to support Cloud services may prove difficult. Identity Management and Access control provides a secure authentication and authorization to an organization. The identity management provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.

- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Affected networks measures, determined systems, and applications, exposed intrusion vector helps to understand an incident response and the activities carried out must be re-modeled.
- **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture, and evaluate the risks required for the organization.
- **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. To prevent Cloud computing, service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. Infected applications need to be monitored and recovered by the Cloud security drivers.

### 8.2.8 Advantages of Cloud Computing

If cloud computing is used properly and to the extent necessary, working with data in the cloud can vastly benefit all types of businesses. Major advantages of Cloud Computing are given as follows:

- **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- **Almost Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.
- **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
- **Automatic Software Integration:** In the cloud, software integration is usually something that occurs automatically. This means that we do not need to take additional efforts to

## 8.13 Information Systems Control and Audit

---

customize and integrate the applications as per our preferences. This aspect usually takes care of itself. Not only that, cloud computing allows us to customize the options with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.

- **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
- **Quick Deployment:** Lastly and most importantly, cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes. Of course, the amount of time taken here will depend on the exact kind of technology that we need for your business.

### 8.2.9 Pertinent Issues

Just like any other technology, before its progress to stabilization and maturity, cloud computing also has several issues. Some of the well-identified issues stand out with cloud computing are described briefly as follows:

- **Threshold Policy:** Let's suppose, we had a program that did credit card validation in the cloud, and we hit the crunch for the buying season. Higher demand would be detected and more instances would be created to fill that demand. As we moved out of the buying crunch, the need would be diminished and the instances of those resources would be de-allocated and put to other use. In order to test if the program works, develop, or improve and implement, a threshold policy is of immense importance in a pilot study before moving the program to the production environment. Checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work needs to work out in the context. That is working out thresholds is really a matter of concern and would go a long way to assure the effectiveness.
- **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary APIs and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. We may need to reformat/reorganize data or change the logic in applications. Although industry cloud-computing standards do not exist for APIs or data import/export, IBM and Amazon Web Services have worked together to make interoperability happen.
- **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another

instance of incurring network costs, companies, who are far from the location of cloud providers could experience latency, particularly when there is heavy traffic.

- **Unexpected Behaviour:** Let's suppose that credit card validation application works well at our company's internal data centre. It is important to test the application in the cloud with a pilot study to check for unexpected behaviour. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.
- **Security Issues:** Security is a major issues relating to cloud computing. Instead of waiting for an outage to occur, consumers should do security testing on their own checking how well a vendor can recover data. Apart from the common testing practices, what one needs primarily to do is to ask for old stored data and check how long it takes for the vendor to recover. If it takes too long to recover, ask the vendor why and how much service credit we would get in different scenarios. Moreover, in such cases, verifying the checksums match with the original data is a requisite.

Another area of security testing is to test a trusted algorithm to encrypt the data on the local computer, and then try to access data on a remote server in the cloud using the decryption keys. If we can't read the data once we have accessed it, the decryption keys are corrupted, or the vendor is using its own encryption algorithm. We may need to address the algorithm with the vendor. Another issue is the potential for problems with data in the cloud. To protect the data, one may want to manage his/her own private keys. Checking with the vendor on the private key management is no longer a simple as it appears so.

- **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as SLA and security, are allocated to the production cloud. The managers can limit projects to certain clouds. For instance, services from portions of the production cloud can be used for the production configuration. Services from the development cloud can be used for development purpose only. To optimize assets at varying stages of the project of software development, the managers can get cost-accounting data by tracking usage by project and user.
- **Environment Friendly Cloud Computing:** One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data centre and replacing them with

cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems in remote centres, they can be handled more efficiently as a group.

### 8.3 Mobile Computing

It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of the biggest problem of business people on the move i.e. mobility. A primitive scenario of mobile computing in practice is given in the Fig. 8.3.1.

