SET -D

PAPER 4

"Digital Ecosystem and Controls"

Compiled By:- **KAJAL AGARWAL (CA Finalist)**

@LIVINGCALIFE

http://linkedin.com/in/kajal0307

Disclaimer: - All the important topics are highlighted in the ICAI Module on the basis of my memory and discussion with some other people, it is also advised to go through whole module once then focus on the highlighted topics. Kindly do ICAI MCQs of each chapter as they come for around 6-8 marks.

ALL THE BEST !!

SOME OF THE REPEATED QUESTIONS / TOPICS (Based on memory)

1. Phased and parallel changeover
2. Benefit of COSO
3. Integrated test facility def, advantage, disadvantage
4. SCARF
5. CAAT full form
6. IMPS full form
7. IT act 2000 penalty
   - employee has stolen hard disk
   - penalty on company for non-compliance of privacy and security.
   - Punishment for identity theft sec 66C
8. Windfall model/Spiral model/Agile model/ RAD
9. Data protection is combination of data security and data privacy.
10. Hybrid model disadvantages
11. Treat risk- High likelihood low impact
12. Firewall
13. Data mining
14. Tableau
15. Types of AI
16. Cloud computing
17. BCM cycle
18. SDLC phases - Preliminary/ Development/ Post implementation
19. Concurrent audit/ Post implementation audit
20. Preventive / Directive controls
21. Supporting process - HR management
22. Encryption
23. Donught chart
24. Big data disadvantages
25. IAAS
26. SAAS uses
27. Which method can be used for Cash deposit- AEPS
28. MMID is used for?
29. Visa cash is - Debit card
30. If we have IFSC and MMID and Aadhar no. So, the suitable digital payment option ?
31. what is e-rupi
32. The condition for sending money through AEPS
33. Then One Q was related to BHIM UPI payment
34. Q on Robo advisor
35. Q related to who among the below is not eg. of narrow AI
36. Permission less Blockchain applicable to whom
37. 2-3 Q on deployment model of cloud computing
38. 3-4 Q on service model of cloud computing
39. What are 3v of big data
40. Then there was section no. of computer related offence along with penalty, so 3 ques. was related to matching the section no. correctly and penalty.

SET

D

SELF-PACED STUDY MATERIAL

PAPER-4

DIGITAL ECOSYSTEM AND CONTROLS

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

www.icai.org https://boslive.icai.org

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 in the subject. In case students need any clarification or have any suggestion for further improvement of the material contained herein, they may write to the Joint Director, Board 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.

Basic draft of this publication was prepared by CA. (Dr.) Rashmi Goel

Edition	:	March, 2024
Committee/Department	:	Board of Studies
E-mail	:	bosnoida@icai.in
Website	:	www.icai.org
Price	:	₹ /-
ISBN No.	:	978-81-19472-60-4
Published by	:	The Publication & CDS Directorate on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi 110 002 (India)
Printed by	:	

BEFORE WE BEGIN.....

The traditional role of a chartered accountant restricted to accounting and auditing, has now changed substantially and there has been a marked shift towards strategic decision making and entrepreneurial roles that add value beyond traditional financial reporting. The primary factors responsible for the change are the increasing business complexities on account of plethora of laws, borderless economies consequent to giant leap in e-commerce, emergence of new financial instruments, emphasis on corporate social responsibility, significant developments in information technology, to name a few. These factors necessitate an increase in the competence of chartered accountants to take up the role of not merely an accountant, auditor or more specifically an IS Auditor, but a global solution provider. Towards this end, the scheme of education and training is being continuously reviewed so that it is in sync with the requisites of the dynamic global business environment; the competence requirements are being continuously reviewed to enable aspiring chartered accountants to acquire the requisite professional competence to take on new roles.

Under the New Scheme of Education and Training, the content of the study material of the **"Paper: Digital Ecosystem and Controls"** under Self-paced Online Module Set D is to provide the understanding of Governance and Management of Digital Ecosystem, Information Systems Life Cycle, Information System's Control, Digital Data and Analysis and Digital Economy. The overall learning objective of this paper **"To develop competencies and skillsets 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, financial technologies and compliance services"** has been kept in mind while developing the material. The process of learning should help you inculcate the requisite IT skill-sets necessary for achieving the desired professional competence.

Requirement of Professional Knowledge and Skills

Students are required to learn and qualify Self-paced Online Modules after passing Intermediate Examination but before appearing in Final Examination. Accordingly, they are expected to not only acquire professional knowledge but also the ability to apply such knowledge in addressing issues and problem solving. The integrated process of learning through academic education and practical training will help inculcate in them, the requisite technical competence, and professional skills.

Framework of Chapters: Uniform Structure comprising of specific components

Efforts have been made to present the content of Digital Ecosystem and Controls in a lucid manner. Care has been taken to present the chapters in a logical sequence to facilitate easy understanding by the students. Each chapter of the Study Material has been structured uniformly and comprises of the following components:

S. No.	Components of each chapter	About the component
1	**Learning Outcomes**	This lists the understanding and skill set to be acquired by you after the thorough reading of the chapter.
2	**Chapter Overview**	As the name suggests, this chart/table would give you an overall outline of the contents covered in the chapter.
3	**Illustration**	Illustration is provided at the beginning of each chapter to provide an overview of the topics discussed in the specified chapter.
4	**Introduction**	A brief introduction is given at the beginning of each chapter which would help you to get acclimatized with the broad coverage of the topics.
5	**Content**	The concepts are explained in a student-friendly manner and illustrated with the aid of examples/illustrations /diagrams/tables. These value additions would help you develop conceptual clarity and get a good grasp of the topic.
6	**Summary**	A summary of the chapter provides quick recapitulation of the topics covered in the chapter.
7	**Test your Knowledge**	This comprises of Multiple-Choice Questions which test the breadth and depth of your understanding of the entire chapter.

Chapter-wise coverage of various topics in the study material are as follows:

UNIT I: GOVERNANCE AND MANAGEMENT OF DIGITAL ECOSYSTEM

- **Chapter 1 - Concepts of Governance and IT Strategy** introduces the concept of Governance, its framework, and the impact of their automation with the help of Technology. The chapter focusses on the role of Information technology and alignment of Information Systems strategy with business strategy. Further, it provides an insight into IT Governance, Enterprise Governance and Corporate Governance. This chapter

also discusses COBIT framework and Information Technology Infrastructure Library (ITIL).

- **Chapter 2 - Governance, Risk, and Compliance (GRC) Framework** familiarizes with the concept of Governance, Risk, and Compliance. It further discusses the concept of risks, its related terms and risk classification system. The chapter focuses on various types of risks and their mitigation strategies. Various types of malicious attacks and malicious software are also emphasized with the applicable counter measure to prevent or reduce threats.
- **Chapter 3 – Enterprise Risk Management Framework** disseminates the basic concept of Enterprise Risk Management and its related benefits. The chapter deals with implementation of Enterprise Risk Management in organization by Plan, Implement, Measure and Learn (PIML) methods.
- **Chapter 4 – Information System Security Policy** provides the meaning, components of an information system and the working of various components of an information system. It deals with the needs for protection of information systems. This chapter provides an insight on information security policies, procedure, related standards, and guidelines along with the need for information security and the prospects of frauds relating to technology.
- **Chapter 5 – Business Continuity Planning and Disaster Recover Planning** brings into light the core concepts of Business Continuity Planning (BCP) and the key phases in the development of BCP. It also includes the Business Continuity Management Process and various types back up plans and their working. Furthermore, the chapter highlights the key aspects included in implementation of incident Management plan and various areas involved in Disaster Recovery Procedural Plan.

UNIT II: INFORMATION SYSTEMS LIFE CYCLE

- **Chapter 6 – System Development Life Cycle** focuses on the need for development of an information system. It deals with the system development process for an information system. Various stages of system development life cycle are also discussed. Various tools and techniques of system analysis and design and programming are also briefly covered in this chapter.
- **Chapter 7 – System Acquisition and Development Methodologies** devoted to system acquisition and its phase wise activities, methods, tools, controls, etc. it provides the insight on software procurement, acquisition from external sources and evaluation of IT proposals.

It provides the details on various SDLC models with their pros and cons and understanding of the most appropriate model for a particular project.

UNIT III: INFORMATION SYSTEMS' CONTROL

- **Chapter 8 – Information Systems' Control and its Classification** provides a detailed discussion on IS controls, their objective, 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 9 – Information Technology Tools** devoted to auditing of Information system. It highlights the working of various Information technology tools. Furthermore, this chapter discusses the various illustrations to provide insight on risks and controls associated with different business processes such as P2P, O2C, CASA, etc.

UNIT IV: DIGITAL DATA AND ANALYSIS

- **Chapter 10– Digital Data and Privacy** devoted to various concepts of data protection and its principles. Data Analysis and the tools devoted for data protection have been discussed in the chapter. This chapter also provides highlights on Digital Personal Data Protection Act, 2023.
- **Chapter 11– Business Intelligence** deals with the concept of Business Intelligence and its life cycle and functionality. It also discusses the various Business Intelligence tools used in any organization.

UNIT V: DIGITAL ECONOMY

- **Chapter 12– ABCD of Fintech** is devoted to ABCD technologies i.e. Artificial Intelligence, Blockchain, Cloud Computing and Big Data used in Fintech. It provides insight on usage of these technologies in any financial institutions. It highlights the various components, working, advantages and disadvantages of these technologies.
- **Chapter 13– Emerging Technologies** is devoted to emerging technologies. Major evolving technologies/concept such as Internet of Things (IoT), Quantum computing, Regtech and mobile computing. This chapter also deals with various modes of digital payment used in today's world along with their advantages and disadvantages. The applications of these technologies are covered in this chapter.

This study material covers both concepts and practical aspects and hence, students are advised to read the study material not only from examination point of view but also from practical perspective of how this is relevant and can be applied in any work environment.

Happy Reading and Best Wishes!

SYLLABUS – SELF PACED

SET – D

PAPER-4 : DIGITAL ECOSYSTEM AND CONTROLS (100 MARKS)

Objective

"To develop competencies and skillsets 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, financial technologies and compliance services".

Contents

Unit – I : Governance and Management of Digital Ecosystem

- Key concepts of Governance and IT strategy.
- Governance, Risk, and Compliance (GRC) Framework.
- Risk fundamentals and related terms, Sources, and types of risks.
- Enterprise Risk Management Framework.
- Information Systems Security Policy.
- Business Continuity Planning and Disaster Recovery Planning.

Unit – II: Information Systems Life Cycle

- Information System Acquisition.
- Information System Development Methodologies.
- Information Systems Implementation and Maintenance.

Unit – III: Information Systems' Control

- Information Systems' Control and its Classification.
- Overview of Information Technology Tools.
- Illustrations on Risks and Controls of Specific Business Processes.

Unit – IV: Digital Data and Analysis

- Data Privacy.
- Data Assurance.
- Introduction to Personal Data Protection Act, 2023.
- Regulatory Compliance in terms of relevant sections of Information Technology Act, 2000.
- Introduction to Data Analytical Tools and Techniques.
- Introduction to Business Intelligence (BI) Tools and Techniques.

Unit – V : Digital Economy

- ABCD of Fintech.
- Digital Payments, Digital Currency, and Cryptocurrency.
- e-business and their associated risks and controls.
- Emerging Technologies and Concepts.

ai technology ,emerging technology,it control,cobit..4400no,,iitr framewrk(impt)
digital data....control ...case study,,(konse control)
data anytical tools(stastical.predective analysis)data visualisation,fair information practice (digital data)

data 2 factor authentication
data loss
access control(ee access na kai pai
coso(communitee of sponsering objective)
icai mcqs

DETAILED CONTENTS

UNIT-I : GOVERNANCE AND MANAGEMENT OF DIGITAL ECOSYSTEM

Page No.

CHAPTER-1: CONCEPTS OF GOVERNANCE AND IT STRATEGY

CHAPTER-2: GOVERNANCE, RISK, AND COMPLIANCE FRAMEWORK

UNIT-III : INFORMATION SYSTEMS' CONTROL

CHAPTER 8: INFORMATION SYSTEMS' CONTROL AND ITS CLASSIFICATION

CHAPTER 9: INFORMATION TECHNOLOGY TOOLS

UNIT-IV : DIGITAL DATA AND ANALYSIS

CHAPTER 10 : DIGITAL DATA AND PRIVACY

CHAPTER 13 : EMERGING TECHNOLOGIES

UNIT – 1
GOVERNANCE AND MANAGEMENT OF DIGITAL ECOSYSTEM

CHAPTER 1

CONCEPTS OF GOVERNANCE AND IT STRATEGY

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- build an understanding of the concepts of governance, its framework, and related terms.
- understand the role of Information Technology (IT) in real life time, how to align Information Systems (IS) strategy with business strategy and ensure business value from use of it.
- distinguish among key concepts of governance like - IT governance, enterprise governance, and corporate governance.
- comprehend the knowledge about the COBIT framework and Information Technology Infrastructure Library (ITIL).
- get acquainted with ISO 27001 standard.

CHAPTER OVERVIEW

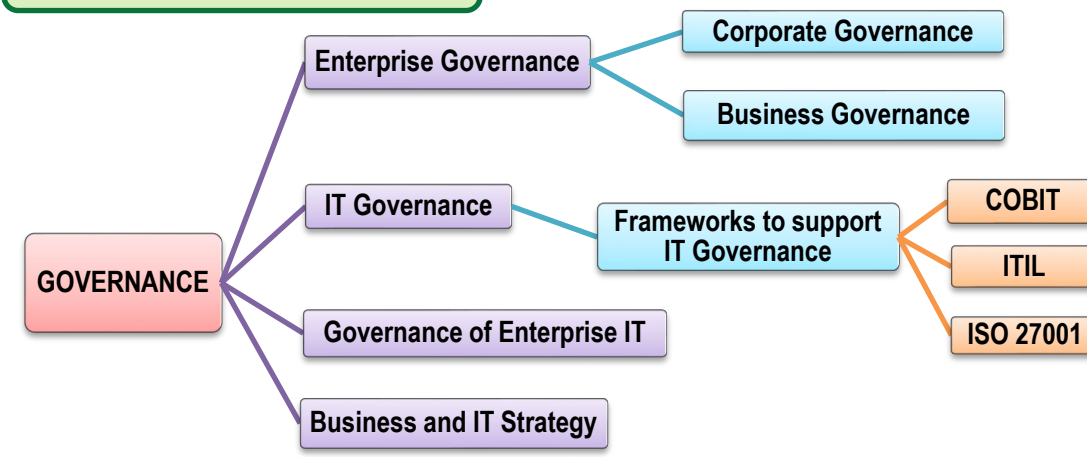


Illustration: Governance in an Organisation

Mr. Sunil had been working in the manufacturing unit of an organization for the past 18 years. On an unfortunate day, he met with an accident on duty and died on the spot. His family demanded compensation. However, the organization denied compensation because it was revealed in the investigation that he was drunk at the time of the accident. The workers of the company went on strike demanding compensation for the family of the deceased. The Chairman of the management board has asked for your recommendation. What recommendation would you provide to the management? Discuss the merits and demerits of each of the recommendations.

Option 1: Let the law take its own course. As the worker was drunk during duty, the company cannot be held responsible for his death. This may sound right as the worker was bound to follow rules at the place of work. However, the strike by the remaining workers could affect the image and productivity of the company. No matter the outcome, the trust between workers and the management would be lost.

Option 2: Recommend the company to offer compensation. But this would set a bad precedent among the management as well as the workers. To offer compensation would mean to let down the safety regulations of the company. The management may also not appreciate the payment as they were not liable for compensation due to negligence of rules showed by the worker.

Option 3: Recommend the management to offer alternative employment to the kin of the deceased. Push the management to adopt stricter prevention and safety measures. The third option is suitable as it would be better to bring the situation under control. The workers could be placated if the kin of the deceased would be offered a job. And also the company may prefer to not lose image and man-days due to the strike.

1.1 INTRODUCTION

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 is shared among many people in the enterprise and when accountability is shared, governance comes into play.

The term "**Governance**" is derived from the Greek verb meaning "to steer" and is a very general concept that can refer to all manner of organizations and can be used in different ways.

- 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 led 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, to satisfy specific enterprise objectives.

Three Principles for a Governance Framework

The three principles for a governance framework are shown in the Fig. 1.1:

1. **Based on Conceptual Model:** A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.
2. **Open and Flexible:** A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency.
3. **Aligned to major standards:** A governance framework should align to relevant major related standards, frameworks, and regulations.

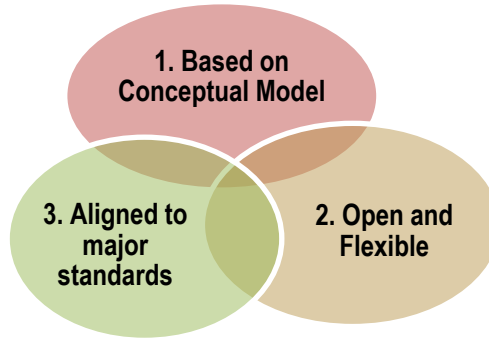


Fig. 1.1: Governance Framework Principles

Many people believe that governance and management are synonymous, but they are not. Governance is about decision making, while management is about making sure that the enterprise's governance process is executed. The perspective of IT governance is distinct in case of definition of new processes and creation of process that are used to produce goods and service from business.

A **governance process** defines the chains of responsibility, authority, and communication to empower people, as well as to define the measurement and control mechanisms to enable people to carry out their roles and responsibilities. Thus, a governance activity is intentionally designed to define organizational structures, decision rights, workflow, and authorization points to create a target workflow that optimally uses a business entity's resources in alignment with the goals and objectives of the business.

A **management process** is the output of the governance process. Unlike a governance process, a management process implements the specific chain of responsibility, authority, and communication that empowers people to do their day-to-day jobs. The management process also implements appropriate measurement and control mechanisms that enable practitioners the freedom to carry out their roles and responsibilities without undue interruption by the executive team. Essentially the management process is implementation of the polices and process defind in the governance process.

Benefits of Governance

Governance is a general concept that can refer to all manners of organizations and can be used in different ways. However, some of the major benefits of governance are 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.
- 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.

1.2 ENTERPRISE GOVERNANCE

We shall here understand what is meant by the term- **Enterprise Governance**.

- It 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.

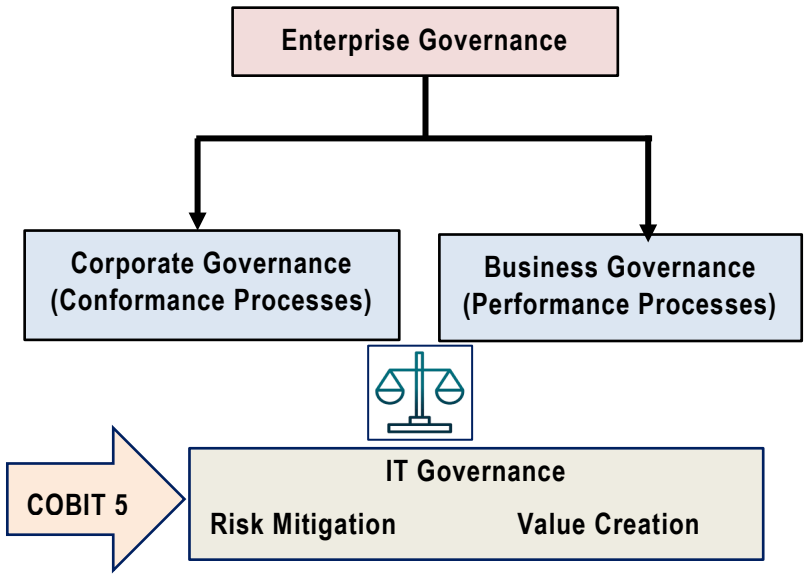


Fig. 1.2: Relation between Enterprise Governance, Corporate Governance, and IT Governance

The enterprise governance constitutes the entire accountability framework of an organization as it involves establishing accountability for decision-making.

As shown in Fig. 1.2, Enterprise Governance has two dimensions **Corporate Governance or Conformance**, and **Business Governance or Performance**. The key message of enterprise governance is that an enterprise must balance the two dimensions of conformance and performance to meet stakeholder requirements and ensure long-term success. To ensure success of business, both conformance and performance must go hand in hand Corporate governance may create administrative hurdles for performance of business if a practicable approach is not followed.

Corporate Governance

- The Corporate Governance provides a holistic view and focuses on regulatory requirements and 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. 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. The conformance dimension is monitored by the audit committee.
- The Regulatory requirements and standards generally address conformance dimension with compliance to establish 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 such compliances from conformance perspective.
- Good corporate governance exhibit following characteristics:
  - It 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.

- Good corporate governance is important, and it is critical 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.

Business Governance

- **Business Governance** is proactive 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 performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism comparable to the audit committee. Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred 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 OVERVIEW OF 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 is a critical success factor for the achievement of business objectives. IT must 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.

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 objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact 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 are required to be well structured and defined 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. Adequate care is to be taken to ensure that IT governance benefits should give measurable benefits so that the importance can be emphasized to Boards.

1.3.1 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 the following depicted in the Fig. 1.3:

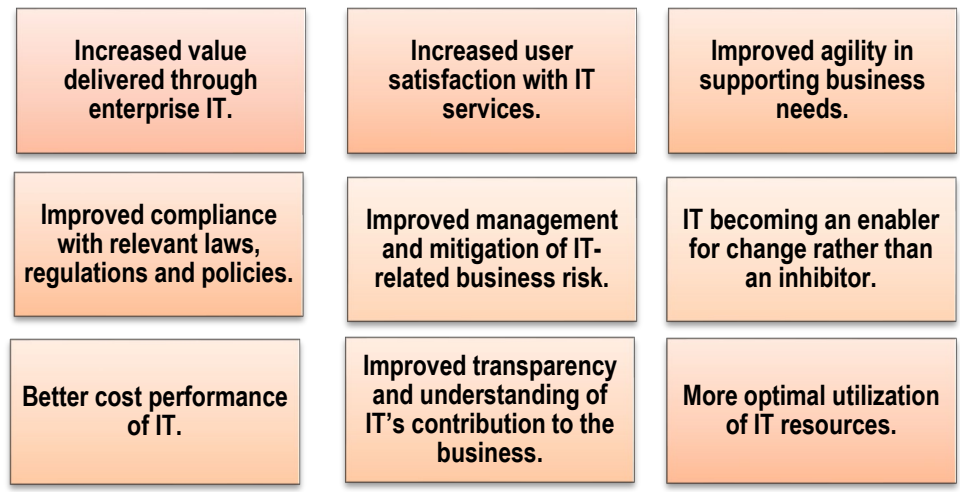


Fig. 1.3: Benefits of IT Governance

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

- ownership is defined and agreed.
- it is relevant and links to 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.
- timely and accurate data for the measure is available or is easy to obtain.

1.3.2 Key practices to determine status of IT Governance

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

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

As per regulatory requirements and best practice 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 in an enterprise. 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.

1.4 GOVERNANCE OF ENTERPRISE IT (GEIT)

Governance of Enterprise IT is a subset 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. Refer Fig. 1.4 to know about the benefits of GEIT.

Benefits of GEIT

- Provides a consistent approach integrated and aligned with the enterprise governance approach.
- Ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.
- Ensures that IT-related processes are overseen effectively and transparently.
- Confirms compliance with legal and regulatory requirements.
- Ensures that the governance requirements for Board members are met.

Fig. 1.4: Benefits of GEIT

1.4.1 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.
- **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.

1.4.2 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. 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. With the advancement of technology, control process can be checked in real time for all transaction instead of merely testing for samples. Further, extensive organization restructuring, or business process re-engineering may be facilitated through IT deployments. Implementing IT must consider not only the 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.

1.4.3 EGIT (Enterprise Governance of Information and Technology)

In the light of digital transformation, Information and Technology has become crucial in the support, sustainability, and growth of enterprises. Previously, governing Boards (Boards of directors) and senior management could delegate, ignore, or avoid IT-related decisions which is not the case now.

Enterprise governance of IT is a relatively new concept that is gaining traction in both the academic and practitioner worlds. Given the centrality of I&T for enterprise risk management and value generation, a specific focus on Enterprise Governance of Information and Technology (EGIT) has arisen over the last three decades.

Going well beyond the implementation of a superior IT infrastructure, enterprise governance of IT is about defining and embedding processes and structures throughout the organizations that enable both business and IT people to execute their responsibilities, while maximizing the value created from their IT-enabled investments.

EGIT is an integral part of overall enterprise governance and is focused on IT performance and the management of risk attributable to the enterprise's dependencies on IT. It is exercised by the Board that oversees the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from I&T-enabled business investments.

1.5 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 adopted, relevant policies and procedures are formulated. From a 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 strategies separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business plan 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. The IT function will be aiding in each of this role to make an effective strategy of the business.

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 consultation 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 a 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. The policies and procedures along with control has to be embedded in the IT system for effective management.

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 organization to perform on a tactical basis and to guide the efforts of personnel to improve maturity of practices. The results will enable the IT functions 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. Auditors are even called upon to check the operation and effectiveness of the controls both as part of confirmatory function in IS assurance and risk mitigation.

1.5.1 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. This is achieved 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.

1.5.2 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 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 functional 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 IT Steering Committee would include the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives.
- To establish the 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 the result of IT projects in terms of return on investment, etc.
- To review the status of IS plans and budgets and overall IT performance. exm

- To review and approve standards, policies and procedures.
- To make decisions on all key aspects of IT deployment and implementation. exm
- 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.
- To report to the Board of Directors on IT activities on a regular basis. exm

1.5.3 IT Strategic Planning

The strategic planning has to be dynamic in nature and IT management and business process owners should ensure that 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 plans 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 based on feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

1.5.4 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:

(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 organizational 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. For an organization to thrive, 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 must focus on striking an optimum balance of IT opportunities and IT business requirements as well as

ensuring its 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 as follows:

- Robust 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 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. 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.
- 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. 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:** Based on the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan that includes:

- specific application systems to be developed and an associated time schedule.
- hardware and software acquisition/development schedule.
- facilities required.
- organization changes required.

Senior management is responsible for developing and implementing long and short-range plans that enable the 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. The 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 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.

1.5.5 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:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Also consider 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. It is advisable to 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.

1.5.6 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 IT costs, benefits and risk is implemented. Some of the key metrics which can be used for such evaluation are as follows:

- 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.
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.
- Benchmarking the benefits realized with the industry practice and evaluation of industry matrices vis a vis company.

1.6 FRAMEWORKS TO SUPPORT EFFECTIVE IT GOVERNANCE

There are several formal frameworks that are identified in any survey of IT governance frameworks. An organization that adopts and pursues an IT governance framework must ensure that it satisfies four separate audiences: **Customers, Stakeholders, Regulators,** and the **Board Members** themselves.

- **Customers** need some certainty that their supplier will be around for the long term, that their personal or business details won't be exposed, and that they will get what they are paying for—whether it's quality, services, or goods.
- **Stakeholders** (including shareholders, employees, and suppliers) also want to be sure that the organization will be around for the long term, and that their investment (of shareholder cash, uncompensated labor, or as-yet unpaid invoices) is not only safe but likely to turn into better—through effective leveraging of IT and intellectual assets combined with clear-sighted, transparent management and control of the ICT (Information and Communications Technology) infrastructure within the context of the business model and business strategy.
- **Regulators** want to be convinced that their regulations are and will continue to be adhered to.
- The **Board members** want to be sure that their reputations will survive their time at the organization and that a personal contribution to the settlement of a class action suit never become an issue for them.

1.6.1 COBIT as an IT (Information and Technology) Governance Framework

Over the years, best-practice frameworks have been developed and promoted to assist in the process of understanding, designing and implementing Enterprise Governance of IT (EGIT). COBIT® 2019 builds on and integrates more than 25 years of development in this field, not only incorporating new insights from science, but also operationalizing these insights as practice. From its foundation in the IT audit community, COBIT® has developed into a broader and more comprehensive Information and Technology (I&T) governance and management framework and continues to establish itself as a generally accepted framework for I&T governance.

COBIT is a framework for the governance and management of information and technology, aimed at the whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organization but encompasses broader concept.

The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organizational structures and serve different purposes.

- **Governance** ensures that:
  - stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives.
  - direction is set through prioritization and decision making.
  - performance and compliance are monitored against agreed-on direction and objectives.

  In most enterprises, 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** plans, builds, runs, and monitors activities, in alignment with the direction set by the governance body, to achieve enterprise objectives.

In most enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO). COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.

Misconceptions about COBIT

- Its not a full description of the whole IT environment of an enterprise.
- Its not a framework to organize business processes.
- It is not an (IT) technical framework to manage all technology.
- It does not make or prescribe any IT-related decisions.

COBIT defines the design factors that should be considered by the enterprise to build a best-fit governance system. COBIT addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

It will not decide what the best IT strategy is, what the best architecture is, or how much IT can or should cost. Rather, COBIT defines all the components that describe which decisions should be taken and how and by whom they should be taken.

COBIT Principles

COBIT® 2019 was developed based on two sets of principles:

(i) Principles that describe the core requirements of a **governance system** for enterprise information and technology.

(ii) Principles for a **governance framework** that can be used to build a governance system for the enterprise.

Six Principles for a Governance System

The six principles for a **Governance System** are depicted in the Fig. 1.5:

(i) **Provide Stakeholders value:** Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.

(ii) **Holistic approach:** A governance system for enterprise I&T is built from several components that can be of different types and that work together in a holistic way.

(iii) **Dynamic Governance System:** A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.

(iv) **Distinct Governance from Management:** A governance system should clearly distinguish between governance and management activities and structures.

(v) **Tailored to enterprise needs:** A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.

(vi) **End-to-end Governance System:** A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless of where the processing is located in the enterprise.

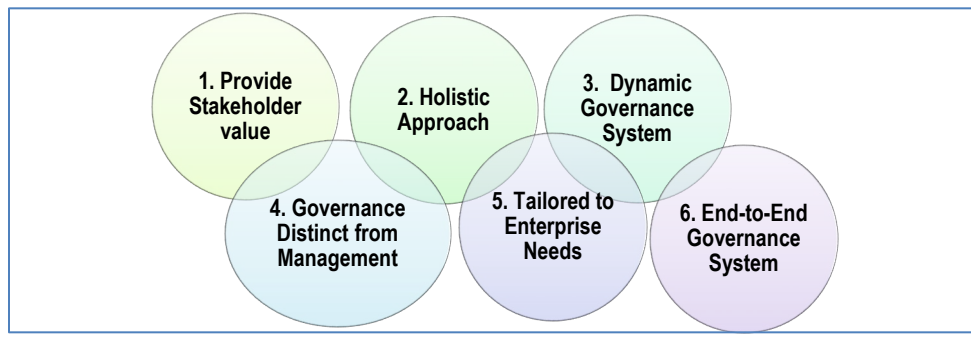


Fig. 1.5: Principles of Governance System

Governance and Management Objectives

For information and technology to contribute to enterprise goals, several governance and management objectives should be achieved. Basic concepts relating to governance and management objectives are as follows:

1. A governance or management objective always relates to one process (with an identical or similar name) and a series of related components of other types to help achieve the objective.

2. A governance objective relates to a governance process, while a management objective relates to a management process. Board and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.

COBIT® 2019 includes 40 governance and management objectives organized into five domains – **EDM, APO, BAI, DSS** and **MEA**. The domains have names with verbs that express the key purpose and areas of activity of the objective contained in them. Refer Fig. 1.6:

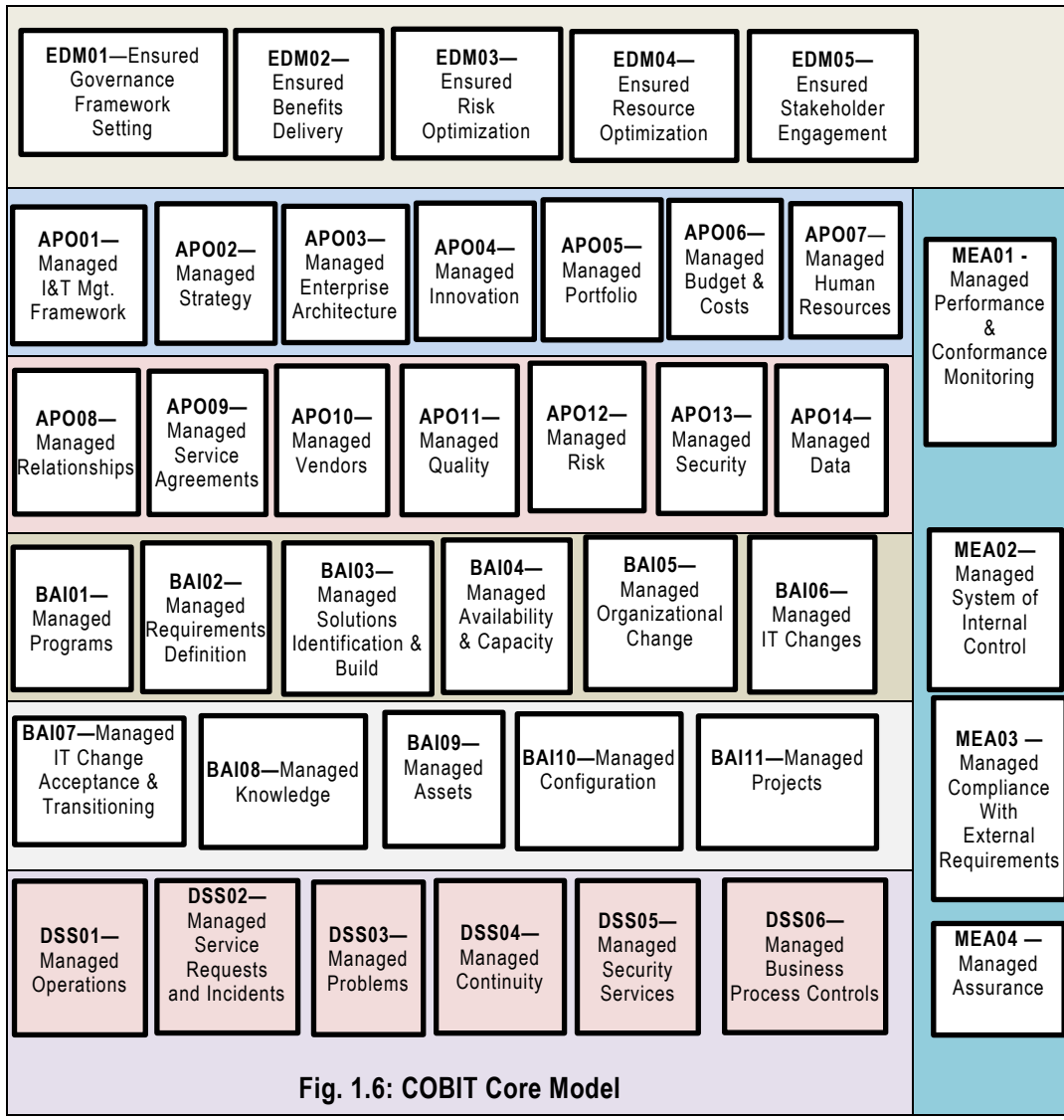


Fig. 1.6: COBIT Core Model

(i) **Governance objectives** are grouped in the **Evaluate, Direct and Monitor (EDM) domain (EDM01 to EDM05)**. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.

(ii) **Management objectives are grouped in four domains:**

- **Align, Plan and Organize (APO01 to APO14)** addresses the overall organization, strategy and supporting activities for I&T.
- **Build, Acquire and Implement (BAI01 to BAI11)** treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
- **Deliver, Service and Support (DSS01 to DSS06)** addresses the operational delivery and support of I&T services, including security.
- **Monitor, Evaluate and Assess (MEA01 to MEA04)** addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

Components of the Governance System (Refer Fig. 1.7)

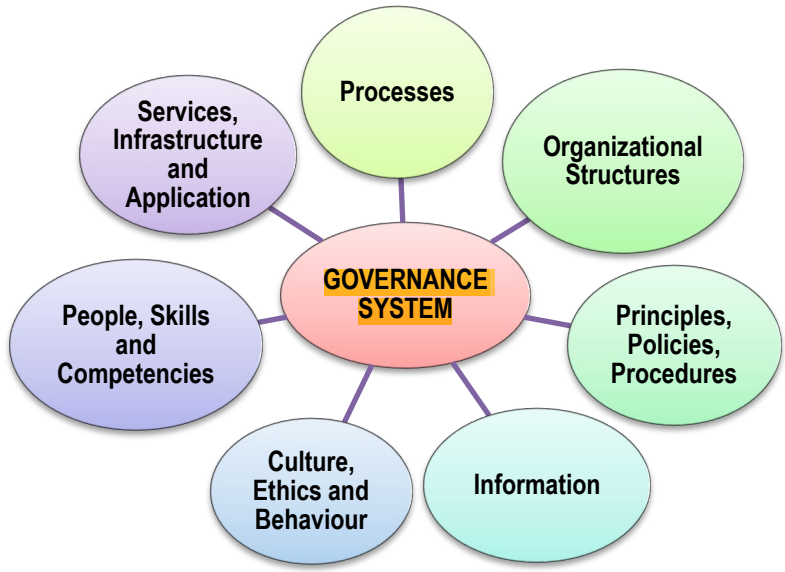


Fig. 1.7: COBIT Components of a Governance System

To satisfy governance and management objectives, each enterprise needs to establish, customise and sustain a governance system built from a number of components.

- Components are factors that, individually and collectively, contribute to the good operations of the enterprise's governance system over Information & Technology.

- Components interact with each other, resulting in a holistic governance system for Information & Technology.
- Components can be of different types. The most familiar are processes. However, components of a governance system also include organizational structures; policies and procedures; information items; culture and behavior; skills and competencies; and services, infrastructure, and applications.
  - **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.
  - **Organizational structures** are the key decision-making entities in an enterprise.
  - **Principles, Policies and Frameworks** translate desired behavior into practical guidance for day-to-day management.
  - **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. COBIT focuses on information required for the effective functioning of the governance system of the enterprise.
  - **Culture, Ethics and Behavior** of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
  - **People, Skills, and Competencies** are required for good decisions, execution of corrective action and successful completion of all activities.
  - **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with the governance system for I&T processing.

COBIT Implementation Approach

Phase 1—What Are the Drivers?

Phase 1 of the implementation approach identifies current change drivers and creates at executive management levels a desire to change that is then expressed in an outline of a business case. A change driver is an internal or external event, condition or key issue that serves as a stimulus for change. Events, trends (industry, market or technical), performance shortfalls, software implementations and even the goals of the enterprise can all act as change drivers. Risk associated with implementation of the program itself is described in the business case and managed throughout the life cycle. Preparing, maintaining, and monitoring a business case are fundamental and important disciplines for justifying, supporting and then ensuring successful outcomes for any initiative,

including improvement of the governance system. They ensure a continuous focus on the benefits of the program and their realization.

Phase 2—Where Are We Now?

Phase 2 aligns I&T-related objectives with enterprise strategies and risk, and prioritizes the most important enterprise goals, alignment goals and processes. Based on the selected enterprise and IT-related goals and other design factors, the enterprise must identify critical governance and management objectives and underlying processes that are of sufficient capability to ensure successful outcomes. Management needs to know its current capability and where deficiencies may exist. This can be achieved by a process capability assessment of the current status of the selected processes.

Phase 3—Where Do We Want to Be?

Phase 3 sets a target for improvement followed by a gap analysis to identify potential solutions. Some solutions will be quick wins and others more challenging, long-term tasks. Priority should be given to projects that are easier to achieve and likely to give the greatest benefit. Longer-term tasks should be broken down into manageable pieces.

Phase 4—What Needs to Be Done?

Phase 4 describes how to plan feasible and practical solutions by defining projects supported by justifiable business cases and a change plan for implementation. A well-developed business case can help ensure that the project's benefits are identified and continually monitored.

Phase 5—How Do We Get There?

Phase 5 provides for implementing the proposed solutions via day-to-day practices and establishing measures and monitoring systems to ensure that business alignment is achieved, and performance can be measured. Success requires engagement, awareness, communication, understanding and commitment of top management, and ownership by the affected business and IT process owners.

Phase 6—Did We Get There?

Phase 6 focuses on sustainable transition of the improved governance and management practices into normal business operations. It further focuses on monitoring achievement of the improvements using the performance metrics and expected benefits.

Phase 7—How Do We Keep the Momentum Going?

Phase 7 reviews the overall success of the initiative, identifies further governance or management requirements and reinforces the need for continual improvement. It also prioritizes further opportunities to improve the governance system.

Program and project management is based on good practices and provides for checkpoints at each of the seven phases to ensure that the program's performance is on track, the business case and risk are updated, and planning for the next phase is adjusted as appropriate. It is assumed that the enterprise's standard approach would be followed.

Further guidance on program and project management can also be found in COBIT management objectives BAI01 Managed programs and BAI11 Managed projects. Although reporting is not mentioned explicitly in any of the phases, it is a continual thread through all the phases and iterations.

1.6.2 Information Technology Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is a globally recognized framework for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. ITIL 4 is the latest version of the ITIL framework and was released back in February 2019. It is highly value-centric, primarily focusing on bringing different stakeholders in an organization together to co-create value for the end-users. It enables businesses to collaborate with the IT team to deliver IT services to stakeholders.

Some of the benefits ITIL practices allow businesses to gain include lower costs, high-quality IT services, increased business productivity, improved Return on Investment (RoI), greater customer satisfaction and improved resource utilization.

ITIL Dimensions

ITIL 4 is all about a holistic approach to service management. Because of this, the framework defines four dimensions that are critical to creating value for stakeholders, including customers. These four ITIL 4 dimensions are as follows:

- **Organizations and people** – The corporate culture needs to support an organization's objectives, and the right level of staff capacity and competency.
- **Information and technology** – Within the ITIL 4 service value system, this refers to the information, knowledge, and technologies that are needed for the management of services.
- **Partners and suppliers** – The suppliers that are involved in the design, deployment, delivery, support, and continual improvement of services and their relationship to the organization.
- **Value streams and processes** – These are the different parts of the organization working in an integrated and coordinated way? This is important to ITIL for the creation of value through products and services.

An appropriate amount of focus needs to go into each of these dimensions such that the ITIL 4 service value system remains balanced and effective.

ITIL Management Practices

ITIL 4 includes 34 management practices as "**sets of organizational resources designed for performing work or accomplishing an objective**". For each practice, ITIL 4 provides various types of guidance, such as key terms and concepts, success factors, key activities, information objects, etc. These 34 ITIL 4 practices are grouped into three categories as shown in the Fig. 1.8:

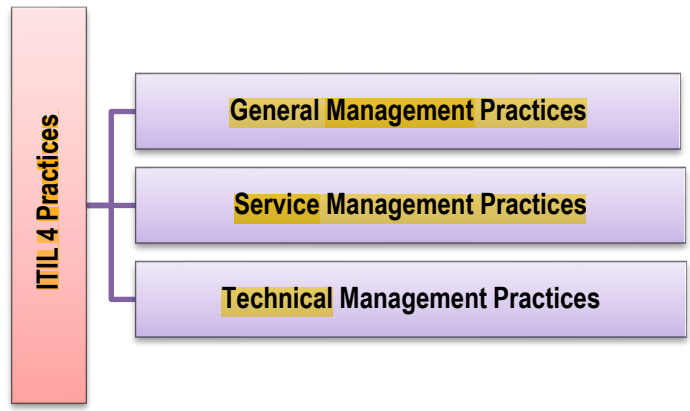


Fig. 1.8: ITIL 4 Practices

The ITIL 4 General Management Practices

1. Architecture management

This practice helps organizations manage the often-complex way in which their organizational architecture relates to various parts of the business. It provides the principles, standards, and tools to help manage changes in a structured and agile way.

2. Continual improvement

Organizations must be able to align their processes and services with changing business needs. The continual improvement practice helps them achieve this. It ensures that organizations identify opportunities for improvement within services, service components, practices, or other parts of service management.

3. Information security management

This practice relates to the way an organization protects its sensitive information from misuse. Specifically, information security management looks at ways to prevent breaches of the confidentiality, integrity, and availability of data. In this context, confidentiality refers to information

being viewed only by authorized parties, integrity to information being accurate, and availability to information being accessible when necessary.

4. Knowledge management

This practice helps organizations improve the way that they use data. It focuses on the convenience, effectiveness and efficiency of knowledge and data use.

5. Measurement and reporting

To make good decisions and continually improve systems, organizations must conduct evidence-based research. This practice provides a framework for doing that, recommending risk assessments and the collection of relevant data.

6. Organizational change management

This practice helps organizations implement the changes recommended during the continual improvement process. It emphasizes the human aspect of change management and the lasting benefits that can be had if the challenges and opportunities of individuals are accounted for.

7. Portfolio management

This practice ensures that the organization has the right combination of programs, products, and services to achieve its goals. It also accounts for the organization's funding and resource constraints.

8. Project management

This practice helps organizations oversee their ongoing projects and ensure that they are delivered successfully. It addresses the way projects are planned, delegated, monitored, and maintained. It also addresses the relationships between stakeholders and aims to keep those involved in the project motivated.

9. Relationship management

For projects to be successful, organizations must establish and nurture the relationships between stakeholders. This practice helps organizations identify, analyze, monitor and continually improve relationships.

10. Risk management

This practice helps organizations understand and address risks. There are countless ways that problems could materialize, and it's essential that they are spotted as soon as possible to prevent disruption, financial consequences, and sustainability issues.

11. Service financial management

This practice supports the organization's strategies and plans by ensuring that financial resources and investments are used efficiently.

12. Strategy management

This practice helps organizations define specific goals and ways to achieve them. It also ensures that necessary resources are allocated to meet those goals and clarifies the organization's priorities.

13. Supplier management

Organizations must manage their suppliers effectively if they are to ensure the smooth production and delivery of products and services. This practice helps foster those relationships, focusing on creating opportunities for collaboration and identifying ways to make improvements.

14. Workforce talent management

This practice helps organizations put talented and skilled people in the right roles. It focuses on the planning, recruiting, onboarding, and training of employees. It also looks at the way organizations evaluate the performance of employees and how to develop succession planning.

The ITIL 4 Service Management Practices

15. Availability management

With this practice, organizations can ensure that the availability of products and services meets the customer's needs. Those needs should have been agreed upon at the outset of the project.

16. Business analysis

This practice helps organizations analyze their business processes or elements within them. It's intended to help solve specific issues and improve value creation for stakeholders.

17. Capacity and performance management

This practice helps organizations ensure that their products and services meet expected performance levels. It also addresses current and future demands, helping organizations identify any changes that could affect their capacity.

18. Change enablement

This practice ensures that organizations maximize successful IT changes. It does so by ensuring that risk assessments are conducted, that proper authorizations are in place for implementing change and that changes are managed efficiently.

19. Incident management

The objective of this practice is to mitigate the negative impact of disruptive incidents. It helps organizations identify ways of restoring normal service operation as quickly as possible.

20. IT asset management

This practice helps organizations manage the complete lifecycle of their IT assets. It's based on value maximization, cost control, risk management, decision making, asset reuse management and retirement. It also addresses the regulatory and contractual requirements related to IT assets.

21. Monitoring and event management

With this practice, organizations can systematically observe services and service components, and record and report selected changes. They can do this by identifying and prioritizing infrastructure, services, business processes and information security events. The practice also establishes the responses to these events.

22. Problem management

This practice helps organizations mitigate the impact and likelihood of disruptive events. It does so by focusing on the identification of potential causes of incidents and the ways to navigate them.

23. Release management

This practice focuses on the way services are deployed. It addresses both new and changed services and features.

24. Service catalogue management

This practice ensures that organizations have a single source of consistent information for all their services. It guarantees that information is available for relevant audiences whenever it is required.

25. Service configuration management

This practice ensures that information about the configuration of an organization's services remains available and accurate. It also addresses the configuration items that support those services.

26. Service continuity management

This practice provides a framework for building organizational resilience. It helps organizations protect services in the event of a disruptive incident and ensure that their availability and performance remain at a sufficient level.

27. Service design

This practice helps organizations design products and services that are fit for use and in line with their defined purpose. It also ensures that services can be successfully delivered by the organization in its current ecosystem. The practice focuses on product and service planning, as well as the management of people, partners, suppliers, information, communication networks and technology.

28. Service desk

This practice helps organizations capture demand for incident resolution and service requests. It should also be the contact point for the service provider and its users.

29. Service level management

This practice sets business targets for the performance of services. It ensures that service delivery can be properly assessed, enabling the organization to identify issues and improve its practices.

30. Service request management

With this practice, organizations can support the agreed quality of service by handling all pre-defined, user-initiated service requests in an effective and user-friendly manner.

31. Service validation and testing

This practice ensures that new or changes products and services meet their defined requirements. Organizations should do this by measuring service value based on input from customers, business objectives and regulatory requirements.