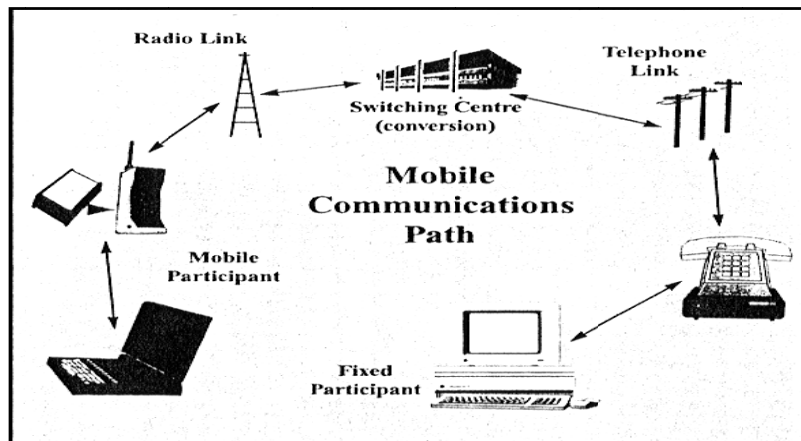


Fig. 8.3.1 Mobile Computing\*

#### 8.3.1 Mobile Computing Services

The ability to share information across a wireless platform is becoming more vital to the today's business communication needs. Various companies design and develop several wireless applications and solutions for Blackberry, iPhone, Google Android G1, iPad, Windows Mobile, Symbian, Brew devices, PDA, Palm & Pocket PC. Mobile Computing Services allow mobile workforces to access a full range of corporate services and information from anywhere, at any time and it improves the productivity of a mobile workforce by connecting them to corporate information systems and by automating paper-based processes.

#### 8.3.2 Mobile Computing Benefits

In general, the mobile computing is a versatile and strategic technology that increases information quality and accessibility, enhances operational efficiency, and improves

\* \*Source: [www.cloud-computer-network.com](http://www.cloud-computer-network.com)



management effectiveness. But, more specifically, it leads to a range of tangible benefits, including the following:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

## 8.4 Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Renowned research organization 'Gartner' has predicted that by 2014, 90% of organizations will support corporate applications on personal devices. Though it has led to an increase in employees satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

In the early 1990s, executing different tasks necessitated the use of different devices. For instance, an mp3 player was needed to listen to music; whereas chores, tasks and schedules were tracked by a PDA. An addition to this, list was a bulky laptop and a camera and it seemed waiting till eternity that we would ever have a single device to suit our different needs. However, remarkable advances in technology in the last decade have made it possible to perform all the above mentioned tasks using a single hi-tech device. Different technologies can work in synergy with each other, which improves user productivity and convenience. The introduction of the Xbox 360 and Apple TV in 2006 are perfect examples of technology convergence as it allows users to play games, listen to music, watch movies and sports on a single black box.

### 8.4.1 Emerging BYOD Threats

Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

## 8.17 Information Systems Control and Audit

---

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.
- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.
- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

### 8.4.2 Mobile Computing and BYOD

Mobile computing, including BYOD is the single most radical shift in business since the PC revolution of the 1980s. Over the next decade, it will have a huge impact on how people work and live, how companies operate, and on the IT infrastructure. These services will focus on the issues and opportunities surrounding the new way to communicate and consume computing services. Mobile computing is not just PCs on the move. Mobile devices such as smart phones, tablets, and the iPod Touch, the last PDA standing are a radically different kind of devices, designed from the ground up as end points of data networks both internal corporate networks and the Internet rather than primarily as stand-alone devices. They are optimized for mobility, which means that they have to be light, easy to handle, and maximize battery life. Where laptops has a three hour battery life, the tablet and smartphone regularly run 12 hours or more between charging and serve as windows into the Cloud.

## 8.5 Social Media and Web 2.0

Related aspects of Social Media and Web 2.0 are given as follows:

### 8.5.1 Social Media

While considering a network, we imagine a set of entities connected with each other on a logical or a physical basis. Physical networks like computer networks are those that can be planned, implemented and managed very optimally and efficiently. However, when we move from physical to logical networks, the visualization becomes much more difficult. Social networks are comprised of the most intelligent components- human beings. Being so, any activity involved with the social networks, be it participation, management, or optimization becomes extremely complicated and context based. Due to the various facets of the human species, we can have multiple types of social networks in all the fields and areas. This can range from a network of researchers, to a network of doctors to a network of academics. Each type of network has its own focus area, member size, geographical spread, societal impact and objective. Managing such networks is not only complicated but requires lot of collective efforts and collaboration. There have been uncountable social networks formed but only a few has finally achieved their true goal/s, which emphasizes the complexity of such a matter.

A social network is usually created by a group of individuals, who have a set of common interests and objectives. There are usually a set of network formulators followed by a broadcast to achieve the network membership. This happens both in public and private groups depending upon the confidentiality of the network. After the minimum numbers are met, the network starts its basic operations and goes out to achieve its goal. Success of a social network mainly depends on contribution, interest and motivation of its members along with technology backbone or platform support that makes the life easier to communicate and exchange information to fulfill a particular communication need.