The ITIL 4 Technical Management Practices

32. Deployment management

Deployment management practices help organizations move new or changed hardware, software, documentation, and processes from a production to a live environment. It also helps them move those components to other environments for testing or staging.

33. Infrastructure and platform management

This practice helps organizations oversee their infrastructure and platforms, enabling them to monitor technologies that are deployed internally and by service providers.

34. Software development and management

This practice ensures that applications meet the needs of stakeholders. It addresses software functionality, reliability, maintenance, compliance, and their ability to be audited.

Table 1.1: COBIT vs. ITIL	
COBIT	**ITIL**
COBIT is more on strategy focusing governance.	ITIL is mostly and operational focusing on actual working.
Broadly focuses on risk management that can be applied to various business areas.	Keeps a narrow focus on ITSM (IT service management.
COBIT audits are conducted by ISACA Certified Information Systems Auditors (CISAs).	Needs a third-party tool like to document compliance.

1.6.3 ISO 27001

ISO/IEC 27001 is an independent, non-governmental international organization to manage information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005, revised in 2013, and again most recently in 2022. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

Information Security Management System: ISO 27001 defines an information security management system (ISMS) as "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources." An ISMS, in other words, exists to preserve confidentiality, integrity, and availability.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining, and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

Why is ISO/IEC 27001 important?

With cyber-crime on the rise and new threats constantly emerging, it can seem difficult or even impossible to manage cyber-risks. ISO/IEC 27001 helps organizations become risk-aware and proactively identify and address weaknesses.

ISO/IEC 27001 promotes a holistic approach to information security in terms of vetting people, policies, and technology. An Information Security Management System (ISMS) implemented

according to this standard is a tool for **risk management, cyber-resilience, and operational excellence.**

Nowadays, data theft, cybercrime and liability for privacy leaks are risks that all organizations need to factor in. Any business needs to think strategically about its information security needs, and how they relate to its own objectives, processes, size, and structure. The ISO/IEC 27001 standard enables organizations to establish an information security management system and apply a risk management process that is adapted to their size and needs, and scale it as necessary as these factors evolve.

Companies that adopt the holistic approach described in ISO/IEC 27001 will make sure information security is built into organizational processes, information systems and management controls. Benefits of this standard have convinced companies across all economic sectors, all kinds of services and manufacturing as well as the primary sector; private, public, and non-profit organizations. They gain efficiency and often emerge as leaders within their industries.

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.
- 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.

How does ISO 27001 work?

ISO 27001 works in a top-down, technology-neutral, risk-based approach. The specification defines six planning processes which include the following as referred in Fig. 1.9.

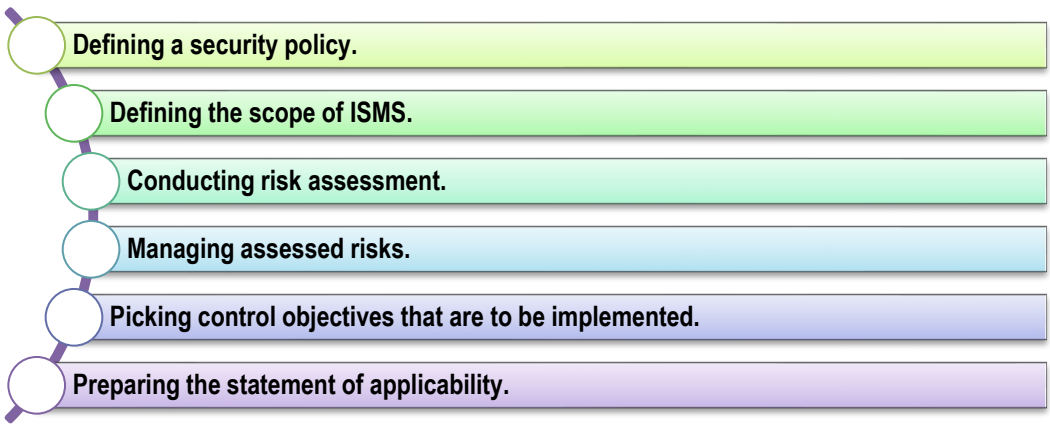


Fig. 1.9: Working of ISO 27001

ISO 27001 draws coordination between all sections of an organization and enhances management responsibility, ensures continual improvement, conducts internal audits, and undertakes corrective and preventive actions.

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:

- Suitable for protecting critical and sensitive information.
- 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.
- Once certified, globally accepted.

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 to ensure that both conformance and performance objectives are covered. The key concepts of governance, enterprise governance, corporate governance, IT governance and Governance of Enterprise IT have been explained. This will enable us 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.

IT compliance as part of Governance, Risk and Compliance under the umbrella of corporate governance is also discussed. The chapter has also provided a brief overview of COBIT 5 and highlighted the need for using globally accepted framework 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 in 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.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Which of the following domains of COBIT 5 covers areas such as operational delivery and support of IT services, including security within the IT system?

   (a) Align, Plan and Organize

   (b) Build, Acquire and Implement

   (c) Deliver, Service and Support

   (d) Monitor, Evaluate and Assess

2. Which of the following domains of COBIT 5 addresses the overall organization, strategy and supporting IT related activities within the IT system?

   (a) Align, Plan and Organize

   (b) Build, Acquire and Implement

   (c) Deliver, Service and Support

   (d) Monitor, Evaluate and Assess

3. A governance system typically refers to all the means and mechanisms that will enable _____ in an enterprise to have an organized mechanism to satisfy specific enterprise objectives.

   (a) Multiple stakeholders

   (b) Several processes

   (c) Intrinsic goals

   (d) Numerous products

4. Which of the following IT processes contained in the Deliver, Service and Support domain of COBIT manages the operations?

   (a) DSS02

   (b) DSS03

   (c) DSS94

   (d) DSS01

5. COBIT is a framework for the _____and _____ of information and technology aimed at the whole enterprise.

   (a) governance, management

   (b) support, services

   (c) monitoring, management

   (d) governance, support

ANSWERS/SOLUTIONS

1.	(c)	2.	(a)	3.	(a)	4.	(d)	5.	(a)

CHAPTER 2

GOVERNANCE, RISK, AND COMPLIANCE (GRC) FRAMEWORK

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- understand the concept of Governance, Risk, and Compliance (GRC).
- comprehend the concepts of risk, its related terms, and risk classification systems.
- distinguish between different types of risks and their mitigation strategies.
- identify different types of malicious attacks, malicious software and the counter measures to prevent or reduce possible threats.

CHAPTER OVERVIEW

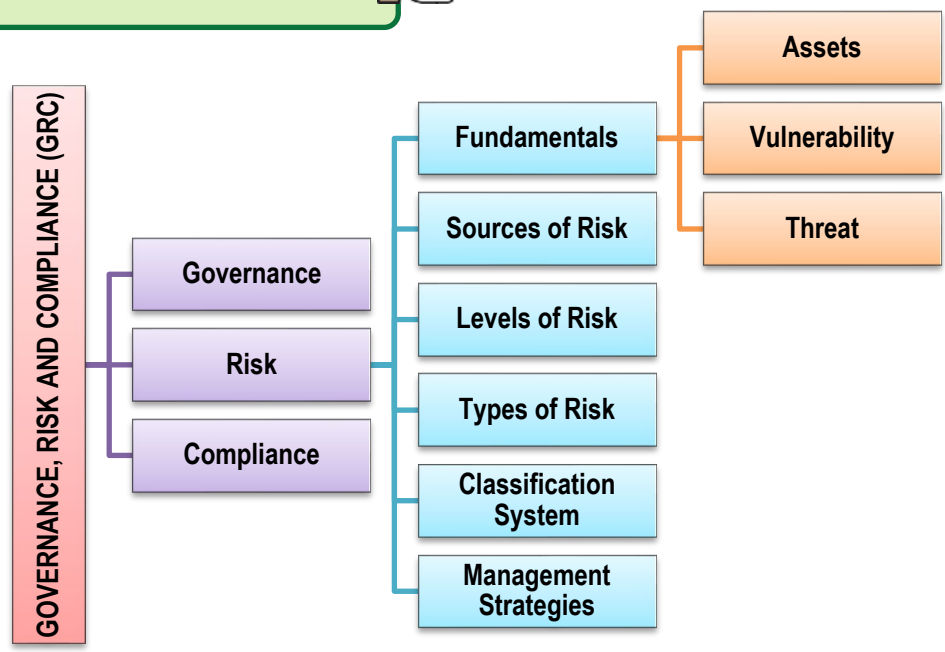


Illustration: ABC Bank of India

The ABC Bank of India is governed by Board of Directors headed by its Governor and assisted by three deputy governors in Administration, Economic and Financial policies, and Financial stability.

The Challenges Bank Faced

- **Risk Management:** The bank followed a manual, siloed, document, email, and spreadsheet-based risk management program with no real-time risk intelligence. Most risk and control assessments were performed in silos where users would leverage different risk scoring methodologies and calculations thereby leading to inconsistencies in risk data which, in turn, made it difficult to analyze risks at the enterprise level.
- **Internal audit:** The bank followed varying and non-standard auditing practices. The biggest challenge was consolidating vast amounts of data from multiple audit programs across the organization without a single system for monitoring and controlling audit activities at the corporate level.
- **Compliance management:** The bank was managing their compliance initiatives manually with the compliance data scattered across multiple spreadsheets. They were

finding it increasingly difficult to keep track of compliance across their operations and it was taking considerable time and effort to aggregate and sort the data into meaningful compliance reports.

- **Policy and document management:** The bank had multiple internal business groups across the enterprise developing documents in different templates at different places. Lack of standardization often resulted in duplication of effort, costs, and content. Different policies were stored in different repositories, and it was challenging for stakeholders to quickly search for and locate the policy they needed when they needed it.

To stay relevant in a highly dynamic banking environment, the bank decided to adopt a federated approach to manage their GRC operations to automate manual GRC activities across the bank in a more efficient, streamlined, and integrated manner and to ensure that the bank would adopt a paperless approach to execute all its GRC activities.

After evaluating several GRC solutions, they decided to go with XYZ enterprise GRC platform to build a strong risk culture and enhance their brand and reputation. The XYZ solution provided the following benefits to the bank:

- **Enterprise Risk Management** managed, monitored, and assessed enterprise and operational risks of the bank. It enabled the bank to deliver dynamic reports, charts, and heat maps for senior management, enabling better decision-making.
- **Compliance Management** provided a comprehensive system to manage a range of regulatory and corporate compliance requirements for the bank. The XYZ solution integrated and mapped compliance mandates and controls in a central framework, thereby simplifying compliance management and monitoring. The bank could now streamline and standardize compliance and control processes, minimizing deviations and redundancies. Graphical dashboards provided in-depth visibility across the compliance program, enabling the bank to proactively identify and address areas of concern.
- **Internal Audit Management** managed the complete audit process from audit planning through audit execution and reporting. It enabled the bank to initiate and follow-up with audit related issues till closure through the issue management functionality.
- **Policy and Document Management** enabled the bank to manage all documents (across various departments of the bank) such as contracts, notices, policies, and procedures throughout their lifecycle from creation, to publishing, to retirement, and finally archiving. The solution reduced the usage of the paper-based processes at the bank and adds value in terms of deployment of physical resources, time savings, and process improvements in terms of automated ownership and change management of documents.

2.1 INTRODUCTION

GRC (Governance, Risk, and Compliance) is an organizational strategy for managing governance, risk management, and compliance with industry and government regulations. GRC also refers to an integrated suite of software capabilities for implementing and managing an enterprise GRC program. GRC's set of practices and processes provides a structured approach to aligning IT with business objectives. GRC helps companies effectively manage IT and security risks, reduce costs, and meet compliance requirements. It also helps improve decision-making and performance through an integrated view of how well an organization manages its risks.

Fig. 2.1: GRC Overview

The GRC overview and processes are depicted in Fig. 2.1 and Fig. 2.2 respectively.

GRC tools are software applications that businesses can use to manage policies, assess risk, control user access, and streamline compliance. GRC tools are a way to manage operations and ensure a company is meeting compliance and risk standards. Tools can also help determine and mitigate risks associated with use, ownership, operation, involvement, influence, and adoption of IT within a company.

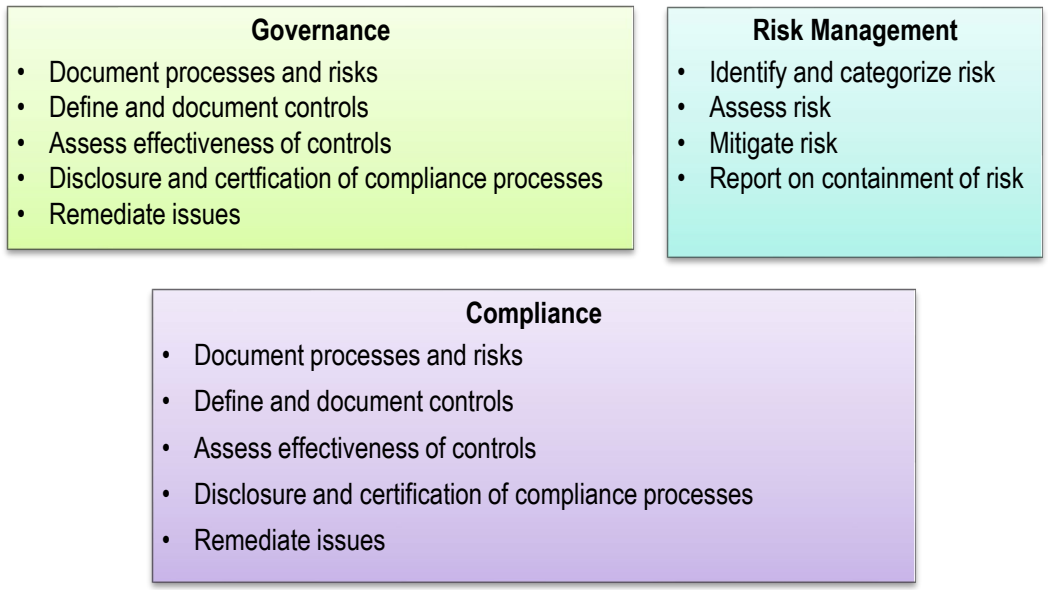


Fig. 2.2: GRC Processes

GRC tools should encompass operational risk, policy and compliance, IT governance, and internal auditing. Most GRC tools have some of the following features:

- Content and document management that helps businesses create, track, and store digitized content.
- Risk data management and analytics that help to measure, quantify, and predict risk—and determine steps to reduce it.
- Workflow management to help companies establish, execute, and monitor GRC-related workflows.
- Audit management to organize information and simplify processes for conducting internal audits.
- A dashboard that provides a central interface where key performance indicators relevant to business processes and objectives can be monitored in real-time.

Effective GRC tools create and distribute policies and controls and map them to regulations and compliance requirements. They help assess, whether controls have been deployed, are functioning correctly, and are improving risk assessment and mitigation.

2.2 RISK FUNDAMENTALS

Some risk related terms are described below. The relationship and different activities among these terms may be understood by Fig. 2.3.

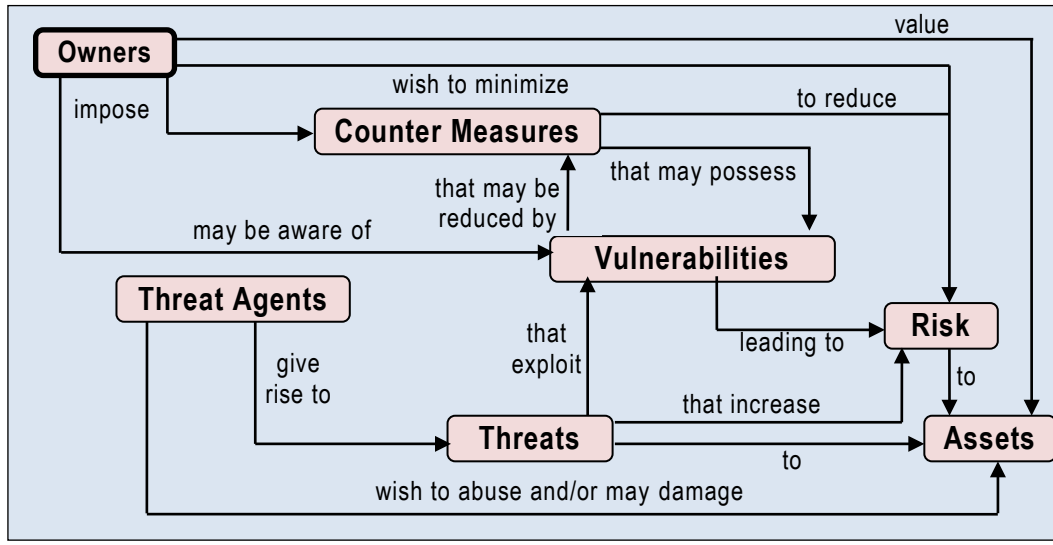


Fig. 2.3: Risk Related Terms

2.2.1 Asset

Asset can be defined as something of value to the organization, for example - 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 of all.
- 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.

Although all items in an organization have some value, the term asset generally applies to those items that have substantial value. An organization's assets can include the following:

- **Customer data:** Name, address, phone, Aadhaar Number, date of birth, cardholder data, and protected health care information.
- **IT assets and network infrastructure:** Hardware, software, and services.

- **Intellectual property:** Sensitive data such as patents, source code, formulas, or engineering plans.
- **Finances and financial data:** Bank accounts, credit card data, and financial transaction data.
- **Service availability and productivity:** The ability of computing services and software to support productivity for humans and machinery.
- **Reputation:** Corporate compliance and brand image.

It is the responsibility of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets. To secure information, we must protect its **Confidentiality, Integrity, and Availability (CIA)** as discussed in Table 2.1.

Table 2.1: Tenets of Secure Information

• **Confidentiality** refers to the prevention of the unauthorized disclosure of information, i.e. only authorized users can view information. Confidentiality is a common term which means guarding information from everyone except those with rights to it. information includes private data of individuals, intellectual property of businesses and national security for countries and governments.
• **Integrity** deals with the validity and accuracy of the data. This means prevention of the unauthorized modification of information i.e. only authorized users can change the information. Data lacking integrity, i.e. data that is not accurate is not valid, are of no use. For some organizations, data and information are intellectual property assets. Examples include copyrights, patents, secret formulas, and customer databases.
• **Availability** in terms of information security is generally expressed as the amount of time users can use a system, application, and data. In refers to the prevention of the unauthorized withholding of information i.e. information is accessible by authorized users whenever they request the information.

2.2.2 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 (for example- 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.

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, analysis, and penetration testing.

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.

Simply, Vulnerability can be referred to as the weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from flaws in 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:

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

2.2.3 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**. It has the capability to attack a system with intent to harm. It is often used to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has 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.

Threat Types: Majorly there are three threat types that directly threaten each of the CIA tenets, which are as follows:

exm

- **Disclosure Threats:** Disclosure occurs any time unauthorized users access private or confidential information that is stored on a network resource or while it is in transit between

network resources. Disclosure can also occur when a computer or device containing private or confidential data such as database related to medical, banking or tax records is lost or stolen. Two techniques that attackers employ to illegally obtain or modify data are as follows:

- **Sabotage:** It is the deliberate destruction of property or obstruction of normal operations i.e. attack on the availability of information security. A data breach is the release of confidential, private, or otherwise sensitive information into an unsecured environment. A data breach can occur accidentally, or as the result of a deliberate attack. A data breach can easily result in identity theft when sensitive information is exposed to unauthorised individuals. Hackers can use this information to steal a person's identity and commit fraudulent activities, such as opening new accounts or making unauthorised purchases. A privacy breach occurs when someone accesses information without permission.
- **Espionage:** It is the act of spying to obtain secret information typically to aid another nation state. Terrorists and enemy might well be involved in activities to obtain sensitive government information that they can use to perpetuate future attacks.

- **Alteration Threats:** This type of attack compromises a system by making unauthorized changes to data on a system, either intentionally or unintentionally; thereby violating information integrity. This change might occur while the data is stored on a network resource or while they are moving between two resources. Data corruption is when errors in computer data occur and introduce unintended changes to the original data, changing its form and making it unreadable. Intentional changes are usually malicious while unintentional changes are usually accidental. For example - a user might modify database files, operating systems, application software, and even hardware devices. Modifications might include creating, changing, deleting, and writing information to a network resource. It's a good idea to put techniques in place that enable you to track or audit these changes as they happen. That way, you can have a record of who, what, when, where, and how modifications were made. In addition, change management systems limit who can make changes, how they make changes, and how they document changes. It is very important that only authorized parties change assets, and only in authorized ways.
- **Denial of Service/Destruction Threats:** In these threats, a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the devices 'normal functioning thereby making the assets or resources unavailable or unusable. These typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. Any threat

that destroys information or makes it unavailable violates the availability tenet of information security. A denial or destruction attack is successful when it prevents an authorized user from accessing a resource either temporarily or permanently. A DoS attack is an example of a denial or destruction threat. A DoS attack, which is usually malicious, prevents authorized users from accessing computer and network resources. Many organizations are potential victims of DoS attacks. In fact, any computer connected to the Internet is a DoS threat candidate. This type of attack can represent a minor problem or a great danger, depending on the importance of the blocked asset or resource. For example, suppose an attacker floods a specific port on a server. If the port is not for a critical resource, the impact may be minimal. However, if the port supports authorized user access to your company's website, it could prevent customers from accessing it for minutes or hours. In that case, the impact could be severe.

2.3 RISK

Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset.

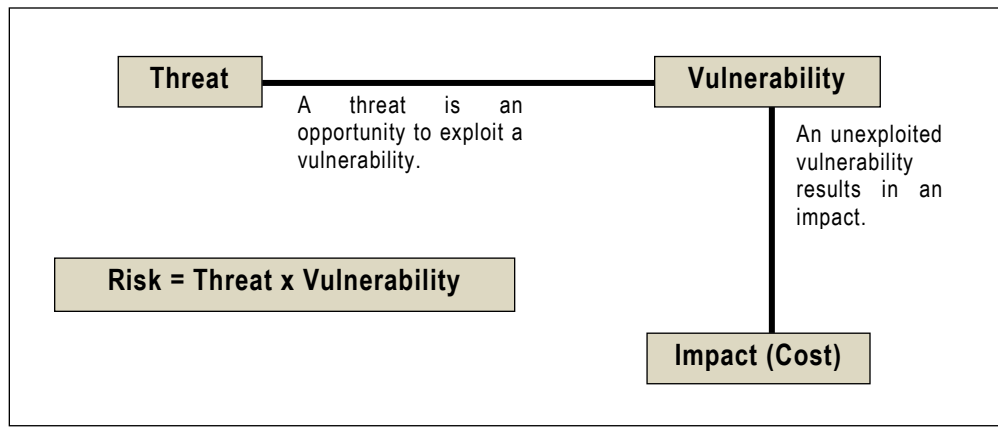


Fig. 2.4: Risks, Threats, and Vulnerabilities

Risks, threats, and vulnerabilities go together as depicted in Fig. 2.4. Risk is the probability that something bad can happen. A threat is any action that can damage or compromise an asset. A vulnerability is a weakness in the design or software code itself. A vulnerability that can be exploited is a threat.

If a vulnerability exists in a system, there is always a possibility of threat. Any threat against a vulnerability creates a risk that a negative event may occur. You can't eliminate threats, but you can protect against vulnerabilities. That way, even though a threat still exists, it cannot exploit the

vulnerability. The key to protecting assets from the risk of attack is to eliminate or address as many vulnerabilities as possible.

For example- Consider the case of the real-world example of a hurricane. The **threat** of a hurricane is outside one's control. However, knowing that a hurricane could strike can help business owners assess weakness and develop an action plan to minimize the impact. In this scenario, a **vulnerability** would be not having a data recovery plan in place in the event that your physical assets are damaged as a result of the hurricane. The **risk** to your business would be the loss of information or a disruption in business as a result of not addressing your vulnerabilities.

Accurately understanding the definitions of these security components will help you to be more effective in designing a framework to identify potential threats, uncover and address your vulnerabilities to mitigate risk.

Information systems can generate many direct and indirect risks that lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by following factors:

- 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.
- 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.
- 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.

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. 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 off-site. ATM is 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.

Any risk remaining still 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. If 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. The 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 strength of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

2.3.1 Sources of Risk

The most important step in the 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 strategies can be adopted. Some of the common sources of risk are 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:

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

2.3.2 Levels of Risk

Refer Table 2.2 to understand the level of risks that have been identified if no controls are in place.