Implementing social networks and sustaining them is one of the biggest challenges and people have formulated many mechanisms in the past to keep alive such networks. This has been largely supported by the advancements in the field of IT. The large scale computerizations and the powerful advent of E-Commerce have aided this also, but overall, the need for a structured support was and is still there. Web 2.0 has been one of the greatest contributors in this area and it has been a great contributor in the era called 'technology diminishing the humane distance'.

### 8.5.2 Web 2.0

Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over the time, Web 2.0 has been used more as a marketing term than a Computer Science based term. Blogs, wikis, and Web services are all seen as components of Web 2.0. Web 2.0 tries to tap the power of humans connected electronically through its new ways at looking at social collaboration. This is one of the

commonalities between social networks and Web 2.0 - both have people as their fulcrum. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mashups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

The components of Web 2.0 help to create and sustain social. Blogging is the art of social conversation and have replaced personal home pages and this helps for a more consolidated flow of thoughts and ideas. Wikis have enabled collaborative contribution and authoring among distributed teams. Tagging or folksonomy is a collaborative means of identifying information widgets to increase the power of any web site and searching required information in a faster way. Combined with other such concepts, Web 2.0 provides an ideal platform for implementing and helping Social Networks to grow.

### 8.5.3 Components of Web 2.0 for Social Networks

In today's environment, computer literacy is at its peak and tools that are aided through the computerization age are most effective in keeping alive a concept as complicated as Social Networks. The beauty of Web 2.0 fitment to Social Networks is that all the components of Web 2.0 are built for the growth and sustenance of Social Networks. Major components that have been considered in Web 2.0 include the following:

- **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.
- **Blogging:** Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.
- **Wikis:** A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.
- **Folksonomy:** Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.
- **File Sharing/Podcasting:** This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.
- **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

As we see from the above components of Web 2.0, each of them contribute to help the implementation and continued existence of social Networks on a meaningful basis. While wikis and communities help to create an online space for the networks, blogging, folksonomy and

file sharing help to information flow across the virtual world of the social networking community (as shown in Fig. 8.5.1).

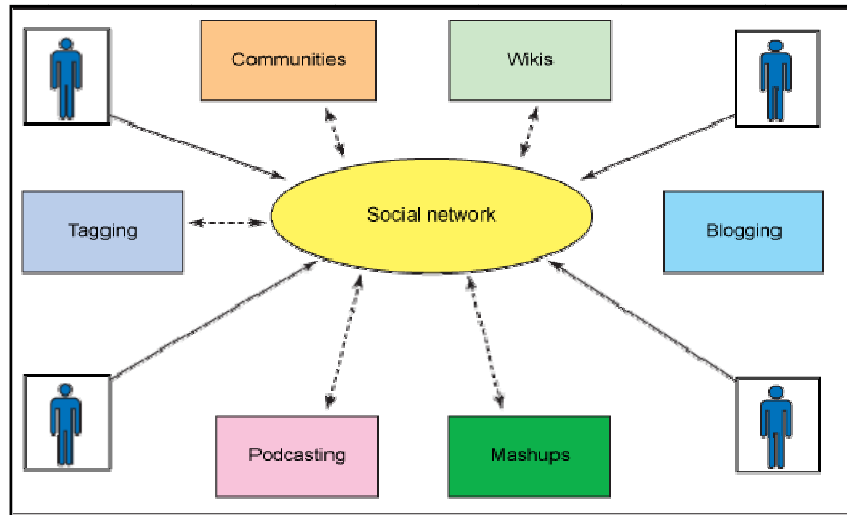


Fig. 8.5.1: Information Flow in Social Networks\*

#### 8.5.4 Types and Behaviour of Social Networks

The nature of social networks makes its variety. We have various types of social networks based on needs and goals. Compartmentalizing social networks is quite a challenging activity. Social networks exist in various domains-within and outside organizations, within and outside geographical boundaries, within and outside social boundaries and many other areas. Such huge variations make the reach of social networks grow to all sectors of the society. Keeping these in mind, the main categories identified are given below:

- **Social Contact Networks:** These types of networks are formed to keep contact with friends and family. These have become the most popular sites on the network today. They have all components of Web 2.0 like blogging, tagging, wikis, and forums. Examples of these include Orkut, Facebook and Twitter.
- **Study Circles:** These are social networks dedicated for students, where they can have areas dedicated to student study topics, placement related queries and advanced research opportunity gathering. These have components like blogging and file sharing. Examples of these include, Fledge Wing and College Tonight.
- **Social Networks for Specialist Groups:** These types of social networks are specifically designed for core field workers like doctors, scientists, engineers, members of the corporate industries. A very good example for this type of network is LinkedIn.

\* Source: www.ibm.com

## 8.21 Information Systems Control and Audit

- **Networks for Fine Arts:** These types of social networks are dedicated to people linked with music, painting and related arts and have lots of useful networking information for all aspiring people of the same line.
- **Police and Military Networks:** These types of networks, though not on a public domain, operate much like social networks on a private domain due to the confidentiality of information.
- **Sporting Networks:** These types of social networks are dedicated to people of the sporting fraternity and have a gamut of information related to this field. Examples of these include Athlinks.
- **Mixed Networks:** There are a number of social networks that have a subscription of people from all the above groups and is a heterogeneous social network serving multiple types of social collaboration.

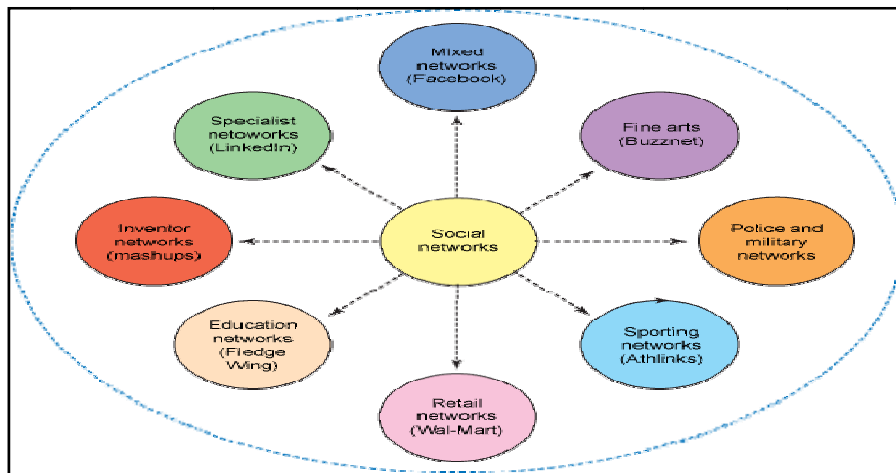


Fig. 8.5.2: Various Social Networks\*

- **Social Networks for the 'inventors':** These are the social networks for the people who have invented the concept of social networks, the very developers and architects that have developed the social networks. Examples include Technical Forums and Mashup centres.
- **Shopping and Utility Service Networks:** The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behaviour and send related information for the same to respective marts and stores.
- **Others:** Apart from the networks outlined above, there are multiple other social networks, which serve huge number of the internet population in multiple ways. Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to a more specialist network as shown in the Fig. 8.5.2.

\* Source: [www.ibm.com](http://www.ibm.com)

### 8.5.5 Life Cycle of Social Networks

The concept of social networks and the components of Web 2.0, which are significant for social networks have been outlined above. Next, we will see how Web 2.0 gets linked with the entire life cycle of a social network. For any social network, there are a number of steps in its life cycle. In each of the life cycle step of an online social network, Web 2.0 concepts have a great influence, as depicted in the Fig. 8.5.3. For all the steps in the life cycle, Web 2.0 provides tools and concepts, which are not only cost effective but very easy to implement. Often, online networks have a tendency to die out very fast due to lack of proper tools to communicate. Web 2.0 provides excellent communication mechanism concepts like Blogging and individual email filtering to keep everyone in the network involved in the day to day activities of the network.