Table 2.2: Levels of Risk

Level of Risk	Description
Inherent	The level of risk before any actions have been taken to change the likelihood or magnitude of the risk.
Current/Residual	The level of risk after initial control measures have been put in place.
Target	The level of risk that is desired or will be obtained with the application of further control measures.

2.3.3 Types of Risks

The types of risks that impact companies vary depending on the home country location, industry, level of globalization, and many other factors. Risk is now defined as the "effect of uncertainty on objectives", which focuses on the effect of incomplete knowledge of events or circumstances. Every risk has its own characteristics that require management or analysis. The risks can be broadly categorized as follows:

- **Compliance (Or Mandatory Risk):** This includes risks that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations. They are associated with adherence to the law of the country and the regulations that apply to the sector in which the company operates. Compliance risk captures the legal and financial penalties for failing to act or acting inappropriately and is especially significant for those business sectors that are heavily regulated.
    - Compliance mandatory requirements represents a 'license to operate' and failure to achieve the level of compliance required by the relevant regulator will impact routine business activities.
    - Penalties may be financial but increasingly they are personal to the management involved. Examples include violation of laws or regulations governing areas such as environmental, employee health and safety, lack of due diligence, protection of personal data in accordance with global data protection requirements and local tax or statutory laws. New and emerging regulations can have a wide-ranging impact on management's strategic direction, business model and compliance system. It is, therefore, important to consider regulatory requirements while evaluating business risks. Examples include violation of laws or regulations governing areas such as environmental, employee health and safety, lack of due diligence, protection of

personal data in accordance with global data protection requirements and local tax or statutory laws. New and emerging regulations can have a wide-ranging impact on management's strategic direction, business model and compliance system. It is, therefore, important to consider regulatory requirements while evaluating business risks.

- **Hazard (Or Pure) Risks:** These are associated with a source of potential harm or a situation with the potential to undermine objectives in a negative way. Hazard risks are the most common risks associated with operational risk management including occupational health and safety programmes, natural disasters; various insurable liabilities; impairment of physical assets; terrorism, theft, etc.
- **Control (Or uncertainty) Risks:** These are associated with unknown and unexpected events and can be extremely difficult to quantify. Control risks are frequently associated with new projects where it is known that events will occur, but the precise consequences of those events are difficult to predict and control. Therefore, the approach is based on managing the uncertainties around the timing, eventual cost, or delivery of the project.
- **Opportunity (Or Speculative) Risks:** These fall into two categories – the risks associated with taking the opportunity, and the risks of not acting. Although opportunity risks are taken with the intention of obtaining a positive outcome, this is not guaranteed. In the rapidly changing environment caused by the global pandemic, organizations have deliberately taken risks in order to survive.

illustration: Start-up in the financial sector of India

- The company will need to be authorized by the relevant authorities and the company will need to nominate senior managers to be responsible for its **compliance risks**.
- Theft or fraud caused by an employee is an **operational or hazard risk**.
- When they design their new software package, **control risks** will be associated with this project.
- When released, the software may have the potential to be used by clints in a sector they had not specifically targeted, thereby creating an **opportunity risk;** the intention is to achieve results by attracting customers, but it is possible that the project will fail to deliver the functionality that was intended. In fact, the failure of the functionality of the new software may critically undermine the operations of the organization.

There are several classification systems available that sort the risks according to the timescale of their impact or according to the nature of the risk, the source of the risk and/or the nature of the impact or size and nature of the consequences.

Advantages of Risk Classification System (Refer Fig. 2.5)

- Accumulations of risk that could undermine a key dependency or business objective and make it vulnerable can be more easily identified.
- Responsibility for improved management of each different type of risk can be more easily identified/allocated if risks are classified.
- Decisions and knowledge about the type of control(s) that will be implemented can be taken on a more structured and informed basis.
- Circumstances where the risk appetite of the organization is being executed (or the risk criteria not being implemented) can be more readily identified.
- Categorizing risks according to a single risk classification system may not be sufficient to reveal all risks. Therefore, a combination of systems can be used to provide a complete picture.

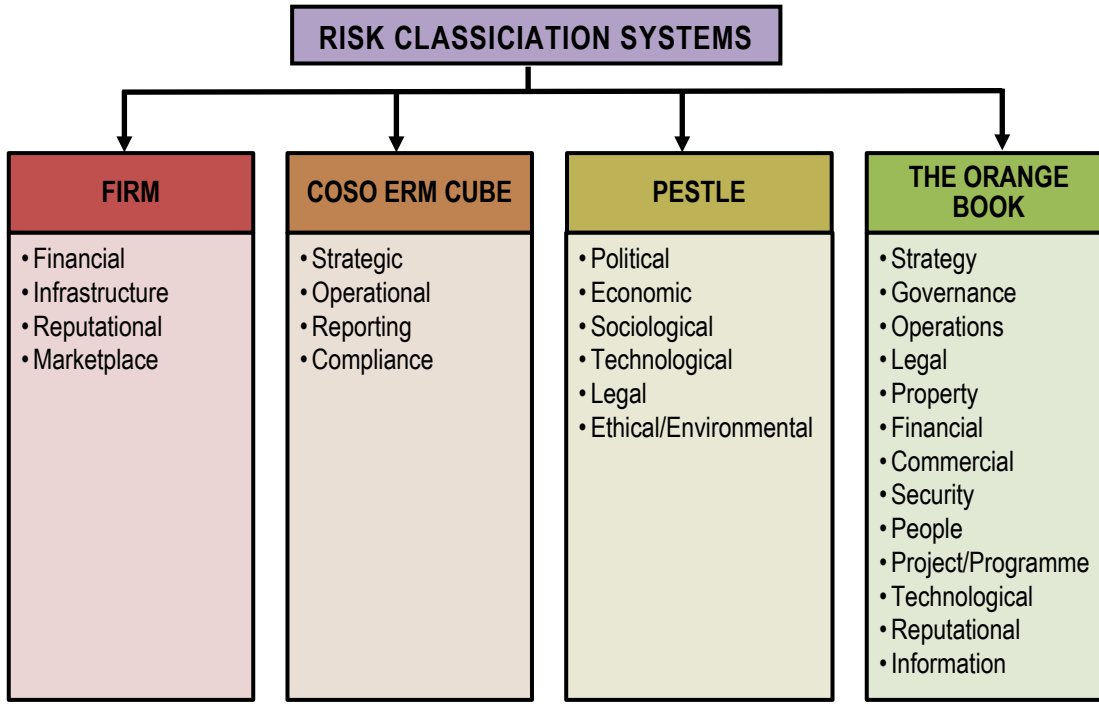


Fig. 2.5: Risk Classification Systems

These terminologies are defined below collectively: exm

- **Financial Risks:** Financial risks are those risks that could result in a negative financial impact to the organization (waste or loss of assets). Examples include risks from volatility in foreign currencies, interest rates, and commodities, credit risk, liquidity risk, and market risk.

- **Infrastructure Risks:** Risks that will impact the level of efficiency and cause dysfunction within the core processes that may include under-provisioning or over-provisioning, hardware incompatibility, software incompatibility, network issues and outages, migration issues, downtime, disaster recovery, vendor reliability, and unexpected costs.

exm- **Reputational Risks:** Reputational risk is the damage that can occur to a business when it fails to meet the expectations of its stakeholders and is thus negatively perceived. Risks arising from adverse events, including ethical violations, lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, may lead to damage to reputation and/or destruction of trust and relations. It can affect any business, regardless of size or industry and hugely impact the desire of customers to deal or trade, and the level of customer retention.

- **Marketplace Risks:** These are the risks that will impact on the level of customer trade or expenditure that may include changes in equity prices or commodity prices, interest rate movements or foreign exchange fluctuations.

- **Strategic Risks:** These are the risks that would prevent an organization from accomplishing its objectives (meeting its goals). Examples include risks related to strategy, political, economic relationship issues with suppliers and global market conditions; also, could include reputation risk, leadership risk, brand risk, and changing customer needs. It is to be remembered that the strategic risk are higher level risk and stem from macro-economic or political relationships. exm

- **Operational Risks:** Operational risks include those risks that could prevent an organization from operating in the most effective and efficient manner or be disruptive to other operations due to inefficiencies or breakdown in internal processes, people, and systems. Examples include risk of loss resulting from inadequate or failed internal processes, fraud or any criminal activity by an employee, business continuity, channel effectiveness, customer satisfaction and product/service failure, efficiency, capacity, and change integration.

exm

- **Reporting Risks:** These are the risks that are associated with lapses in identifying and reporting risks to the management that are tied to or have an immense potential to impact an organization's business processes.

- **Compliance Risks:** This includes risks that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations. Examples include violation of laws or regulations governing areas such as environmental, employee health and safety, lack of due diligence, protection of personal data in accordance with global data protection requirements and local tax or statutory laws. New and emerging regulations can have a wide-ranging impact on management's strategic direction, business model and compliance system. It is, therefore, important to consider regulatory requirements while evaluating business risks.

exm

- **Political Risks:** Political risks are the risk an investment's returns could suffer as a result of political changes or instability in a country. This includes tax policy, employment laws, environmental regulations, trade restrictions and reform, tariffs and political stability.

- **Economic Risks:** Economic risks are the risk involved in investing in a business opportunity in an international market that arises from changes in sovereign policies, market fluctuations, and counterparty credit risk.

- **Sociological Risks:** These risks can be defined as the exposure to adverse consequences stemming from population-based activities and negative public perception. For example - cultural norms and expectations, health consciousness, population growth rate, age distribution, career attitudes, emphasis in safety, global warming, etc.

- **Ethical or Environmental Risks:** These are the risks that have ethical and environmental aspects, although many of these factors will be economic or social in nature.

- **Governance Risks:** These risks arise from unclear plans, priorities, authorities, and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

- **Legal Risks:** Risks arising from a defective transaction, a claim being made or some other that results in liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets. For example - intellectual property.

- **Property Risks:** Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

- **Commercial Risks:** Risks arising from weaknesses on the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance,

inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.

- **People Risks:** Risks arising from ineffective leadership and engagement suboptimal culture, inappropriate behaviors, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
- **Technological Risks:** Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
- **Information Risks:** Risks arising from a failure to produce robust, suitable, and appropriate data/information and to exploit data/information to its full potential.
- **Security Risks:** Risks arising from a failure to prevent unauthorized and/or inappropriate access to the estate and information, including cybersecurity and noncompliance with general data protection requirements.
- **Project/Programme Risks:** Risks that change programs and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits in time, cost, and quality.

2.3.4 Risk Management/Mitigation Strategies

With the recent jump in regulatory mandates and changing market dynamics- both locally and globally, many organizations have started to identify and manage areas of risk in their business: whether it is financial, operational, IT, brand, or reputation related risk. These risks are no longer considered the sole responsibility of specialists – executives and the boards demand visibility into exposure and status so they can effectively implement the organization's long-term strategies. As a result, companies are looking to systemically identify, measure, prioritize, and respond to all types of risk in the business, and then manage any exposure accordingly. A risk management process provides a strategic orientation for companies of all sizes in all geographies with a formal process to identify, measure, and manage risk. Risk insights can help organizations take strategic advantage of any market conditions.

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. While determining the control for risk, it's to be remembered that the cost of control should not outweigh the risk otherwise, there is no point of control or mitigation of such risk.

Risk Management enables an organization to evaluate all risks at enterprise level and relevant controls and monitor mitigation actions in a structured manner. After defining risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Based on the type of risk, project, and its significance to the business, Board and Senior Management may choose to take up any of the following risk management strategies in isolation or combination as required.

Various Risk management strategies can be described as the 4T's which are explained below:

- **Transfer/Share the risk:** Risk mitigation approaches can be shared with trading partners and suppliers. Risk transference involves handing the risk off to a willing third party. Many companies outsource certain operations as part of risk management so that they can focus on their core competencies. This might be done by conventional insurance, or it might be done by paying a third-party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. Some of its examples are as follows:
  - **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.
  - **Purchasing insurance or other insurance types of services:** To transfer risk, an organization may agree to pay some other company for its services such as managing and securing its data or an insurance company that will pay for losses in the event of a business disruption.
- **Tolerate/Accept/Retain 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. This means that exposure may be tolerable without any further action being taken. Even if it is not tolerable, the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In this case, consciously accepting the risk as a cost of doing business is appropriate. The risks should be reviewed periodically to ensure that their impact remains low. A common example of risk acceptance is planning for potential production delays (within a reasonable time range) since it's often difficult to predict a precise delivery schedule in advance.
  - Small businesses often take the stance that they cannot afford to avoid, limit, or transfer risk and therefore, they accept risk by default. This is a mistaken and limited view and should not be the default position going into this planning. Risk acceptance should be evaluated along with the other options to determine the implications,

appropriate actions, and costs of various mitigation strategies. Risk acceptance is the least expensive option in the near-term and the most expensive option in the long-term should an event occur.

- For example - Mr. Babu owns a store and wants his store to get renovated. For the flooring purpose, he must purchase white marble worth ₹ 25 Lakhs including the transportation cost. He can get the same quality of the product from a nearby city but will cost him almost double amount of what he can get from a far-off place. He understands that there are chances that the marble sheets may get broken during the transit from far off place, still he decides not to purchase it from the nearby city. He accepts that transportation involves the risk of losing money, but it is acceptable as the cost of avoiding this risk would have been double.

- **Terminate/Eliminate/Avoid the risk:** Risk avoidance is the opposite of risk acceptance because it's an all-or-nothing kind of stance. Especially in the case of risks that have high probability and impact values, it may be best to modify any project strategy to avoid them altogether. In other words, these risks will only be treatable, or containable to acceptable levels by terminating the activity. For example – the risks associated with the use of a technology, supplier, or vendor can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

  - Risk avoidance is usually the most expensive of all risk mitigation strategies, but it has the result of reducing the cost of downtime and recovery significantly. In business continuity and disaster recovery plans, risk avoidance is the action that avoids any exposure to the risk whatsoever. If data loss is to be avoided, you have fully redundant data systems or you manually shut down systems and move them in advance of an oncoming hurricane.

  - Shutting down systems is costly in advance of a hurricane, but if they are packed and shipped to another location and fired up, the cost to recover from the business disruption is minimal. This option is not feasible for many types of risks or for many types of companies. However, it is a viable option to consider as you develop your risk mitigation strategies.

- **Treat/Mitigate/Control/Reduce the risk:** By far the large number of risks will be addressed in this way. The purpose of the treatment is that, whilst continuing within the organization with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level. Suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects. This risk limitation strategy falls between

acceptance and avoidance both in terms of early costs and costs after the business disruption.

- The strategy may include installing firewalls to keep networks safe, creating backups to keep data safe, practicing fire drills to keep employees safe, and more. The cost of that implementation is finite and known and usually ends at some point in time. Thus, while the near-term costs of risk control and risk transference may appear to be similar, it's important to understand the duration of the cost about these strategies.
- A good example of risk mitigation is planning for the eventuality in case an enterprise will not have sufficient capacity or supplies to deal with a very high demand. In that case, the enterprise shall have a mitigation strategy in place that allows them to rapidly scale their capacity, or to subcontract some of the work to other parties to meet the high demand. Another example can be performing daily backups of critical business. It doesn't stop a disk drive from crashing, it doesn't ignore the potential for disk failure, it accepts that drives fail and when they do, having backups helps you recover in a timely manner.

Fig. 2.6 suggests that in each of the four quadrants of the risk matrix, one of the 4T's will be dominant.

- **Transfer** will be the dominant response for the **high-impact/low-likelihood risks**.
- **Terminate** will be the dominant response for the **high-impact/high-likelihood risks**.
- **Tolerate** will be the dominant response for the **low-impact/low-likelihood risks**.
- **Treat** will be the dominant response for the **low-impact/high-likelihood risks**.

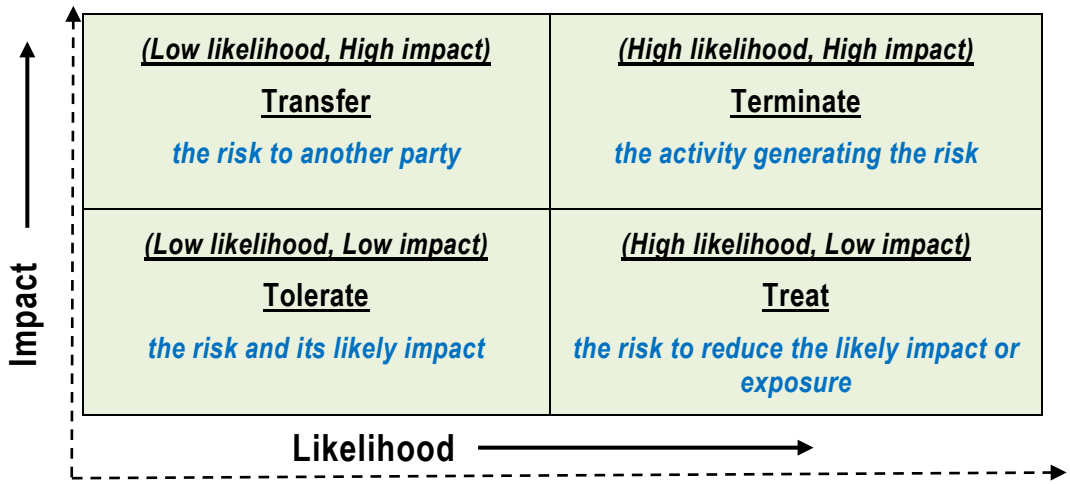


Fig. 2.6: Risk Matrix and 4T's of Risk Management Strategies

2.4 MALICIOUS ATTACKS

Security threats can be active or passive which can have negative repercussions for an IT infrastructure.

- An **active attack** is a physical intrusion that involves modification of the data stream or attempts to gain unauthorized access to computer and networking systems.
- In a **passive attack**, the attacker does not make changes to the system. This type of attack simply eavesdrops and monitors transmissions.

Active threats include the following as discussed in the Table 2.3:

Table 2.3: Active Threats

Brute-force Password Attacks In this attack, the attacker tries different passwords on a system until one of them is successful. Usually, the attacker employs a software program to try all possible combinations of a likely password, user ID, or security code until it locates a match. It is called as a **Brute-Force Attack** because the attacker simply hammers away at the code.
Dictionary Password Attacks A simple attack that relies on users making poor password choices. A simple password-cracker program takes all the words from a dictionary file and attempts to log on by entering each dictionary entry as a password. Users often engage in the poor practice of selecting common words as passwords. A password policy that enforces complex passwords is the best defense against a dictionary password attack. Users should create passwords composed of a combination of letters and numbers both in capital and small letters, and the passwords should not include any personal information about the user.
IP Address Spoofing It is a type of attack in which one person, program, or computer disguises itself as another person, program, or computer to gain access to some resource. A common spoofing attack involves presenting a false network address to pretend to be a different computer. An attacker may change a computer's network address to appear as an authorized computer in the target's network. If the administrator of the target's local router has not configured it to filter out external traffic with internal addresses, the attack may be successful. IP address spoofing can enable an attacker to access protected internal resources. **Address Resolution Protocol**

(ARP) poisoning is an example of a spoofing attack. In this attack, the attacker spoofs the MAC address of a targeted device, such as a server, by sending false ARP resolution responses with a different MAC address. This causes duplicate network traffic to be sent from the server. Another type of network-based attack is the Christmas (Xmas) attack. This type of attack sends advanced TCP packets with flags set to confuse IP routers and network border routers with TCP header bits set to 1, thus lighting up the IP router like a Christmas tree.

Masquerading

In a **masquerade attack**, one user or computer pretends to be another user or computer. Masquerade attacks usually include one of the other forms of active attacks, such as IP address spoofing or replaying. Attackers can capture authentication sequences and then replay them later to log on again to an application or operating system. For example, an attacker might monitor usernames and passwords sent to a weak web application. The attacker could then use the intercepted credentials to log on to the web application and impersonate the user.

Phishing

It is a type of fraud in which an attacker attempts to trick the victim into providing private information such as credit card numbers, passwords, dates of birth, bank account numbers, Automated Teller Machine (ATM) PINs, and Aadhar number or PAN numbers or other Social Security Number. A phishing scam is an attempt to commit identity theft via email or instant message. The message appears to come from a legitimate source, such as a trusted business or financial institution, and includes an urgent request for personal information. Phishing messages usually indicate a critical need to update an account (banking, credit card, etc.) immediately. The message instructs the victim to either provide the requested information or click on a link provided in the message. Clicking the link leads the victim to a spoofed website. This website looks identical to the official site but in fact belongs to the scammer. Personal information entered into this web page goes directly to the scammer, not to the legitimate organization.

- A variation of the phishing attack is **Spear phishing** that uses email or instant messages to target a specific organization, seeking unauthorized access to confidential data. As with the messages used in regular phishing attempts, spear-phishing messages appear to come from a trusted source.
- The best way to protect against phishing of any kind is to avoid clicking on a link directly provided by a suspect email.

Hijacking

It is a type of attack in which the attacker takes control of a session between two machines and masquerades as one of them. There are a few types of hijacking:

- **Browser or URL hijacking**—In a browser or **URL hijacking** attack, the user is directed to a different website than what he or she requested, usually to a fake page that the attacker has created. This gives the user the impression that the attacker has compromised the website when in fact the attacker simply diverted the user's browser from the actual site. This type of attack is also known as **Typo Squatting**. Attackers can use this attack with phishing to trick a user into providing private information such as a password.
- **Session hijacking**—In **Session hijacking**, the attacker attempts to take over an existing connection between two network computers. The first step in this attack is for the attacker to take control of a network device on the LAN, such as a firewall or another computer, in order to monitor the connection. This enables the attacker to determine the sequence numbers used by the sender and receiver. After determining the sequence numbering, the attacker generates traffic that appears to come from one of the communicating parties. This steals the session from one of the legitimate users. To get rid of the legitimate user who initiated the hijacked session, the attacker overloads one of the communicating devices with excess packets so that it drops out of the session.

Replay Attacks

These involve capturing data packets from a network and retransmitting them to produce an unauthorized effect. The receipt of duplicate, authenticated IP packets may disrupt service or have some other undesired consequence. Systems can be broken through replay attacks when attackers reuse old messages or parts of old messages to deceive system users. This helps intruders to gain information that allows unauthorized access into a system.

Man-in-the-Middle Attack

In this type of attack, an attacker intercepts messages between two parties before transferring them on to their intended destination. Web spoofing is a type of man-in-the-middle attack in which the user believes a secure session exists with a particular web server. In reality, the secure connection exists only with the attacker, not the web server. The attacker then establishes a secure connection with the web server, acting as an invisible go-between. The attacker passes traffic between the user and the web server. In this way, the attacker can trick the user into supplying passwords, credit card information,

and other private data. Attackers use man-in-the-middle attacks to steal information, to execute DoS attacks, to corrupt transmitted data, to gain access to an organization's internal computer and network resources, and to introduce new information into network sessions.

For example, if Neena and Smita want to communicate, the attacker pretends to be Neena when talking with Smita and pretends to be Smita when talking to Neena. Neither Neena nor Smita know they are talking to the attacker. The attacker can collect substantial information and can even alter data as they flow between Neena and Smita. This attack enables the attacker to either gain access to the messages or modify them before retransmitting. A man-in-the-middle attack can occur from an insider threat. An insider threat can occur from an employee, contractor, or trusted person within the organization.

Eavesdropping

Eavesdropping or sniffing, occurs when a host sets its network interface to promiscuous mode and copies packets that pass by for later analysis. Promiscuous mode enables a network device to intercept and read each network packet, even if the packet's address doesn't match the network device. It is possible to attach hardware and software to monitor and analyze all packets on that segment of the transmission media without alerting any other users. Candidates for eavesdropping include satellite, wireless, mobile, and other transmission methods.

Social Engineering

Attackers often use a deception technique called **Social Engineering** to gain access to resources in an IT infrastructure. In nearly all cases, social engineering involves tricking authorized users into carrying out actions for unauthorized users. The success of social engineering attacks depends on the basic tendency of people to want to be helpful.

Social engineering places the human element in the security breach loop and uses it as a weapon. A forged or stolen vendor or employee ID could provide entry to a secure location. The intruder could then obtain access to important assets. By appealing to employees' natural instinct to help a technician or contractor, an attacker can easily breach the perimeter of an organization and gain access.

Personnel who serve as initial contacts within an organization, such as receptionists and administrative assistants, are often targets of social engineering attacks. Attackers with some knowledge of an organization's structure will often also target new, untrained employees as well as those who do not seem to understand security policies.