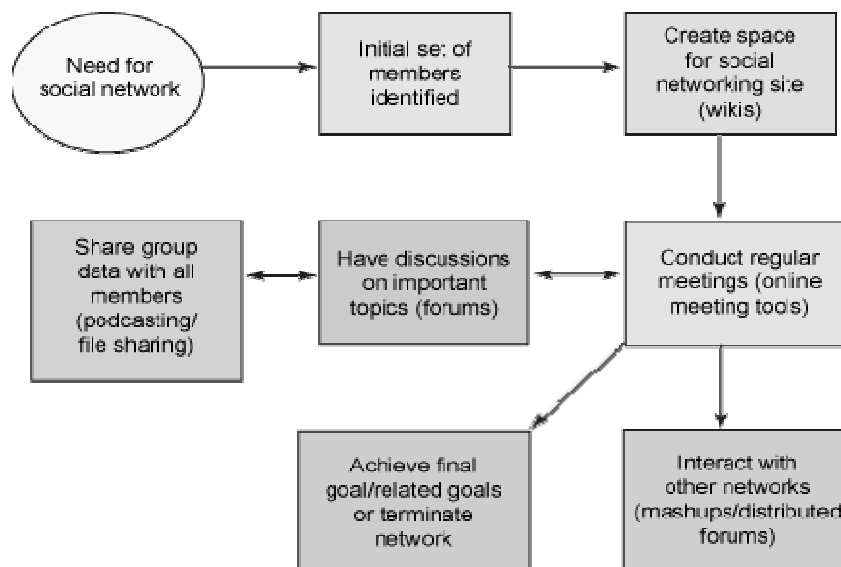


Fig. 8.5.3: Life Cycle of Social Networks with Web 2.0\*

### 8.5.6 Impact of Social Networks Using Web 2.0

Various implementations of social networks using Web 2.0 have already had a profound effect on society as a whole. One of the most important groups of people - the medical community already has reaped significant benefits from the technology and is translating the same towards the betterment of public life. According to a survey conducted by a website, almost "89% of physicians use at least one Web 2.0 tool in their medical practice" along with some other impressive figures that prove how Web 2.0 has been helping in the day-to-day activities. There are numerous reports detailing how doctors are connecting using Web 2.0 for increasing their knowledgebase.

\* Source: [www.ibm.com](http://www.ibm.com)

## 8.23 Information Systems Control and Audit

---

Social networks built on Web 2.0 concepts has become so cost affordable and easy to use that more and more people are migrating to this wave. This has also helped NGO's and other social service organizations to create meaningful social networks to reach out to people in a much more structured manner and in turn benefit the needy and deprived sector of the society.

### 8.5.7 Future Scope of Web 2.0 in Social Networks

There is a lot of contribution that Web 2.0 has already made for social networks as well as other areas. However, the reach for the technology has not been complete and there are still a number of areas that need improvements so that the true power of the technology integrated with social networks can be truly felt. A majority of social networks still operate in an offline and unstructured manner and if proper education on Web 2.0 can be imparted, then a greater number of such networks will come under the wing of social networks.

Areas like space exploration, scientific experimentation, social sciences along with the area of collaborative research through social networks are something that Web 2.0 practitioners can actively contribute. The social impact that the technology is making via social networks is also making aware of the power and flexibility and is making Web 2.0 an integral part of social networks throughout the world.

The future of Web 2.0 itself is something, which will be providing much more exciting features for social networks. As time progresses, the technology is becoming more secure, robust, transparent and much more user-oriented. The concept of semantic Web is being crystallized, which will aid the growth of social networks even more. New features like online video conferencing instead of scrap messages/blogs and Object Oriented Programming will also help in introducing new features within the social network.

### 8.5.8 Benefits and Challenges for Social Networks using Web 2.0

Web 2.0 has provided a number of benefits to social networks. It provides a platform where users of the network need not to worry about the implementation or underlying technology at a very affordable cost and a very easy pickup time. Concepts of Web 2.0 like blogging are some things that people do on a day-to-day basis and no new knowledge skills are required. Web 2.0 techniques are very people centric activities and thus, adaptation is very fast. People are coming much closer to another and all social and geographical boundaries are being reduced at lightning speed, which is one of the biggest sustenance factors for any social network. Using Web 2.0 also increases the social collaboration to a very high degree and this in turn helps in achieving the goals for a social network.

There are a number of challenges that are faced within the implementation of social networks using Web 2.0 concepts. One of the major aspects is data security and privacy and in such public domains, there is a huge chance of data leak and confidentiality loss because there are usually no centrally mandated administrative services to take care of such aspects. Privacy of individual users also arises and can create a huge problem if malicious users somehow manage to perpetuate the social networks. This is more important for public utility networks like doctors and police. A majority of the social networks are offline, and for bringing these under the purview of online social networks, a lot of education and advertising needs to be



done, which itself becomes a cost burden, when the people involved are not computer literate. This becomes more viable in the areas of the world that are developing and do not have the basic amenities. The fact is that these areas are the ones that can benefit the most using social networks in an online mode and a huge amount of effort would be needed to help them using the technologies.

Web 2.0 has introduced a number of powerful features that social networks are utilizing. These have provided significant advances, which can be seen by the worldwide acceptance of networking sites with these technologies. In spite of all challenges, the worldwide acceptance of social networks and its implementation using Web 2.0 is here to stay and flourish. It is up to us to participate in this movement and continue to contribute towards the betterment of the technology and concept for more contribution to the society as a whole.