Eliminating social engineering attacks can be difficult, but here are some techniques to reduce their impact which are as follows:

- Ensure that employees are educated on the basics of a secure environment.
- Develop a security policy and computer use policy.
- Enforce a strict policy for internal and external technical support procedures.

Phreaking

Phone phreaking, or simply **phreaking**, is a slang term that describes the activity of a subculture of people who study, experiment with, or explore telephone systems, telephone company equipment, and systems connected to public telephone networks. Phreaking is the art of exploiting bugs and glitches that exist in the telephone system.

Pharming

It is another type of attack that seeks to obtain personal or private financial information through domain spoofing. A pharming attack doesn't use messages to trick victims into visiting spoofed websites that appear legitimate, however. Instead, pharming "poisons" a domain name on the Domain Name Server (DNS), a process known as **DNS poisoning**. The result is that when a user enters the poisoned server's web address into his or her address bar, that user navigates to the attacker's site. The user's browser still shows the correct website, which makes pharming difficult to detect—and therefore more serious. Where phishing attempts to scam people one at a time with an email or instant message, pharming enables scammers to target large groups of people at one time through domain spoofing.

2.5 MALICIOUS SOFTWARE

Some software infiltrates one or more target computers and follows an attacker's instructions causing damage, escalating security privileges, divulging private data, or even modifying or deleting data. The purpose of malware is to damage or disrupt a system, the effects of which can range from slowing down a PC to causing it to crash, enabling the theft of credit card numbers, and worse. Simply surfing the Internet, reading email, or downloading music or other files can infect a personal computer with malware—usually without the user's knowledge. Refer Fig. 2.7.

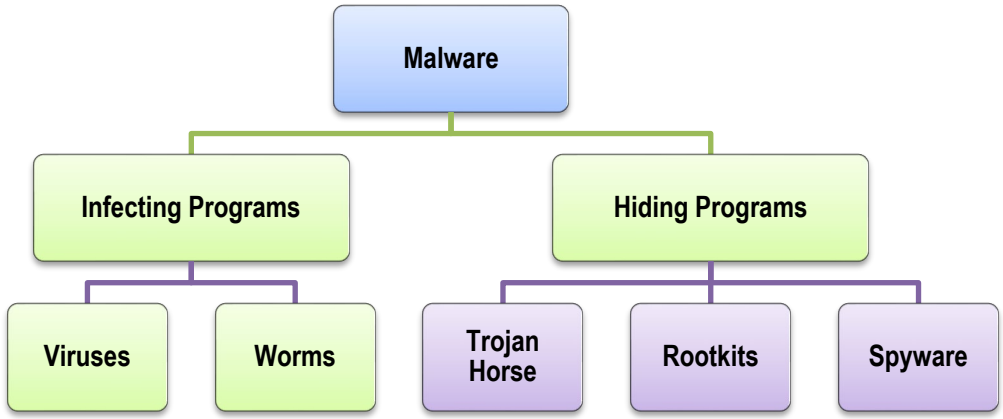


Fig. 2.7: Categories of Malware

Malware exists in two main categories: **Infecting programs** and **Hiding programs**. Infecting programs actively attempt to copy themselves to other computers with the main purpose is to carry out an attacker's instructions on new targets, whereas hiding programs hide in the computer, carrying out the attacker's instructions while avoiding detection. Refer Table 2.4.

Table 2.4: Categories of Malware

Virus	A computer virus is a software program that attaches itself to or copies itself into another program on a computer. The purpose of the virus is to trick the computer into following instructions not intended by the original program developer. Users copy infected files from another computer on a network, from a flash drive, or from an online service. Alternatively, users can transport viruses from home and work on their portable computers, which have access to the Internet and other network services. A computer virus acts in a similar fashion to a biological virus. It "infects" a host program and may cause that host program to replicate itself to other computers. The virus cannot exist without a host, and it can spread from host to host in an infectious manner.
Worm	A worm is a self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action. The worm's purpose may be simply to reduce network availability by using up bandwidth, or it may take other nefarious actions. The main difference between a virus and a worm is that a worm does not need a host program to infect. The worm is a standalone program.
Trojan Horse	It is a malware that masquerades as a useful program. They look like programs that perform useful tasks, but they hide malicious code that uses

	their outward appearance to trick users into running them. Once the program is running, the attack instructions are executed with the user's permission and authority. Trojans can hide programs that collect sensitive information, open backdoors into computers, or actively upload and download files.
Rootkit	A rootkit modifies or replaces one or more existing programs to hide traces of attacks. Although rootkits commonly modify parts of the operating system to conceal traces of their presence, they can exist at any level—from a computer's boot instructions up to the applications that run in the operating system. Once installed, rootkits provide attackers with easy access to compromised computers to launch additional attacks. Rootkits exist for a variety of operating systems, including Linux, UNIX, and Microsoft Windows. Because there are so many different types of rootkits, and because they effectively conceal their existence once installed on a machine, they can be difficult to detect and remove.
Spyware	Spyware is a type of malware that specifically threatens the confidentiality of information. It gathers information about a user through an Internet connection, without his or her knowledge. Spyware is sometimes bundled as a hidden component of freeware or shareware programs that users download from the Internet, similar to a Trojan horse. Spyware can also spread via peer-to-peer file swapping. Once installed, spyware monitors user activity on the Internet. Spyware can also gather information such as email addresses and even passwords and credit card numbers. The spyware can relay these data to the author of the spyware. The author might use the data simply for advertising or marketing purposes but could employ it to facilitate identity theft. Because spyware exists as independent executable programs, it can perform a few operations, including the following: ♦ Monitoring keystrokes. ♦ Scanning files on the hard drive. ♦ Snooping other applications, such as chat programs or word processors. ♦ Installing other spyware programs. ♦ Reading cookies. ♦ Changing the default homepage on the web browser.

2.6 COUNTER MEASURES

A countermeasure is an action, device, procedure, technique, or other measure that is applied to prevent, avert, or reduce potential threats to computers, servers, networks, Operating Systems (OS) or Information Systems (IS). Countermeasure tools include anti-virus software and firewalls.

Countering Malware

Malware provides a platform for attacks on both personal and business networks. Anti-malware measures are the first line of defense against these attacks. You must take steps to prevent the introduction of malware into your environment. It's always better to prevent malware than to have to fix damage caused by malware. You must develop a security program for preventing malware.

Following are six general steps for preventing malware:

- Create an education (information security awareness) program to keep your users from installing malware on your system.
- Post regular bulletins about malware problems.
- Never transfer files from an unknown or untrusted source unless the computer has an anti-malware utility installed.
- Test new programs or open suspect files on a quarantine computer, one that is not connected to any part of your network, before introducing them to the production environment.
- Install anti-malware software, make sure that software and data are current, and schedule regular malware scans to prevent malicious users from introducing malware and to detect any existing malware.
- Use a secure log on and authentication process.

Another important tactic for countering malware is staying abreast of developments in malware. In addition, you should use anti-malware software on your system to scan all files introduced to workstations and on mail servers.

Protecting Your System with Firewalls

A **firewall** is a program or dedicated hardware device that inspects network traffic passing through it and denies or permits traffic based on a set of rules you determine at configuration. A firewall's basic task is to regulate the flow of traffic between computer networks of different trust levels, for example, between the LAN-to-WAN domain and the WAN domain, where the private network meets the public Internet.

2.7 INTERNAL CONTROLS

Just as risk and opportunity go hand in hand, risk, compliance, and internal controls go hand in hand. Compliance and internal controls are needed to meet an increasing number of laws and regulations and internationally accepted standards.

The process an organization, its internal and external auditors, and its regulators would typically follow to validate the effectiveness of internal controls in controlling risk would include these elements:

- Identify business processes, especially those impacting financial reporting.
- Identify the risks associated with each process.
- Identify the internal controls used to mitigate the risks for each process.
- Create a hierarchy of business processes, risks, and controls.
- Identify the tests to be used in determining the effectiveness of the internal controls.
- Test the internal controls and publish findings.
- Provide an opinion as to the effectiveness of the controls.
- If the controls are found to be ineffective, recommend changes (remediations) and retest the controls.
- Create and maintain a documentation library of the processes, risks, controls, tests, findings, remediations, and so on involved in the risk/control process. This would include a risk/control matrix, process narratives, process flow charts, test procedures, and so forth.
- If the internal controls are found to be effective, business owners and external auditors sign off as part of a certification process.

2.7.1 Internal Control Framework as per Standards on Auditing

A company's management team is responsible for the development of internal control policies and procedures. SA315 defines the system of Internal Control as “the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity’s objectives regarding reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations”.

An Internal Control System -

- facilitates the effectiveness and efficiency of operations.

- helps ensure the reliability of internal and external financial reporting.
- assists compliance with applicable laws and regulations.
- helps safeguarding the assets of the entity.

As per SA315, the five components of any internal control as they relate to a financial statement audit are explained below. All these components must be present to conclude that internal control is effective. Refer Fig. 2.8.

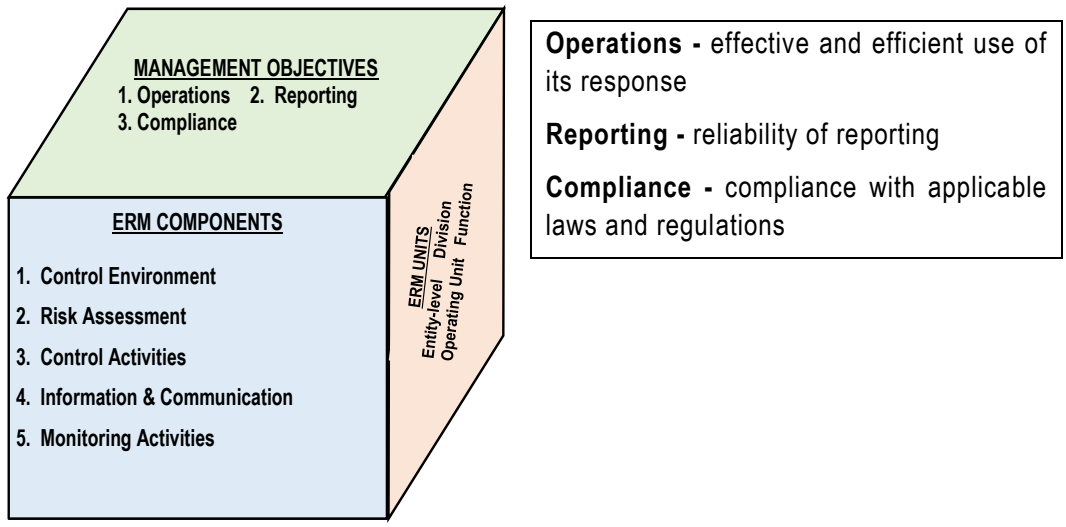


Fig. 2.8: Internal Controls

I. Control Environment

The **Control Environment** is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The Board of Directors and Senior Management establish the tone at the top regarding the importance of internal control, including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

II. Risk Assessment

Every entity faces a variety of risks from external and internal resources. Risk may be defined as the possibility that an event will occur and adversely affect the achievement of objectives. **Risk Assessment** involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances.

Thus, Risk Assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives linked at different levels of the entity. Management specifies objectives within categories of operations, reporting, and compliance with sufficient clarity to be able to identify and assess risks to those objectives. Because economic, industry, regulatory and operating conditions will continue to change; risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Risk assessment includes the following:

- Identification of threats and vulnerabilities in the system.
- The 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.
- The identification and analysis of security controls for the information system.

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.

III. Control Activities

Control Activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

Broadly, the control activities include the 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. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency

objectives. 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.

IV. Information and Communication

Information is necessary for the entity to carry out internal control responsibilities in support of the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Pertinent information must be identified, captured, and communicated in a form and time frame that enables people to carry out their responsibilities.

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the enterprise, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities should be taken seriously. External communication is two-fold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

V. Monitoring of Controls

Monitoring of Controls is an ongoing cyclical process. Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component is present and functioning. Ongoing evaluations built into business processes at different levels of the entity provide timely information. Separate evaluations conducted periodically will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against management's criteria and deficiencies are communicated to management and the Board of Directors as appropriate.

2.7.2 Limitations of Internal Control System

Internal control, no matter how effective, can provide an entity with only reasonable assurance and not absolute assurance about achieving the entity's operational, financial reporting and compliance objectives. Internal control systems are subject to certain inherent limitations, such as:

- Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.
- The fact that most internal controls do not tend to be directed at transactions of an unusual nature, the reasonable potential for human error such as – due to carelessness, distraction, mistakes of judgment and misunderstanding of instructions.

- The possibility of circumvention of internal controls through collusion with employees or with parties outside the entity.
- The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.
- Manipulations by management with respect to transactions or estimates and judgments required in the preparation of financial statements.

2.8 COMPLIANCE

Compliance ensures that an organization has the processes and internal controls to meet the requirements imposed by governmental bodies, regulators, industry mandates or internal policies. However, it can also be -

- a voluntary response to a trade association or vertical industry body, to adopt common practices that make it easier for customers to work with the industry as opposed to a substitute industry.
- a response to a mandated industry standard, such as PCI DSS (Payment Card Industry Data Security Standard) for the handling of information such as that related to credit card transactions.
- an intentional response to protect an enterprise against lawsuits.
- a voluntary response to follow good practices to protect intellectual assets (e.g., patents or trade secrets).

Organizations are tasked with providing proper risk prevention, risk assessment, and effective internal controls for operations, finance, HR, strategy, Board of Directors, and legal to ensure that all corporate compliance obligations are met. To greatly improve organizational control and compliance from the frontline to the executive ranks, controls should be standardized and automated with workflow management systems.

GRC compliance involves aligning organizational activities with the laws and regulations that impact them. These regulations could be legal mandates, like privacy or environmental laws, or voluntarily established company policies and procedures.

For example, a compliance officer at a software company might work to ensure that their systems abide by regulations whereas an environmental inspector might search a construction site for environmental code violations and take the necessary steps to address them.

Compliance involves adhering to rules, policies, standards, and laws set forth by industries and/or government agencies. GRC frameworks encourage organizations to centralize compliance monitoring and stay on top of any laws or regulations that could affect their processes. Breaking compliance could result in devastating financial, legal, and reputational consequences. These could include fines, time and money spent in court, and a tarnished reputation.

SUMMARY

We see that Governance is broader than Compliance as Governance is concerned with the overall conduct of an organization, whereas compliance only results in constraints on that governance. Failing to comply could cost an organization in terms of poor performance, costly mistakes, fines, penalties, and lawsuits.

Regulatory compliance covers external laws, regulations, and industry standards that apply to the company. Corporate or internal compliance deals with rules, regulations, and internal controls set by an individual company. It is important for the internal compliance management program to be integrated with external compliance requirements. The integrated compliance program should be based on a process of creating, updating, distributing, and tracking compliance policies and training employees on those policies.

An initiative to comply with a regulation typically begins as a project as companies race to meet deadlines to comply with that regulation. These projects consume significant resources as meeting the deadline becomes the most important objective. However, compliance is not a one-time event - organizations realize that they need to make it into a repeatable process, so that they can continue to sustain compliance with that regulation at a lower cost than for the first deadline and effectively manage new, updated, and changed compliance requirements. When an organization is dealing with multiple regulations at the same time, a streamlined process of managing compliance with each of these initiatives is critical, or else, costs can spiral out of control and the risk of non-compliance increases. The compliance process enables organizations to make compliance repeatable and hence enables them to sustain it on an ongoing basis at a lower cost.

To create an effective compliance program, organizations need to identify the areas prone to the greatest risk and then develop, implement, and communicate to employees the policies to address those areas of risk. Guidance should be developed to make it easier for employees and vendors to follow compliance policies.

We can now conclude that although Governance, risk management, and compliance can be described separately, individually, and distinctly; they are interrelated and overlap. Therefore, integration of a GRC framework in which all three are considered simultaneously is important so that the focus can be on what needs to be done rather than on how to divide responsibilities among each of the three GRC pillars.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. The objective of Internal Control is to enable an organization to manage its challenges or disruptions seamlessly. Identify which of the following is not an objective of Internal Control.

   (a) Compliance with applicable laws and regulations

   (b) Meeting sales targets

   (c) Reliability of internal and external financial reporting

   (d) Effectiveness and efficiency of operations

2. When DXN Ltd. decided to adopt automation to support its critical business processes, it exposed itself to number of risks. One risk that the automated process could lead to breakdown in internal processes, people and systems is a type of _____.

   (a) Operational Risk

   (b) Financial Risk

   (c) Strategic Risk

   (d) Compliance Risk

3. A huge oil spilled from an oil well run by ABC Petroleum, one of largest oil companies in world, and resulted in an assessed environmental damage of about USD 20 Billion. The company expanded an amount of USD 2 Billion on promotional ads informing the world that it is an environment friendly company. The promotional advertisements were done to prevent the company from _____ damage.

   (a) Strategic

   (b) Operational

   (c) Financial

   (d) Reputational

4. Risk Management enables an organization in various manner except one. Choose the correct answer.

   (a) to evaluate all risks at enterprise level

   (b) monitor mitigation actions

   (c) measure and manage the risk

   (d) organizing the risk

5. Mr. X has setup his new business of manufacturing color pens. He is well known about various kinds of risks involved in his business; however, he unintentionally violated some industry regulations while setting up his business. Which category of the risk does this refer to?

(a) Strategic

(b) Financial

(c) Compliance

(d) Operational

ANSWERS/SOLUTIONS

1.	**(b)**	**2.**	**(a)**	**3.**	**(d)**	**4.**	**(d)**	**5.**	**(c)**

CHAPTER 3

ENTERPRISE RISK MANAGEMENT FRAMEWORK

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- build fundamental understanding about Enterprise Risk Management (ERM) and its related benefits.
- comprehend the ERM Framework and its implementation by Plan, Implement, Measure and Learn (PIML).

CHAPTER OVERVIEW

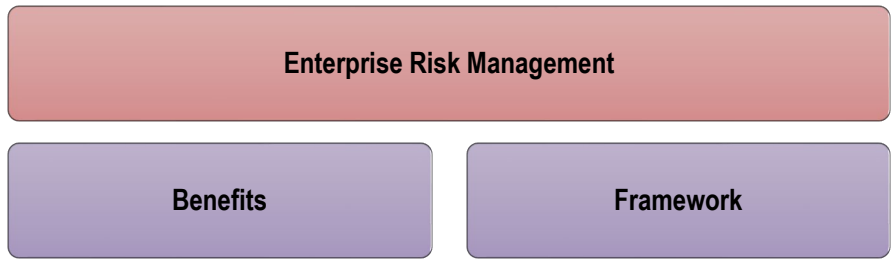


Illustration: ERM Case Study – Kodak

Founded in 1892, Kodak was registered as a trademark for a camera that could be used by the mass market. Kodak grew to be a leading and large enterprise, and at its peak in the early 1980s, it employed 130,000 people worldwide.

One of Kodak's cash cows was its film products. Kodak was a leading manufacturer of various film products to all types of non-digital cameras and video recorders. When the digital products came to market and replaced the old-style cameras, the demand for film products declined.

One of the high impact risks for Kodak back then in the pre-digital era was that a disruptive technology would diminish the demand for its one of the core products: film-based products. This trend presented itself with varying degrees of impact in virtually every market segment it operated in, from consumer film cameras to digital X-rays to digital moviemaking.

Kodak, of course, did move into digital cameras, printers, and related technologies. But clearly not with either enough determination or success. Once an iconic brand, the photo film company failed for decades to act on the threat that digital photography posed to its business and eventually filed for bankruptcy in 2012. The company's own research in 1981 found that digital photos could ultimately replace Kodak's film technology and estimated it had 10 years to prepare.

What went wrong?

Unfortunately, Kodak did not prepare and stayed locked in the film paradigm. The Board reinforced this course when in 1989 it chose a candidate as CEO who came from the film business over an executive interested in digital technology. Had the company acknowledged the risks and employed ERM strategies, it might have pursued a variety of strategies to remain successful. The company's rival, Fuji Film, took the money it made from film and invested in new initiatives, some of which paid off. Kodak, on the other hand, kept investing in the old core business.

Risk Management Perspective

Consider and evaluate the risks of disruptive technologies, and the need to manage transformation when it can be evolution well in advance of looming crises. The bigger the ship, the more time you need to turn it. Some high impact risks, such as the traditional film market dying in the case of Kodak, require broad strategic shifts.

3.1 INTRODUCTION

Organizations practice risk management in several different ways. When an organization adopts a holistic approach and considers all the risks that it faces and how these risks could impact its strategy, projects, and operations, then the organization is embarking towards ERM approach.

Consider a Sports club where the key objective of the management is to maximize the attendance at all the games that may include various activities such as marketing, advertising, allocation and sale of tickets as well as logistical arrangements to ensure that the experience at the game is as good as possible. Part of maximizing attendance at games will be to ensure that there are adequate parking and transport arrangements, together with suitable catering and other welfare arrangements in the ground.

By identifying the key activities that deliver the selected core process, the club can identify the risks that could impact both these activities and the core process. Targets can then be set for increased attendance at future games, and responsibility for the success of this core process has been allocated to the commercial director of the club. A consideration of the opportunities for increasing attendance at games can also be included in this broader Enterprise Risk Management (ERM) approach.

3.2 ENTERPRISE RISK MANAGEMENT (ERM)

ERM is a risk-based approach which includes the methods and processes used by organizations to manage risks. ERM-related goals and objectives are of little value unless they can be organized and modelled together in such a manner that management can look at the various aspects of the task and understand how they interact and relate in a multidimensional manner. ERM provides a framework for risk management which involves:

- identifying potential threats or risks.
- determining how big a threat or risk is.
- what could be its consequence, and its impact, etc.
- implementing controls to mitigate the risks.

"ERM is defined as a process, affected 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."

The following may be considered for the sake of understanding ERM.

- **ERM is a Process.** An often-misused expression, the dictionary definition of a process is a set of actions designed to achieve a result. However, this definition does not provide help for many professionals. The idea to remember is that a process is not a static procedure such as the use of an employee badge that is designed and built to allow only certain authorized persons to enter a locked facility. Such a badge procedure—like a key to a lock—only allows or does not allow someone entry to the facility. A process tends to be a more flexible arrangement. In a credit approval process, for example, acceptance rules are established with options to alter them given other considerations. An enterprise might bend the credit rules for an otherwise good credit customer that is experiencing a short-term problem. ERM is that type of process. An enterprise often cannot define its risk management rules through a small, tightly organized rule book. Rather, there should be a series of documented steps to review and evaluate potential risks and to act based on a wide range of factors across the entire enterprise. Therefore, ERM is a process but a dynamic one wherein the steps are altered and modified to suit the requirements of the business.

- **ERM processes are implemented by people in the enterprise.** An ERM will not be effective if it is only implemented through a set of rules sent into an operating unit from a distant corporate headquarters, where those corporate people who drafted the rules may have little understanding of the various local operating unit decision factors surrounding them. The risk management process must be managed by people who are close enough to that risk situation to understand the various factors surrounding that risk including its implications.

- **ERM is applied by setting strategies across the overall enterprise.** Every enterprise is constantly faced with alternative strategies regarding a vast range of potential future actions. Should the entity acquire another complementary business or just build internally? Should they adopt new technology in their manufacturing processes or stick with the tried and true? An effective ERM should play a major role in helping to establish those alternative strategies. Since many enterprises are large with many varied operating units, ERM should be applied across that entire enterprise using a portfolio type of approach that blends a mix of high- and low-risk activities.

- **Concepts of risk appetite must be considered.** A newer concept or term for many managers, **Risk appetite** is the amount of risk, on a broad level, that an enterprise and its

individual managers are willing to accept in their pursuit of value. Risk appetite can be measured in a qualitative sense by looking at risks in such categories as high, medium, or low; alternatively, it can be defined in a quantitative manner.

Risk tolerance is the amount of loss that an organization/individual is prepared to handle while making a decision. For example - an investor or trader with a high net worth can assume more risk and may get through different times and can take decisions after observing the situation considerably. The smaller the percentage of an investor's overall net worth, the more aggressive the risk tolerance can be. In such a case, the investor may sell his stocks on seeing them dipping in. Risk appetite and risk tolerance can be viewed as the "two sides of the same coin" as they relate to organizational performance over time. Risk appetite is about "taking risk" and risk tolerance is about "controlling risk." For risk appetite to be adopted successfully in decision making, it must be integrated with control environment of the organization through risk tolerance.

An understanding of risk appetite covers a wide variety of issues that will be discussed further in subsequent chapters as part of the discussions of implementing ERM in a variety of organizational environments. The basic idea is that every manager and, collectively, every enterprise should have some level of appetite for risk. Some will accept risky ventures that promise high returns while others prefer more to guaranteed-return low-risk ventures. One can think of this appetite for risk concept or measure in terms of two investors. One may prefer very low risk but typically low-return money market or index funds while another may invest in low-cap start-up technology stocks. That latter investor can be described as having a high appetite for risk. For example, if a company decides to invest in real estate, it represents numerous risks like high capital outlay requirement, or maybe loss of business due to recession. In such a case, there can be a high possibility of failure. However, if the economic conditions will be in favor, this business can get a high return to organization.

- **ERM provides only reasonable, not positive assurance on objective achievements.** The idea here is that an ERM, no matter how well thought out or implemented, cannot provide management or others with any assured guarantee of its outcomes. A well-controlled enterprise, with people at all levels consistently working toward understood and achievable goals, may achieve those objectives period after period—even over multiple years. However, an unintentional human error, an unexpected action by another, or even a natural disaster can occur. For example- The operational efficiency of organizations decreased during covid 19 pandemic, whereas the organization which has applied ERM to raise its liquidity capability generated a positive and significant effect on its operational efficiency. However, despite an effective ERM process, an enterprise can experience a major and totally unexpected failure. Reasonable assurance does not provide absolute assurance.

- **ERM is designed to help attain the achievement of objectives.** An enterprise, through its management, should work to establish high-level common objectives that can be shared by all stakeholders. Examples here are such matters as achieving and maintaining a positive reputation within an enterprise's business and consumer communities, providing reliable financial reporting to all stakeholders, and operating in compliance with laws and regulations. The overall ERM program for an enterprise should help it to achieve those objectives.

Benefits of Enterprise Risk Management

No entity operates in a risk-free environment and ERM does not create such an environment. Rather, it enables management to operate such environment. ERM provides enhanced capability to do the following:

- **Align risk appetite and strategy:** Risk appetite is the degree of risk, on a broad-based level that an enterprise (any type of entity) is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.
- **Link growth, risk, and return:** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks and establish acceptable levels of risk relative to growth and return objectives.
- **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses – risk avoidance, mitigation, transference, and acceptance. ERM provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses:** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
- **Identify and manage cross-enterprise risks:** Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
- **Provide integrated responses to multiple risks:** Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.
- **Seize opportunities:** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- **Rationalize capital:** More robust information on an entity's total risk allows management to assess more effectively overall capital needs and improve capital allocation.

3.3 ERM FRAMEWORK (For IT GOVERNANCE Issues)

The COSO ERM framework for risk management typically involves identifying events or circumstances relevant to an organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. Various potential threats to computer systems affect the **Confidentiality**, **Integrity**, and **Availability (CIA)** of data and computer systems. For successful continuity of business, it is very essential to evaluate these potential threats and control them to minimize the impact of these threats to an acceptable level. By identifying and pro-actively addressing risks and opportunities, business enterprises create and protect value for their stakeholders, including owners, employees, customers, regulators, and society overall.

The approach adopted by COSO suggests that enterprise risk management is a multidirectional, iterative process in which almost any component can and does influence all other components. In simple terms, this framework suggests that in order to achieve a successful ERP initiative, an organization needs to implement all eight components as shown in the Fig. 3.1 in relation to each of the four categories of objectives indicated across the top, in all parts of the organization, as indicated on the side of the cube. The COSO ERM cube illustrates the links between objectives that are shown on the top and the eight components shown on the front, which represent what is needed to achieve the objectives. The third dimension represents the organization's units, which portrays the model's ability to focus on parts of the organization as well as the whole. Refer Fig. 3.1 for COSO ERM Framework.

Relationship of ERM and Internal Controls

The Internal Control Framework (ICF - discussed in Chapter 2) and Enterprise Risk Management (ERM) have similarities and differences. Both frameworks aim to improve risk management in organizations. The ICF focuses on internal controls to ensure the achievement of objectives and the reliability of financial reporting. It includes elements such as control environment, risk assessment, control activities, information and communication, and monitoring. ERM, on the other hand, takes a broader approach by considering risks and opportunities that could affect the achievement of objectives. It includes elements such as internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. While both frameworks address risk management, ERM provides a more comprehensive and integrated approach that considers both internal and external factors. The objectives of COSO ERM Framework (Refer Fig. 3.1) that reflect the responsibility of different executives across the entity and address different needs are provided below:

- **Strategic -** These are mission driven high level goals and objectives (Governance, Strategic objectives, business model, external forces, etc.) and are aligned with an entity's mission.

- **Operations -** These objectives refer to the effective and efficient use of resources development, management, and allocation (Business processes, upstream value chain, downstream value chain, etc.).
- **Reporting -** These objectives surround an entity's need for reliable reporting that involve information gathering, analysis and communication (Information Technology, Financial, Internal, Intellectual property, etc.).
- **Compliance -** These objectives refer to an entity's need to comply with applicable laws and regulations (Securities and Exchange commission, environmental, legal, contractual, etc.).

COSO Coverage Areas

The **four organizational levels of COSO ERM Framework** that emphasize the importance of managing risks across the enterprise to achieve operational, financial, and compliance objectives are **Entity level, Division, Operating Unit** and **Function**.

- **Entity-level** controls are those that influence the entire organization. Often, these controls are focused on establishing and maintaining a good culture and supporting communication throughout the organization. These controls are implemented, or influence actions, throughout the organization. For example, one entity-wide control in an organization would be a corporate code of ethics.
- **Division level** controls may be one level removed, or below, entity-wide controls. Depending on the organization's structure, there may or may not be divisions. When there are, they are often associated with national or regional boundaries such that the internal controls align with regulatory requirements, such as filing Securities and Exchange Board of India (SEBI) reports on time and accurately.
- An **Operating Unit** isn't always limited to physical proximity, but instead is focused on the activities the operating unit is responsible for performing. For example, an accounting department may be responsible for accounts payable, accounts receivable, cash management, and financial reporting. Accounts receivable may have a control that requires a monthly outstanding balance report to be reviewed.
- **Function** refers to a specific job in the operating unit.

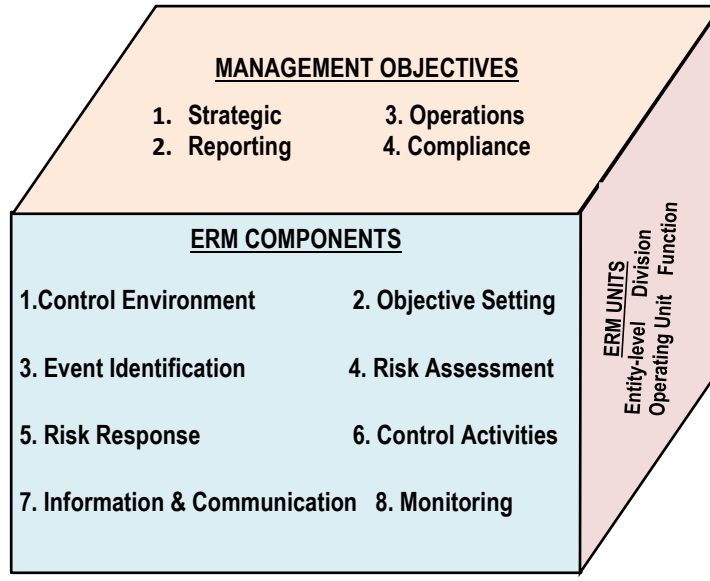


Fig. 3.1: COSO ERM Cube

ERM framework consists of eight interrelated components that are derived from the way management runs a business and are integrated with the management process. These components are as follows (Fig. 3.1):

(i) **Control Environment:** The control environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. Management sets a philosophy regarding risk and establishes a risk appetite. The control environment sets the foundation for how risk and control are viewed and addressed by an entity's people. The core of any business is its people – their individual attributes, including integrity, ethical values, and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

(ii) **Objective Setting:** Objectives should be set before management can identify events potentially affecting their achievement. ERM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite. Objectives need to be set in reality and with sufficient resources available to achieve them and meet the **SMART** test.

- **Specific:** Clearly defined,
- **Measurable:** Easily quantifiable in monetary terms,

- **Attainable:** Achievable through best efforts,
- **Relevant:** Entity must be in need of these, and
- **Timely:** Achieved within a given time frame.

(iii) **Event (or Risk) Identification:** Potential events that might have an impact on the entity should be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Opportunities are channeled back to management's strategy or objective-setting processes. Management identifies inter-relationships between potential events and may categorize events to create and reinforce a common risk language across the entity and form a basis for considering events from a portfolio perspective.

(iv) **Risk Assessment:** Identified risks are analyzed to form a basis for determining how they should be managed. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

(v) **Risk Response:** Management selects an approach or set of actions to align assessed risks with the entity's risk tolerance and risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing, and sharing risk.

(vi) **Control Activities:** Policies and procedures are established and executed to help ensure that the risk responses that management selected are effectively carried out.

(vii) **Information and Communication:** Relevant information is identified, captured, and communicated in a form and time frame that enables people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing, and responding to risk. Effective communication also should occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities.

(viii) **Monitoring:** The entire ERM process should be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of the ERM processes or a combination of both.

COSO ERM Rainbow Double Helix

In 2017, COSO published an additional guidance entitled ERM – Integrating Strategy and Performance to connect ERM more clearly with a multitude of stakeholder expectations; position risk in the context of performance, rather than as an isolated exercise; enable organizations to better anticipate risk, not simply the potential for crises; and provide an understanding that change creates opportunities. This is to bring greater focus to the positive contribution to performance that can be made by ERM as shown in Fig. 3.2.

The basis of the 2017 COSO guidance is that ERM should be embedded into the activities of an organization, including the mission, vision, and core values. In developing strategy, business and performance objectives, an organization should consider the implications of the selected strategy; the risks to strategy and performance; and the possibility of the strategy not aligning with core values.

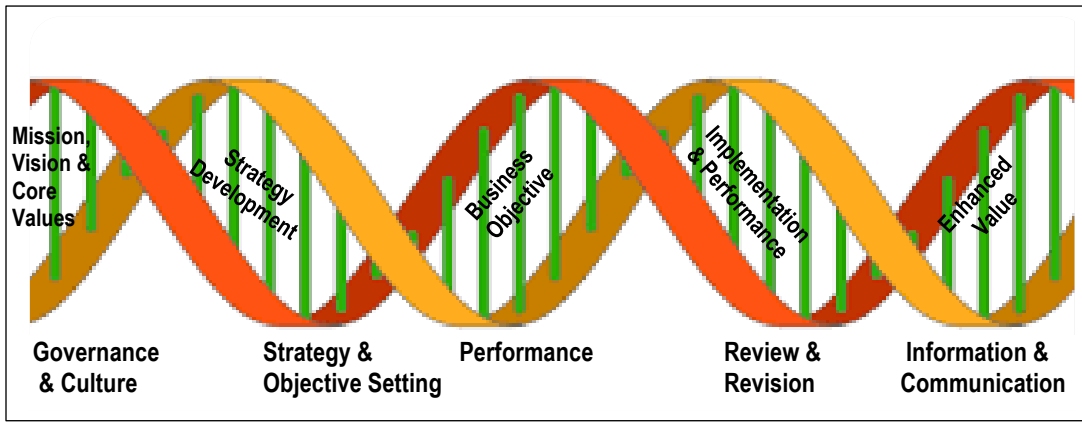


Fig. 3.2: COSO ERM Rainbow Double Helix

The 2017 COSO ERM framework clearly differentiates between ERM and internal control and enhances the references to risk appetite and risk tolerance. The intention of the framework is to elevate discussion of strategy, enhance the alignment between performances and more explicitly link ERM into decision-making. There is greater emphasis on the relationship between risk and value and the benefits of integration of ERM. Finally, the framework underlines the role of culture in the achievement of successful ERM. ERM is strategic and Internal control is operational and targeting a particular risk items or control violation. The organizations need to identify the best framework for optimizing strategy and performance to integrate ERM throughout the organization to achieve benefits, including:

- identifying new opportunities.
- identifying and managing risk organization-wide to sustain and improve performance.

- increasing positive outcomes and reducing negative surprises.
- reducing performance variability and minimize disruption.
- improving resource deployment and enhance resource allocation.
- enhancing enterprise resilience, not only to survive but also to evolve and thrive.

COSO's new ERM framework now includes five components or categories with 20 principles spread throughout each component. Those components are as follows:

1. **Governance and Culture:** Governance sets the tone for the organization and establishes oversight responsibilities for ERM. Culture which relates to ethical values, desired behaviors and understanding of risk, is reflected in decision-making and includes ethical values and responsible business behavior. There are five principles for this component as provided in the Table 3.1 below:

Table 3.1: Principles for Governance and Culture

Exercises Board Risk Oversight	Risk governance and culture start at the top with the influence and oversight of the board. Board members must be accountable and responsible for risk oversight and possess the required skills, experience, and business knowledge.
Establishes Operating Structures	Strategy is executed by organization and execution of day-to-day operations to achieve business objectives. How the operating model is administered and governed can introduce new and different risks or complexities.
Defines Desired Culture	COSO frames desired behaviors within the context of culture, core values and attitudes toward risk. Whether an organization considers itself to be risk adverse, risk neutral or risk aggressive, it should have a risk-aware culture.
Demonstrates Commitment to Core Values	Culture and tone at the top is defined by the operating style and personal conduct of management and the board of directors and it must be driven deep down into the organization.
Attracts, Develops and Retains Capable Individuals	Management must define the knowledge, skills and experience needed to execute strategy; set appropriate performance targets; attract, develop, and retain appropriate personnel and strategic partners; and arrange for succession.

2. Strategy and Objective-Setting: The updated COSO framework elevates the discussion of strategy and the integration of ERM with strategy by asserting that all aspects and implications of strategy need to be considered when setting strategy. There are four principles for this component as provided in the Table 3.2 below:

Table 3.2: Principles for Strategy and Objective-Setting	
Analyses Business Context	The updated framework considers the business context and the role of internal and external stakeholders. The point is that management must consider risk from changes in the business context and adapt accordingly in executing strategy.
Defines Risk Appetite	The organization defines risk appetite in the context of creating, preserving, and realizing value. The risk appetite statement is considered during strategy setting, communicated by management, embraced by the board, and integrated across the organization.
Evaluates Alternative Strategies	Alternative strategies are built on different assumptions – and those assumptions may be sensitive to change. The organization evaluates strategic options and sets its strategy to enhance value, considering risk resulting from the strategy chosen.
Formulates Business Objectives	Management establishes objectives that align with and support the strategy at various levels of the business. These objectives should consider, and be aligned with, risk appetite. ERM, strategy and objective-setting work together in the strategic-planning process. Risk appetite should be aligned with strategy and business objectives to successfully implement strategy.

3. Performance: Risks that can impact achievement of strategy and business objectives need to be identified and assessed and risks prioritized by severity in the context of risk appetite, so that risk responses can be selected. There are five principles for this component as provided in the Table 3.3 below:

Table 3.3: Principles for Performance	
Identifies Risk	The organization identifies new and emerging risks, as well as changes to known risks to the execution of its strategy. The risk identification process should consider risks arising from a change in the business context and risks currently existing but not yet known.
Assesses Severity of Risk	Depending on the anticipated severity of the risk, COSO suggests the use of qualitative and quantitative approaches in assessment processes. Scenario analysis may be appropriate in assessing risks that could have an extreme impact.

Prioritizes Risk	The organization prioritizes risks as a basis for selecting risk responses using appropriate criteria. Risk criteria might include adaptability, complexity, velocity, persistence and recovery, as well as acceptable variation in performance.
Implements Risk Responses	Risk responses may accept, avoid, exploit, reduce and share risk. In selecting risk responses, management considers such factors as the business context, costs and benefits, severity of the risk, and the appetite for risk.
Develops Portfolio View	Portfolio view is a composite view of the risks the organization faces relative to business objectives, which allows management and the board to consider the nature, likelihood, relative size, and interdependencies of risks, and how they may affect performance.

4. **Review and Revision:** The fourth component focuses on monitoring risk management performance. By reviewing organization performance, an organization can effectively monitor how well the ERM components are functioning over time and following substantial change, emerging risks and what revisions are necessary. There are three principles for this component as provided in the Table 3.4 below:

Table 3.4: Principles of Review and Revision

Assesses Substantial Change	Change can create significant competitor performance gaps or invalidate critical assumptions underlying strategy. Monitoring substantial change is built into business processes in the ordinary course of running the business.
Reviews Risk and Performance	Risk responses must be evaluated to ensure they are performing as intended. The task of assessing risk responses is typically owned by those accountable for the effective management of identified risks and by assurance providers.
Pursues Improvement in ERM	ERM should be improved continuously over time. Even mature ERM processes can become more efficient and effective in increasing its value contributed. Embedding continuous evaluations can systematically identify improvements.

5. Information, Communication and Reporting: The final component recognizes the vital need for a continuous process to obtain and share relevant information. ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization. There are three principles for this component as provided in the Table 3.5 below:

Table 3.5: Principles of Information, Communication and Reporting	
Leverages Information and Technology	Information systems provide the organization with the data and information to support ERM. Factors influencing technology selection include the strategy, marketplace needs, competitive requirements, and the associated costs and benefits.
Communicates Risk Information	The organization reports on risk at multiple levels across the organization. Organizations use different channels to communicate risk data and information to internal and external stakeholders.
Reports on Risk, Culture and Performance	Risk reporting encompasses information required to support decision-making and enable the board and others to fulfill their risk oversight responsibilities. There are many different types of reports on risk, culture, and performance.

The organizations need to identify the best framework for optimizing strategy and performance to integrate ERM throughout the organization to achieve benefits, including the following factors as given in the Table 3.6 below:

Table 3.6: Factors to integrate ERM in an organization	
Factors	**Explanation**
Increase the range of Opportunities	To identify new opportunities and unique challenges associated with current opportunities.
Identify and manage the risk entity-wide	To identify and manage the entity-wide risks to sustain and improve performance.
Increase positive outcomes and reduce negative surprises	To identify responses, reduce surprises and related costs or losses, while profiting from advantageous developments.
Reduce performance variability	To anticipate the risks that would affect performance and put in place the actions needed to minimize disruption and maximize opportunity.
Improve resource deployment	To assess overall resource needs, prioritize resource deployment, and enhance resource allocation.
Enhance enterprise resilience	To anticipate and respond to change, not only to survive but also to evolve and thrive.

Implementing ERM

Implementing an ERM approach in an organization will certainly affect its culture that may further require process and behavioral modification from everyone involved. It is likely to be an ongoing process that involves applying an initial methodology and through iterations continuously improving the process, to enable as mature and embedded an approach as possible within the organization.

Whilst ERM is an embedded process in some organizations and being adopted by others. There is no single, combined or overwhelmingly accepted methodology that forms ERM and will vary between organizations.

Implementing Risk Management by PIML (Plan, Implement, Measure and Learn)

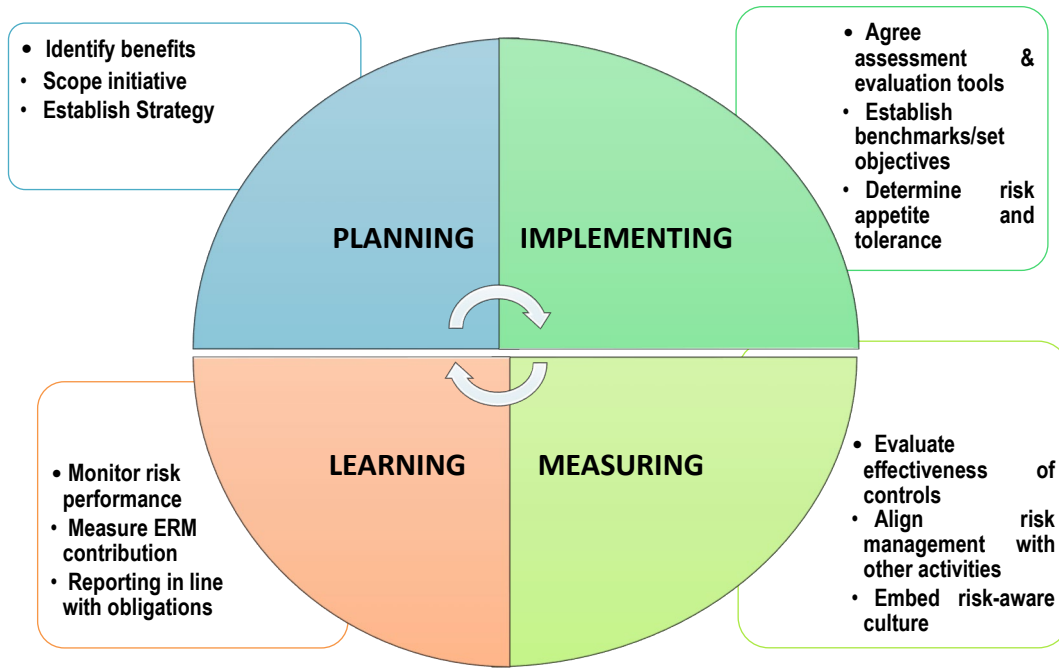


Fig. 3.3: Implementing Risk Management by PIML

The center arrow in the Fig. 3.3 indicates that it's a continuous process such that once the process gets completed from planning to learning, the next round of planning with the scope of improvement after an appropriate time and regular review is required. Refer Table 3.7 for PIML description.

Table 3.7: PIML Description

Planning	1. Identify intended benefits of the ERM initiative and gain board support. 2. Plan the scope of the ERM initiative and develop common language of risk. 3. Establish the ERM strategy, framework, and the roles and responsibilities.
Implementing	4. Adopt suitable risk assessment tools and an agreed risk classification system. 5. Establish risk benchmarks and undertake risk assessments. 6. Determine risk appetite and risk tolerance levels and evaluate the existing controls.

Measuring	7. Evaluate the effectiveness of existing controls and introduce improvements. 8. The risk management activities should be designed to be aligned as far as possible with the existing processes within the organization. 9. Embed risk-aware culture and align risk management with other activities in the organization.
Learning	10. Monitor and review risk performance indicators to measure ERM contribution. 11. Report risk performance in line with obligations and monitor improvement.

SUMMARY

The chapter has highlighted the need for implementing the right type of IT controls as IT is pervasive in all types of enterprises today. For implementing IT controls, it is important to consider both regulatory and management perspectives 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 along with the Enterprise Risk Management have been explained. This will enable us 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. Finally, the features of the COSO frameworks are being addressed. COSO frameworks have more focus on the internal environment, rather than the influence of the business environment, regulatory conditions, and external stakeholders. COSO ERM risks are mostly about losses and risk response is about reducing the likelihood and severity of losses, rather than examining the taking of risk to achieve return. This chapter has also provided an overview of the critical role of IT in achieving business objectives.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Enterprise Risk Management (ERM) framework consists of interrelated components that are used to identify events that are relevant to organization's objective. Identify which of the following is not a component of ERM Framework.

   (a) Internal environment

   (b) Organization chart

   (c) Objective setting

   (d) Event identification

2. Mr. Anil is working with XYZ Company that is under the process of adopting Enterprise Resource Management (ERM) framework. He prepared a list of policies and procedures that need to be established and executed to ensure that the risk responses that management selected are effectively carried out. Which component of ERM is referred here during this activity?

   (a) Risk Assessment

   (b) Control Activities

   (c) Information and Communication

   (d) Monitoring

3. In COSO ERM Cube, …….. are the policies and procedures that are established and executed to help ensure that the risk responses that management selected are effectively carried out.

   (a) Control Activities

   (b) Risk Management

   (c) Risk Response

   (d) Objective Setting

4. Following are the benefits to integrate ERM throughout the organization. Choose the odd one out.

   (a) increase positive outcomes and reduce negative surprises.

   (b) reduce performance variability and maximize disruption.

   (c) improve resource deployment and enhance resource allocation.

   (d) enhance enterprise resilience, not only to survive but allocation

5. Which of the following "Principles for Performance" provides the composite view of risks that organization faces relative to business objectives?

   (a) Implementation of Risk Reponses

   (b) Development of Portfolio view

   (c) Prioritization of Risk

   (d) Formulation of Business Objective

ANSWERS/SOLUTIONS

1.	(b)	2.	(d)	3.	(a)	4.	(b)	5.	(b)

CHAPTER 4

INFORMATION SYSTEM SECURITY POLICY

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- comprehend the knowledge about various components of an information system and its working.
- understand the need for protection of information systems.
- identify information security policies, procedures, related standards, and guidelines.
- acknowledge the need of information security.
- identify the possibilities of frauds relating to technology.