## 8.6 Green IT

Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.

Green computing is the environmentally responsible use of computers and related resources. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste). One of the earliest initiatives toward green computing in the United States was the voluntary labeling program known as Energy Star. It was conceived by the Environmental Protection Agency (EPA) in 1992 to promote energy efficiency in hardware of all kinds. The Energy Star label became a common sight, especially in notebook computers and displays. Similar programs have been adopted in Europe and Asia.

Government regulation, however well-intentioned, is only part of an overall green computing philosophy. The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment. Some of such steps for Green IT include the following:

- Power-down the CPU and all peripherals during extended periods of inactivity.
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
- Power-up and power-down energy-intensive peripherals such as laser printers according to need.
- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- Use notebook computers rather than desktop computers whenever possible.
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
- Minimize the use of paper and properly recycle waste paper.

## 8.25 Information Systems Control and Audit

---

- Dispose of e-waste according to central, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centres.

### 8.6.1 Green IT Best Practices

From the experience of practicing professionals, there are a range of well identified best-practices. A few of those for assurance purposes are listed as follows:

- Involving stakeholders on campus yields policies and green IT initiatives more likely to be embraced by the campus community.
- Partnering takes advantage of existing efforts and ensures wider reach and more effective use of limited resources.
- Guidelines for using the best practices simplify adaption of green IT by campus users and encourage them to consider green computing practices the norm.
- On-going communication about and campus commitment to green IT best practices to produce notable results.

### 8.6.2 Relevant Facts

All businesses are increasingly dependent on technology, and small business is no exception. We work on our PCs, notebooks and smart phones all day, connected to servers running 24x7. Since the technology refresh cycle is fast, these devices quickly become obsolete, and at some point — more often sooner than later — we dispose of old devices and replace them with new ones. We use massive quantities of paper and ink to print documents, many of which we promptly send to the circular file.

In the process, most businesses waste resources, in the form of energy, paper, money and time — resources we could invest to develop new products or services, or to hire and train employees. Even if we aren't a tree hugger, it makes good business sense to green our IT environment and culture. Fortunately, there are many simple steps one can take to do this, no matter what the size of the business, or how far someone is in the process. Many IT vendors have major initiatives underway to green their products, services and practices. These include building computers with more environmentally friendly materials, designing them to be consume less energy, providing recycling programs to dispose of old systems, developing virtualization and cloud computing alternatives, and providing tips to businesses that want to go green.

### 8.6.3 Green IT Security Services and Challenges

IT solutions providers are offering green security services in many ways. What to look in green security products, the challenges in the security services market and how security services fare in a recession. If administered properly with other green computing technologies, green security can be a cost-efficient and lucrative green IT service for solution providers. The basic aim is to increase the customer's energy savings through green security services and assess that 'how sustainable computing technology can immediately help the environment'. Green IT

services present many benefits for clients as well as providers, but knowing 'how to evaluate a client's infrastructure to accommodate green technology is really a vital issue'.

Moreover, apart from the common security issues, the green security emphasizes the role of security tools, methods and practices that reduce a company's environmental impact. But to estimate the scope, to cope with the lack of green security services in the market and get advice on conserving power and purchasing switches is very important and needs a high level of sensitivity. Learning about the challenges of implementing green security and the best practices is a major hope, as the artifacts are still evolving.

## 8.7 Summary

In this chapter, we have learned about the latest and emerging technologies. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for the Internet so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet.

Cloud computing has started to obtain mass appeal in corporate data centres as it enables the data centre to operate like the Internet through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner. For a small and medium size business (SMB), the benefits of cloud computing is currently driving adaption. In the SMB sector, there is often a lack of time and financial resources to purchase, deploy and maintain an infrastructure such as the software, server and storages. In cloud computing, small businesses can access these resources and expand or shrink services as business needs change. The common *pay-as-you-go* subscription model is designed to let SMBs easily add or remove services and you typically will only pay for what you do use.

Mobile computing is an emerging field of teaching and research. The goal of mobile computing is to work towards true computing freedom (free from the tyranny of location), whereby users can connect to the network from anywhere, anytime and operate as if they were sitting in the "home" office.

Green computing, green IT or ICT sustainability, refers to environmentally sustainable computing. It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, and associated subsystems peripheral devices efficiently and effectively with highly mitigated negative impact on the environment. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.