CHAPTER OVERVIEW

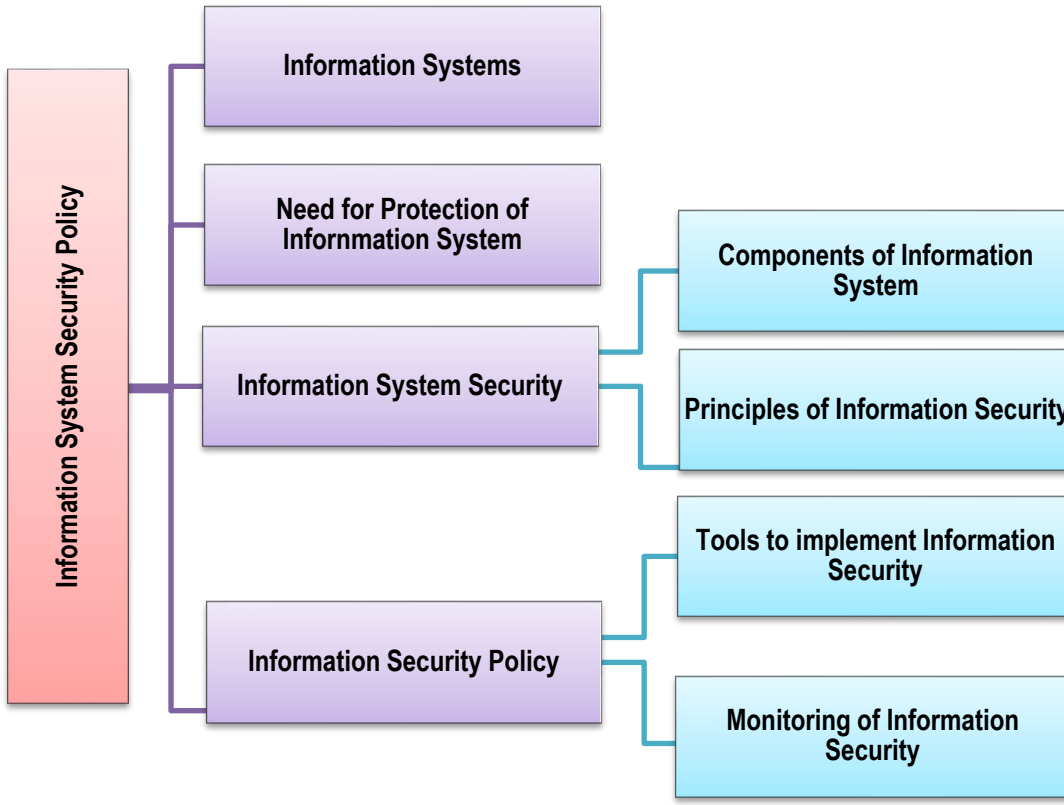


Illustration - Case A

XYZ Ltd. is the Delhi based software solution provider company that deals in developing and customizing software for their clients on a project basis. The company also provides the technical and business support in an outsourced capability. The major business and service areas of company includes IT consulting, web design and development, mobile application development, software development, robotics, and Internet marketing. The company has an employee base of 100-150 people, and has huge clientele from a wide range of industries including aerospace, automotive, consumer goods, food, metal fabrication, medical, pharmaceutical, solar panel, etc.

As the company XYZ Ltd. deals in software development, web applications, and mobile applications development business, any information loss such as losing codes, software

programs, applications, etc. may become crucial for the company and its day- to- day operations. Any information security breach incident may affect the productivity of the organization. This may ultimately result into serious outcomes, such as financial losses, loss of productivity, delayed projects, loss of intellectual property, losing clients and, above all, loss of reputation. The top management and software developers acknowledge that information security is the critical aspect for business continuity of the organization; because if there is any loss in the productivity of the company, that directly affects the relationship with clients or losing the clients. If the client losses the trust in the company, it may not get the business form clients.

Support of Top Management

- Although the top management of company is aware of the importance of information security for the company, yet a consistent support of the same is missing.
- The senior management has reluctant approach towards this issue. They are also facing constraints in budget.
- There is no information security officer or any similar authority in the company.
- Information Security Management (ISM) activities of the organization are managed by the network team. This leads to lack of co-ordination and control.

Information Security Policy

- There was no documented information security policy in the company.
- There are no defined information security roles and responsibilities of employees.
- Also, there is also no classification of accountabilities for various information security-related functions in the organization.
- In an ad-hoc manner, employees can take actions on their own to manage information security related to their work in adhoc manner.

Information Security Training to Employees

- No formal staff training was given to the employees neither at joining nor later.
- The company does not maintain the procedures to identify the information security required by employees as per their specific job requirement.
- Every employee can take their own decision related to information security. There is no formal procedure or consulting authority.
- A need for regular information security training and awareness programmes were realized during of interviews with employees.

- All the decision taken by employees is based on their experience irrespective of how critical it may be.

This case indicates that company needs to identify key risks and vulnerabilities to its information and information assets, and accordingly define an information security policy and implementation mechanism; as there is no documented information security policy, no risk management and security culture in the company. This will certainly help the company to improve in terms of productivity, employees' satisfaction, and clients' trust.

In the absence of information security training program, the employees of company XYZ Ltd. are less aware about various information security threats and its countermeasure. A very few employees knew about the risk related to information but in the absence of any policy or guidelines, they have no idea what to do about it. There is a general lack of awareness about penalties or legal consequences of any information security breach incident. There is no mechanism to monitor the attitude of employees on information security. Moreover, the company does not have any forum to discuss these issues. If anyone faces some problem, they take ad-hoc actions within their peer group to resolve the issue.

The above case raises the following questions:

1. Is information a critical business asset for your organization?
2. What is purpose of Information Security?
3. How information security incident can affect the business activities of an organization?

The answer of these questions are discussed in the later part of this chapter.

4.1 INTRODUCTION

Over the past few centuries, the world has transitioned from connections among individuals to a greater emphasis on connections among systems. We now have systems that are constantly exchanging information about various things and even about us, many a times without human intervention. This inter-networking of physical devices, vehicles, smart devices, embedded electronics, software, sensors or any such device and human resource is often to make an integration among key elements, namely, People, Computer Systems (Hardware, Operating System and other Software), Data Resources, Networking, and Communication System.

4.2 INFORMATION SYSTEMS

- **Information System (IS)** is a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.
- The system needs inputs from user (key in instructions and commands, typing, scanning) which will then be processed (calculating, reporting) using technology devices such as computers, and produces output (printing reports, displaying results) that will be sent to another user or other system via a network and a feedback method that controls the operation.
- The main aim and purpose of each Information System is to convert the data into information which is useful and meaningful. It comprises of two parts: **Information** and **System**.
- An Information System depends on the resources of **people** (end users and IS specialists), **hardware** (machines and media), **software** (programs and procedures), **data** (data and knowledge bases), and **networks** (communications media and network support) to perform input, processing, output, storage, and control activities that transform data resources into information products.
- The Information System model highlights the relationships among the components and activities of information systems. It also provides a framework that emphasizes four major concepts that can be applied to all types of information systems.

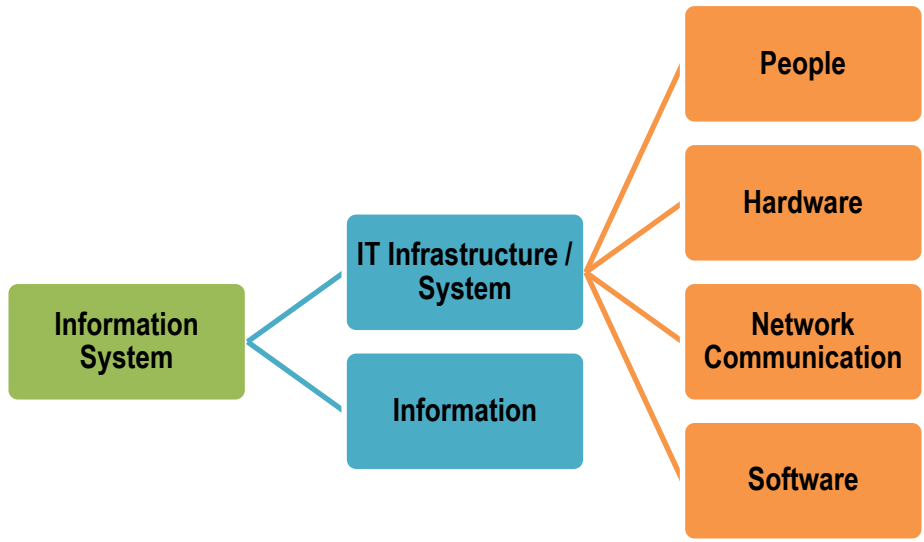


Fig. 4.1: Definition of Information System in an organization

4.3 NEED FOR PROTECTION OF INFORMATION SYSTEMS

- In a computerized Information System, 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 a 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; accurate, 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 x 7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to information security threats than ever before.
- For example, the Denial of Service (DoS) attacks on websites such as yahoo.com and amazon.com, among others, stand as significant cases. These attacks caused these websites to be inaccessible for several hours to a few days, posing a serious threat to the business operations of the affected organizations. Additionally, real concerns arise from virus threats. The IT professionals at organizations affected by infamous viruses like "Melissa" and "I love you" still vividly recall the impact and challenges posed by these incidents.
- Further, hacking and cracking on the Internet is a real threat to virtual organizations which are vulnerable to information theft and manipulations.

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.

Information security performs four important functions for an organization:

- Ensuring the safeguarding of the organization's operational capability.

- Protecting the data and information the organization collects and uses, whether physical or electronic form.
- Enabling the safe operation of applications running on the organization's IT Systems.
- Safeguarding the organization's technology assets.

It is clear from the instances cited above that there are not only many direct and indirect benefits from the use of information systems, but 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;
- Inter connectivity 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.

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. Table 4.1 describes the categorization of various threats that may exist in an organization. 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.

Table 4.1: Threat Categories to Information Security

Category of Threat	Attack Examples
Compromise to intellectual property	Piracy, copyright infringement
Deviation in Quality of Service	Internet Service Provider (ISP)/WAN Service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lighting
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or Vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, Denial of Service
Technical hardware failures/errors	Equipment failure
Technical software failures or errors	Bugs, Code problems, unknown loopholes
Technological Obsolescence	Antiquated or Outdated Technologies
Theft	Illegal confiscation of equipment or information

exm konsa attack hua ha.. destruction se related tha

4.4 INFORMATION SYSTEM SECURITY

The term security is easiest to define by breaking it into pieces. Thus, information systems security is the collection of activities that protect the information system and the data stored in it. People need to protect their privacy. With the increase in the dependency of businesses over information and information system, businesses and organizations are becoming more cautious and responsible for protecting both their intellectual property and any personal or private data they handle. Various laws require organizations to use security controls to protect private and confidential data.

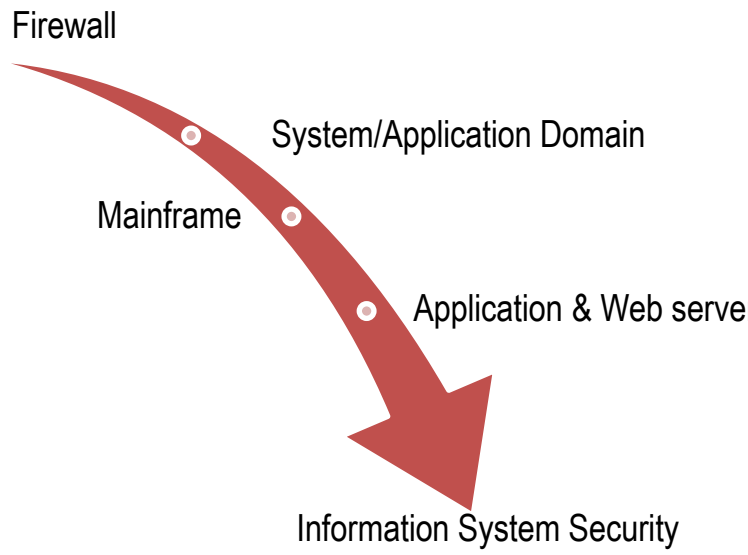


Fig. 4.2: Components of Information System Security

Information system security comprises of the application and technical methods or managerial processes on the information resources such as hardware, software, and data in order to keep organizational assets and personal privacy protected. Information system security is responsible for the integrity and safety of system resources and activities. Most organizations in developed countries are dependent on the secure operation of their information systems.

Information System 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. The hardware system like mainframe or personal computers is protected through password and webserver or application server used in networking can be protected from viruses, bugs, worms, etc. In organizations where a security breach has been experienced, the effectiveness of information security policy and procedures must 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. Table 4.2 reviews the types of information commonly found within an Information infrastructure system.

Table 4.2: The type of information that can be found to be secure in Information infrastructure system

Privacy Data of Individuals	**Corporate Intellectual Property**	**Online B2C and B2B Transactions**	**Government Intellectual Property**
• Name, address, date of birth • PAN number • Bank name, account number • Credit card account number • Utility account number • Mortgage account number • Insurance policy number • Securities and brokerage account number	• Trade secrets • Product development • Sales and marketing strategies • Financial records • Copyrights, patents, etc.	• Online banking • Online health care and insurance claims • E-commerce, e-government, services • Online education and transcripts	• National security • Military and DoD strategies

The components of IT infrastructure are made up of interdependent elements, and the two core groups of components are **Hardware** and **Software**. Hardware uses software—like an operating system—to work. Operating systems also make connections between software applications and physical resources using networking components. The components of Information system infrastructure are defined as below:

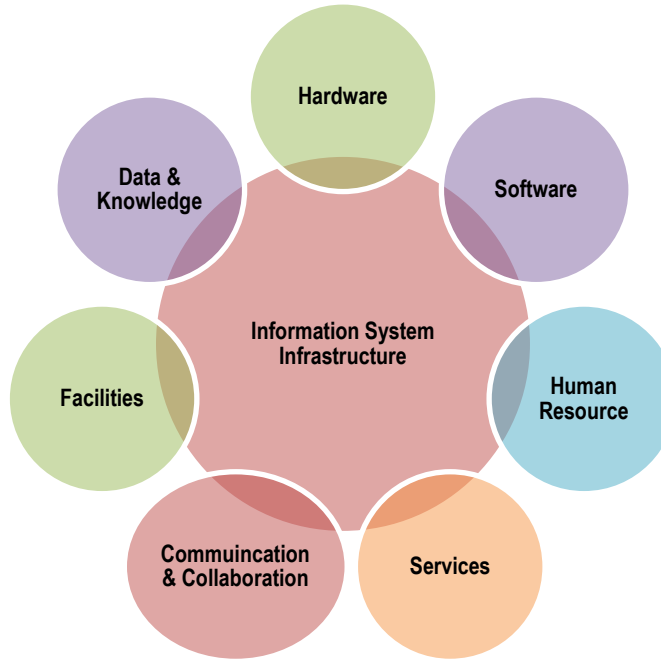


Fig. 4.3: Information System Infrastructure

- **Hardware**
  - Hardware is the tangible portion of our computer systems; something we can touch and see i.e. the physical components of technology.
  - It basically consists of devices that perform the functions of input, processing, data storage and output activities of the computer.
  - Computers, keyboards, hard drives, iPads, and flash drives are all examples of Information Systems' hardware. Hardware components on information system infrastructure include (Refer Fig. 4.4):

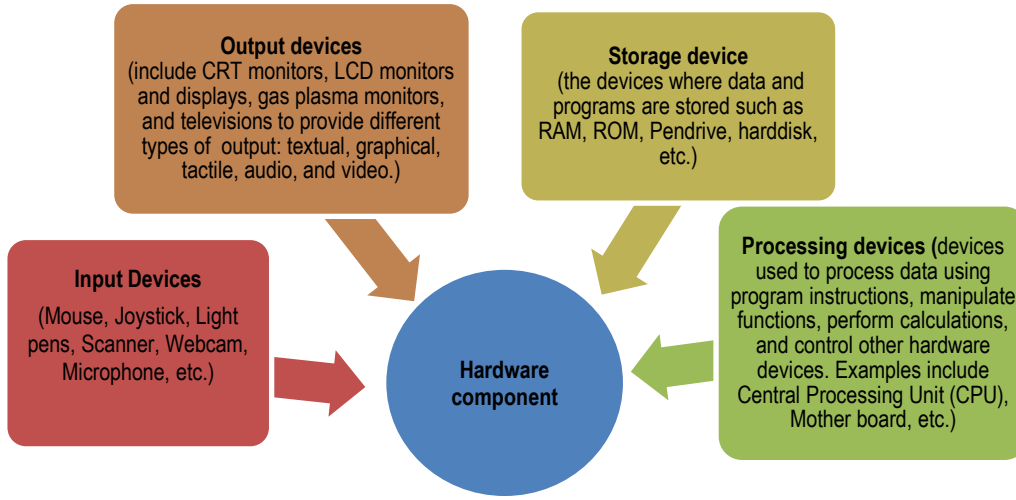


Fig. 4.4: Hardware components

- **Software**
  - Software is defined as a set of instructions that guide the hardware on what tasks to perform. Unlike hardware, software is intangible and cannot be physically touched.
  - Software is created through the process of programming. Without software, the hardware would not be functional. Software components can include:
    - System Software
    - Application Software
- **Facilities**
  - Facilities or physical plants provide space for networking hardware, servers, and data centres.
  - It also includes the network cabling in office buildings to connect components of an IT infrastructure together.
- **Communication and Collaboration**
  - Networks are comprised of switches, routers, hubs, and servers.
  - In today's high-speed world, we cannot imagine an information system without an effective and efficient communication system, which is a valuable resource which helps in good management.
  - Telecommunication networks give an organization the capability to move information rapidly between distant locations and to provide the ability for the employees,

customers, and suppliers to collaborate from anywhere, combined with the capability to bring processing power to the point of the application.

- **Services**
  - In Information system, Infrastructure services are the processes which are not core competencies are often delegated to companies with more experience.
  - Information services of an organization are delivered by an outside firm, by an internal unit, or by a combination of the two.
  - Outsourcing of information services helps with such objectives as cost savings, access to superior personnel, and focusing on core competencies.
  - An information services unit is typically in charge of an organization's information systems.
  - When information services are provided in-house and centralized, this unit is responsible for planning, acquiring, operating, and maintaining information systems for the entire organization.
- **Human Resource**
  - The human resource as the components of the information system may include employees at all levels such as the top management, mid management and low level employee.
  - Human resource includes all those who operate, manage, maintain, and use the system i.e. system administrator, IS personnel, programmers, and end users i.e. the persons, who can use hardware and software for retrieving the desired information.
- **Data and Knowledge**
  - The data, plural of Datum, is the raw fact which is input to the system that may be alphanumeric, text, image, video, audio, and other forms. These are the raw bits and pieces of information with no context that can either be quantitative or qualitative.

Quantitative data can be numeric, that can be generated either by the result of a measurement, count, or some other mathematical calculation.

Qualitative data is descriptive. "Grey silver," the color of a 2019 Wagon R, is an example of qualitative data. By itself, data is not that useful. For it to be useful, it needs to be given context.

Once data is put in the context and it can be aggregated and analyzed to make useful decisions for any organization. Knowledge is the information after processing of the data. Information plus insight becomes knowledge.

4.5 PRINCIPLES OF INFORMATION SECURITY

Every enterprise needs to manage its information in an appropriate and desired manner. For this, an enterprise must know its information needs; acquire that information and organize it in a meaningful way, assure information quality and provide software tools so that users in the enterprise can access the information that they require.

The objective of Information System security is the protection of the interests of those relying on information and protects the information systems and communications that deliver the information from harm resulting from failures of confidentiality, integrity, and availability. Whereas Information security has emerged as a separate discipline with multiple dimensions such as physical security, technical security, operational security, mobile security, application security and behavioral security.

Fig. 4.5 illustrates the three principle of information security. When finding solutions to security issues, the **C-I-A (Confidentiality, Integrity and Availability)** triad can be used. The organization's security baseline goals can be defined using this triad for a typical IT infrastructure. Once defined, these goals will translate into security controls and requirements based on the type of data you are protecting.

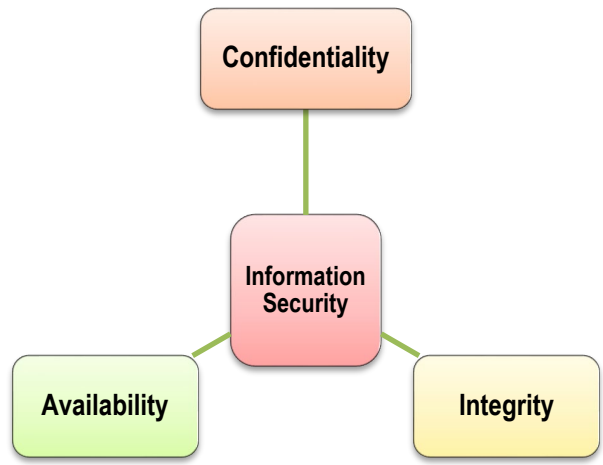


Fig. 4.5: Illustrates the three principle of information security

The information that is secure satisfies three main tenets, or properties, of information. If user can ensure these three principles, s/he satisfies the requirements of secure information. The three principle C-I-A triad are as follows:

- **Confidentiality**— Prevention of the unauthorized disclosure of information i.e. only authorized uses can view information. Confidentiality is a common term which means guarding information from everyone except those with rights to it. Confidential information includes the following:
  - Private data of individuals.
  - Intellectual property of businesses.
  - National security for countries and governments.
- **Integrity**— Prevention of the unauthorized modification of information i.e. only authorized users can change the information.
  - Data without integrity is like data that are not accurate or not valid—it is of no use. Many organizations consider data and information as intellectual property assets.
  - Examples include copyrights, patents, secret formulas, and customer databases. This information can have great value.
  - Unauthorized changes can undermine the value of data. This is why integrity is a fundamental principle of systems security.
- **Availability**— Prevention of the unauthorized withholding of information i.e. information is accessible by authorized users whenever they request the information.
  - Availability is a common term in everyday life. For example, we probably pay attention to the availability of our Internet service, TV service, or cell phone service.
  - In the context of information security, availability is generally expressed as the amount of time users can use a system, application, and data.

4.6 INFORMATION SECURITY POLICY

- Information Security Management (ISM) consists of the set of activities involved in configuring resources in order to meet information security needs of an organization.
- 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, an information security policy is a document that describes an organization's information security controls and activities. The policy does not specify 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 behavior 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.

4.6.1 What type of 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 try 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 be detrimental in the hands of a competitor. Despite many organizations prohibiting the sharing of such data, carelessness often leads to its compromise. This can include the inadvertent storage of data on unauthorized systems, unprotected laptops, and a 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 underprice the market or increase prices. In either case, the damage to an organization may be significant.

4.6.2 What are the issues to address in Information Security?

- 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.

- 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 provide 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.

4.6.3 Components of the Information 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.

4.6.4 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.
  - **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. 4.6.

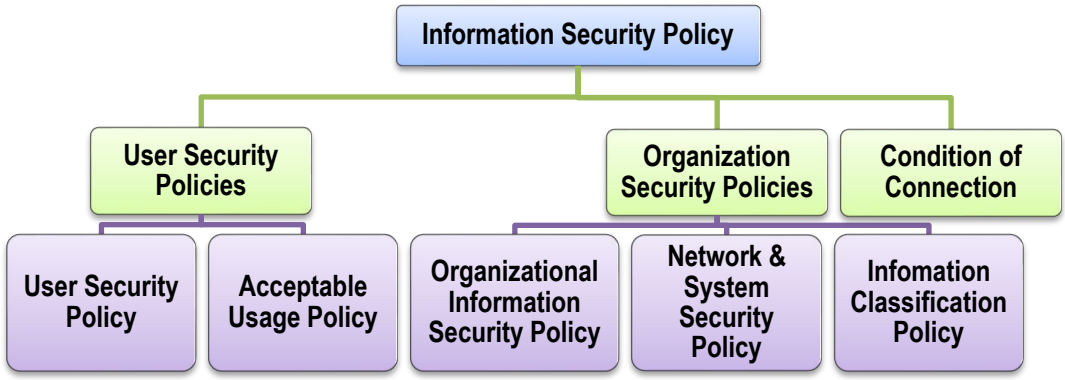


Fig. 4.6: The Hierarchy of Information Security Policies

4.6.5 Tools to Implement Information Security Policy

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. Unless and until we get assurance of user security, cyber security cannot grow. It is the requirement to keep the data private and secure as all businesses run on internet. A security policy framework contains following main components (Table 4.3):

Table 4.3: Components of Security Policy Framework

Standard	Procedure	Guideline
• Standards specify technologies and methodologies to be used to secure systems. • It is a detailed document pertaining definition for hardware and software and how these are to be used. • Standards are compulsory within an organization. Guidelines assist users, systems personnel, and others in effectively securing their systems.	• Procedures are more detailed steps to be followed to accomplish particular security related tasks. • It may comprise of a plan of action, installation, testing, and auditing of security controls. • Procedures normally assist in implementing applicable information security policy.	• Guidelines help in smooth implementation of information security policy. • Guidelines can be specific or flexible regarding use. • 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.

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.

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.

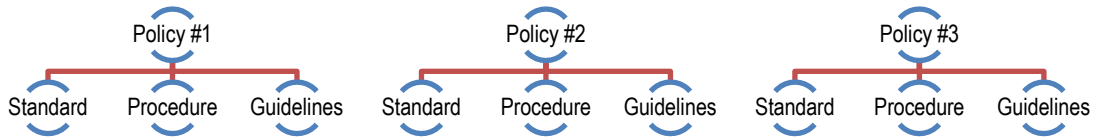


Fig. 4.7: An example of a hierarchical IT security policy framework.

Policies are applicable to an entire organization whereas the standards are specific to a given policy. Each policy along with standard help to define the roles, responsibilities, and accountability of various stakeholders within organization. Policy document should set must set limits as well as refer to standards, procedures, and guidelines.

4.6.6 Monitoring of Information security

When we review our systems, we should check for the following:

- Are security policies comprehensive and appropriate for the business process or activity?
  - The objective of information security is to support vision and mission of the organization and to protect it from various risks. From security point of view, the most visible risks are data breach. The organization's policies and supporting documents should define the risks that affect it.
- "Are our policies understood and followed?"
  - This question comes during audit. Though the audit does not set new policies yet the auditors may make recommendations based on his/her experience or knowledge of new regulations or other requirements.
- Are there implemented controls supporting the policies and culture?

- Are the security controls being in alignment with the organization's strategies and mission?
  - We cannot justify a control by a policy, we may probably remove it. Whenever a control is defined as "for security" with no other explanation, we should remove it. Security is a support department. Its purpose is to protect the organization's assets and revenue stream.
- Is there effective implementation and upkeep of controls?
  - As the organization grows so as the threats, therefore, it is important to make sure that the controls still meet the risks of present.

illustration - Case B

- JK Pvt. Ltd. is an autonomous organization that designs, develops, implements, and maintains IT systems, products and services of one of the major government institutions in India. Governed by Board, the organization has a Managing Director as the top authority.
- Operating with 800 employees, the key functions of the company are to provide IT solutions, manage overall information system, and give IT consulting services to its parent organization. The organization has its headquarters in New Delhi and five regional offices in various cities in India.
- The main functionality of the organization is data and information management and to provide IT support to its parent organization for critical public functions. The survival of the organization is solely dependent upon the proper functioning of its information systems. Thus, information security is essential for the organization.
- The clients of the organization are citizen and the parent government organization. In such case, any deviation in data/information and information system will result in large public outcry. If an internal application of the organization fails, only few users of departments will be affected, but if any of the critical application fails, it will be disastrous for the organization. The two assets that are important for an organization are information and process.

Support of Top Management

- If there is a change in senior executives, there is a varying change in priority regarding information security in the organization.
- For some of the executive, information security is an important aspect, but for others, it is not. However, with the newly created Information Security Officer (ISO) position in the organization, information security has got attention and the Information Security Management activities have started becoming streamlined.

- ISO along with his/her two team members are responsible to manage various Security Management functions of the organization. Now with a push from ISO office, the senior management started realizing the importance of information security and is willing to support its various functions.
- Still, there is a challenge of lack of skilled manpower and funds to support various Security Management functions in the organization.

Information Security Policy

- The Organization has released its information security policy, however, some guidelines related to information security existed earlier. But it was limited in sense and do not cover all aspect of Information security management. Therefore, the security policy was released which had the definition of roles and responsibilities of employees, vendors and third-party contractors with a clause in policy to review it annually. This is the case of compliance issue with information security though comprehensive information security policy is there.

Information Security training to employees

- The organization has definite process to provide information security training to employees.
- There are various internal as well as external information security training programmers for employees.
- Employees are dividing into groups and every group has a representative that coordinates information security activities of the group.
- There are two kinds of training program — general awareness training and specific area related training. The general awareness training is given to each employee whereas the specific training is based on the requirement of job. Experts from industry and other agencies are invited to conduct training sessions, workshops, and seminars.

SUMMARY

- **In illustration - case A,** no information security policy is there in the company therefore no mechanism exits for information security audit. Therefore, it is the responsibility of network team to monitor the log records of the servers and take necessary action in case of any deviations.
- Information security management are ad-hoc and reactive in nature as there is no clear plan for identifying and managing risks to various business operations. The company has no defined information security policy and practices. The company follows a reactive approach towards information security incident management.

- The company uses licensed software and here is no mechanism to check the use of unauthorized software on company systems. Though the top management, managers and other employees of the company acknowledge the fact that information security is a critical aspect of their business, the issue has given very low priority in the company.
- Company in the case A needs a clearly defined disaster recovery and business continuity plan which needs to be discussed with all relevant stakeholders for incident management.

In illustration - Case B, the organization JK Pvt. Ltd. makes an effort to communicate to its employees about risks, threats and counter measures through various training programmes conducted internally as well as outside the organization. Apart from this, organization has a comprehensive information security policy that is been discussed with employees on time to time. All the employees are being educated on their acceptable behaviour towards organization's equipment, network, etc. The main focus of the organization is on creating awareness among its employees on information security. The organization conducted an internal information security audit after based on prescribed guidelines.

- Organization follows layered security architecture, such as logged routers, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), layered firewalls, militarized zones, demilitarized zones, antimalware checks, proxy checks, and antivirus system to protect its network against malicious programmes and cyber-attacks.
- The organization has information security incident management plan defined and documented in the organization's information security policy document, the implementation and compliance of which is dependent upon various application groups. The organization follows a Business Continuity (BC) and Disaster Recovery (DR) plan at its distant geographical location. There is a defined process to take regular data backups which is stored separately off-site.
- The senior management of organization finds the Information security policy effective, as they have not faced any serious security incident yet, except few minor defacement and Distributed Denial of Service (DDoS) attack.
- Organization placed its information security policy and guidelines at its position; however, there is low level of compliance. The management supports the information security policy and has reactive approach most of the time.

This case shows that policy is required at maturity level and moreover, a regular monitoring is essential to improve the level of information security compliance among employees in the organization. It is essential to provide a platform to share the good practices within various teams or groups inside the organization. This helps in peer learning and sharing of best practices across

organization and helps in building a security culture has defined incident management plan and documented information security policy document. However, the implementation and compliance of which is dependent upon various application groups.

The organization should give information security a top priority and top management provides its support to employees. Moreover, a regular monitoring is essential to improve the level of information security compliance among employees in the organization.

As reflected from case A, in absence of any information security policy, there are no clearly defined roles, responsibilities and accountabilities towards company's information and making them prone to information security risks, and threats. Whereas, case B reflects that monitoring compliance to organizational information security policies and guidelines through periodic internal as well as external audits gives confidence to the management and also indicates the areas of improvement.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. An Information Security policy addresses many issues that may involve the following:

   (i) confidentiality, integrity and availability concerns

   (ii) who may access what information and in what manner based on which access decision is made

   (iii) maximized sharing versus least privilege and separation of duties

   (iv) programming new system, maintaining old systems and providing general support software.

   Choose the correct combination of issues addressed under IS Policy.

   (a) (i), (ii), (iii)

   (b) (i), (ii), (iv)

   (c) (ii), (iii), (iv)

   (d) (i), (ii), (iii), (iv)

2. Following are the components of Information System Security except one. Identify

   (a) Firewall

   (b) Mainframe

(c) Application Domain

(d) Personal Data

3. In Information System Infrastructure _____provideS space for networking hardware, servers, and data centers.

(a) Facilities

(b) Software

(c) Hardware

(d) Communication

4. The CIA triad for a typical IT infrastructure of an organization comprises of .....

(a) Confidentiality, Integrity, Availability

(b) Comprise, Integrity, Association

(c) Confidentiality, Important, Availability

(d) Comprise, Integrity, Availability

5. Which Information System Security Policy of sets out the responsibilities and requirements for all IT system users?

(a) Acceptable Usage Policy

(b) User Security Policy

(c) Network & system Security Policy

(d) Information Classification Policy

ANSWERS/SOLUTIONS

1.	(a)	2.	(d)	3.	(a)	4.	(a)	5.	(b)

CHAPTER 5

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- understand the concept of Business Continuity Management (BCM).
- comprehend the key phases in the development of Business Continuity Plan.
- build an understanding of the entire BCM Process.
- grasp the knowledge about various types of plans.
- learn about different types of Back-ups and their working.
- understand the key aspects included in the implementation of Incident Management Plan (IMP).
- identify the areas involved in Disaster Recovery Procedural Plan (DRPP).

CHAPTER OVERVIEW

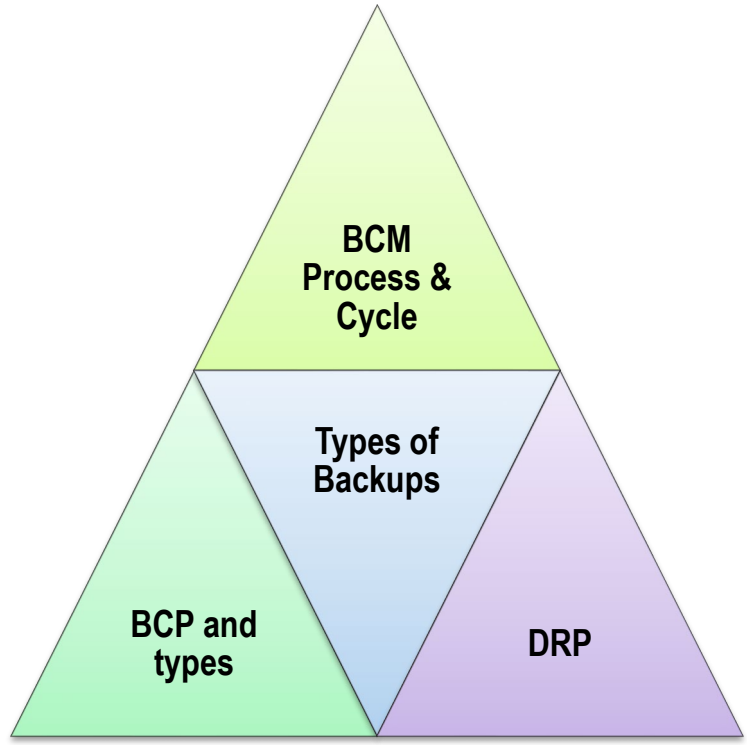


Illustration: Attack on AIIMS Delhi Servers

For years, healthcare organizations have been a top target and remain vulnerable to ransomware attacks. The critical nature of their operations, combined with notoriously lax IT security throughout the industry, are a magnet for ransomware groups looking for big payouts. One such instance is the attack on AIIMs Delhi servers in 2022.

Establishment of AIIMS e-hospital

- In 2016, All-India Institute of Medical Sciences (AIIMS) Delhi had moved to a completely digitized set-up with successful implementation of its e-Hospital project under the government's Digital India Initiative and became the country's first fully digital public hospital.
- A report published in **The Print newspaper** said that the hospital's administration had raised major concerns about data and systems safety and had flagged how lags could have serious repercussions on patient care. It was indicated through reports that the

government department responsible for setting up IT infrastructure had not been strengthened with appropriate systems for upkeep and security. In the absence of database administrator, security administrator, and system administrator at site for the installation, the whole project was at high risk.

Ransomware Attack.

- On 23rd November 2022, the AIIMS Delhi faced a cyber attack paralyzing its servers after which a case of extortion and cyber terrorism was registered by the Intelligence Fusion and Strategic Operations (IFSO) unit of the Delhi Police on 25th November 2022.
- As per the FIR details, the attack on the server of AIIMS Delhi server had originated from China. Of 100 servers (40 physical and 60 virtual), five physical servers were successfully infiltrated by the hackers. Cybercriminals who hacked the digital services of AIIMS and allegedly compromised the data of scores of patients.
- The attack affected five servers and encrypted 1.3 terabytes of data causing operational disruption and non-functionality of critical applications. The attack was analyzed by the Indian Computer Emergency Response Team (CERT-In) and was found to have been caused by improper network segmentation.

Implications of the Attack.

- The personal details of millions of patients in AIIMS Delhi became at risk due to the ransomware attack.
- Internet services at AIIMS were blocked as per the recommendations of the investigating agencies. The servers for AIIMS e-hospital system went down, affecting digital hospital services, including smart lab, billing, report generation, and appointment system. The forerunning AIIMS institute currently manages over 2,500 beds.
- The hospital immediately sought the assistance of the National Informatics Centre (NIC) and the Indian Computer Emergency Response Team (CERT-In) to restore its digital services with the Intelligence Bureau, Central Bureau of Investigation, Ministry of Home Affairs, and the National Investigation Agency also joining in the investigation.
- AIIMS issued a new set of Standard Operating Procedure (SOP) stating that admission, discharge, and transfer of patients will be done manually until the e-hospital system gets back online. The additional staff was deployed to help run diagnostics, labs, and OPD services, however the hospital struggled to cater to patients without unique health IDs and handle patient admissions and discharges.

Why it matters?

- According to a news report, the cyber incident might have exposed the hospital records of around 40 million patients. The exploited AIIMS database might have contained Patient Preference Information (PPIs) of patients and healthcare workers, as well as records on blood donors, ambulances, vaccination, caregivers, and employee login credentials.

The Remedial Actions.

- Most of the functions of e-Hospital applications like patient registration, appointment, admission, discharge etc. could be restored only after two weeks of the cyber-attack.
- All the data of the five physical servers of AIIMS Delhi which were affected could be retrieved from a backup server which was unaffected and restored on new servers.
- Considering the recent cyber-attack on its servers, the AIIMS in Delhi decided to strengthen its e-hospital network and said that it will only be allowed on a dedicated and secure AIIMS LAN/intranet network that will be maintained by its computer facility department.
- CERT-In was mandated to track and monitor cyber security incidents and a "special advisory on security practices to enhance resilience of health sector entities was communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitizing health sector entities regarding latest cybersecurity threats."
- CERT-In issued alerts and advisories regarding the latest cyber threats/vulnerabilities and countermeasures to protect computers and networks, on an ongoing basis. The team also published "India Ransomware Report H1 – 2022" in August 2022, covering the latest tactics and techniques of ransomware attackers and ransomware-specific incident response and mitigation measures.

Some Crucial Lessons to be learnt by AIIMS attack.

- Cyber-attacks have become an increasingly common threat to organizations around the world, and the recent attack on AIIMS highlights the need for organizations to have robust cyber security measures in place to protect their sensitive information.
- The AIIMS attack due to proper network segmentation allowed the threat actors to gain access, leading to the attack. The AIIMS attack is a crucial lesson for organizations about the importance of network segmentation that involves dividing a computer network into different segments or sub-networks to improve security and isolate vulnerabilities.

Because of improper network segmentation, the hackers could gain access to critical servers and data.

- The organizations should conduct regular risk assessments and implement effective network segmentation techniques like firewalls, intrusion detection systems, and network access control, among others to prevent cyber threats.
- Organizations should ensure that all devices and systems are kept up to date with the latest security patches and software updates.
- The attack also underscores the importance of having an Incident Response Plan document in place. This document outlines the steps an organization should take in the event of a cyber-attack, ensuring that organizations respond to any breach in an organized and efficient manner, thereby minimizing damage and downtime.
- Employees shall receive training in cybersecurity to ensure awareness of the latest security threats and readiness to handle them. This training encompasses topics such as phishing, password protection, and data privacy, among others.

5.1 INTRODUCTION

In today's networked society, the scope extends beyond national boundaries, with a heightened reliance on supply chain management that necessitates regulatory compliance, data security, and privacy. Moreover, there is a critical emphasis on enhancing performance and ensuring the continuous availability of services on a 24x7 basis. Meeting their demands in the 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 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.

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.

5.2 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**.
- **Business Continuity Planning (BCP):** It refers to the ability of enterprises to recover from a disaster and continue operations with the 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 an 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.
- **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 the 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 to ensure that the proper procedures will be carried out to ensure the timely restoration of services.

5.2.1 Scope of Business Continuity

The top management of the enterprise plays a crucial role in shaping the scope of the Business Continuity Management (BCM) program. This involves identifying key products and services that align with the enterprise's objectives, obligations, and statutory duties. This process is conducted in accordance with the threat scenario and business impact analysis. In situations involving outsourced services or activities, the enterprise retains risk accountability. It is imperative to establish and implement necessary controls and processes to effectively manage risks associated with outsourced services.

5.2.2 Advantages of Business Continuity Management

The advantages of BCM are that an enterprise:

- is able to proactively assess the threat scenario and potential risks.
- has planned response to disruptions designed to 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.

5.3 BCM POLICY

The main objective of BCP is to minimize or eliminate the loss of 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 to any relevant standards, regulations or policies that must 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 and BCP undergo ongoing testing, revision and updation as required.
- planning and management responsibilities 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.

5.4 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 a 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.

5.4.1 Objectives 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. 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.
- 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.
- reduce the complexity of the recovery effort.

5.4.2 BCP Manual

An incident or disaster affecting critical business operations can strike at any time. 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 regarding the capability of the organization to recover from unexpected incidents or disasters affecting business operations. This includes ensuring the continuity of 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 liasioning teams between the affected functional area(s) 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.
- delivers a proven capability to manage a business disruption and protect the enterprise's reputation and brand.

5.4.3 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 must 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 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.
  - 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.
  - 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 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 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 lead to a denial of access to systems, services and other services and facilities.
- 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 being 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 defining the test purpose/approach; identifying test teams; structuring and 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.

5.5 BUSINESS CONTINUITY MANAGEMENT (BCM) PROCESS

A BCM process should be in place to address the policy and objectives as defined in the BCM policy by providing organization structure with responsibilities and authority, implementation, and maintenance of business continuity management. The management process enables the business continuity, capacity, and capability to be established and maintained. The capacity and capability are established in accordance with the requirements of the enterprise. Refer Fig. 5.1.

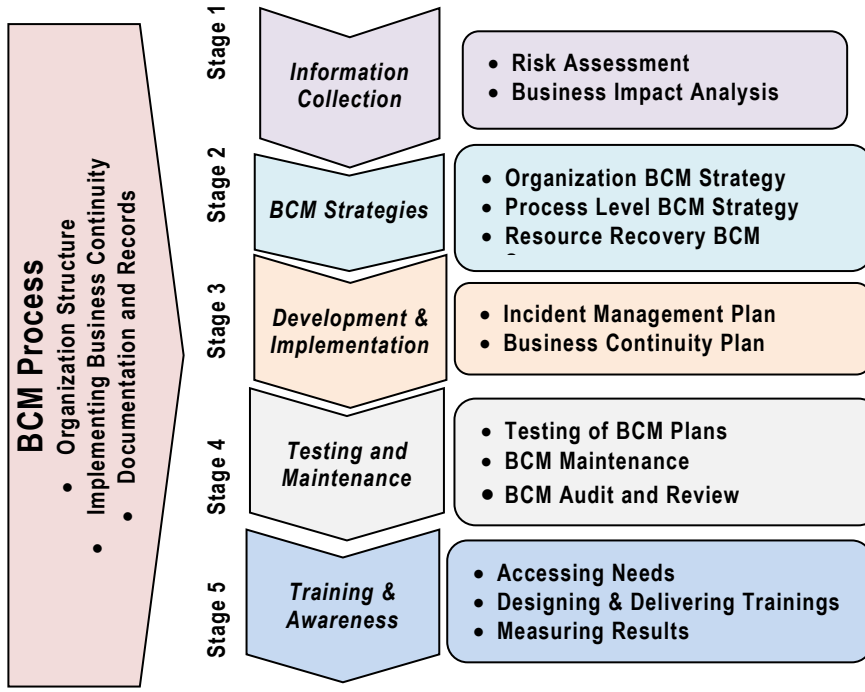


Fig. 5.1: Components of BCM Process

A. **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.

B. **Implementing Business Continuity :** 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 a colleague to

effectively carry out their BCM 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 and context.
- defining roles and responsibilities.
- engaging and involving all stakeholders.
- testing of program on regular basis.
- maintaining the currency and appropriateness of business continuity program.
- reviewing, reworking, and updating the business continuity capability, risk assessments and Business Impact Analysis (BIAs).
- managing costs and benefits associated; and
- convert policies and strategies into action.

C. **BCM Documentation and Records:** All documents that form the BCM are subject to the document control and record control processes. Refer Table 5.1.

Table 5.1: Classified Documents (representative only) being part of the Business Continuity Management System (BCMS)

The Business Continuity Policy	The aims and objectives of each function and the activities undertaken by each function
The BIA Report	The Risk Assessment Report
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	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 references 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, DTP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit.

5.6 BUSINESS CONTINUITY MANAGEMENT (BCM) CYCLE

Refer Fig. 5.2.

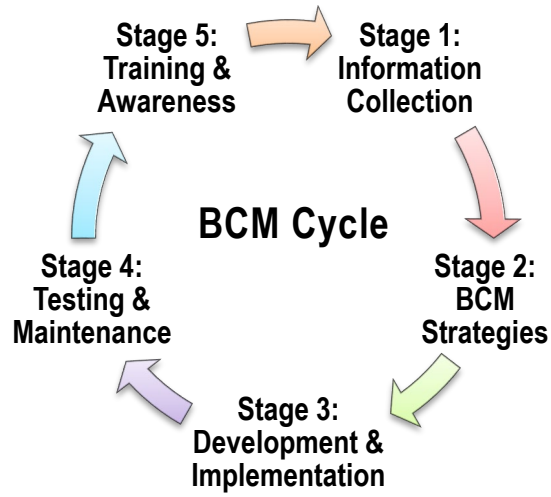


Fig. 5.2: BCM Cycle

Stage 1: 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.

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 involves BIA and Risk Assessment

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 associated risks. This review will ensure that the findings and the decisions made because of the findings are still accurate and relevant to the needs of the operation and its stakeholders.

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 the enterprise's requirements.

Specific threats can be defined as events or actions that have the potential to impact resources. Examples of these threats include, but are not limited to, incidents 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
- 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 the strategies for each critical activity.

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 considers the BIA process.

Stage 2: BCM Strategy

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 consider the processes and technology already present within the enterprise.

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 consider 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.

Stage 3: BCM Development and Implementation

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

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.

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 an 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 incident.

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 as shown in Fig. 5.3.

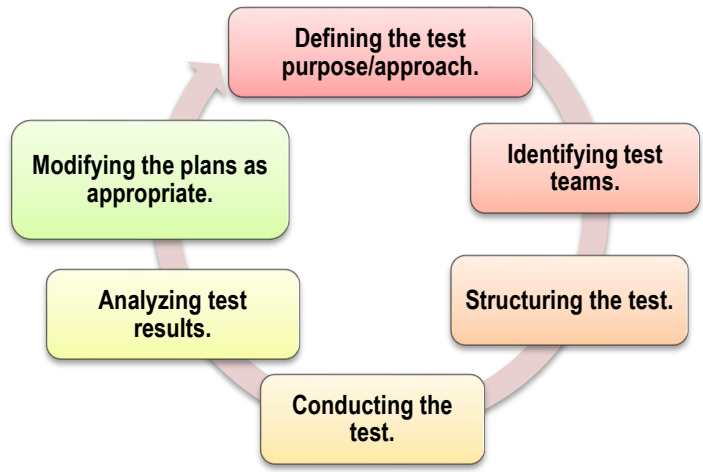


Fig. 5.3: Steps for Implementation

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.

Stage 4: BCM Testing and Maintenance

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.

A BCP must 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, for example - 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.
- 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, considering 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.
- the resources such as business processes, systems, personnel, facilities, and data are obtainable and operational to perform recovery processes.
- the manual recovery procedures and its backup system(s) are current and can either be operational or restored as needed.
- the success or failure of the business continuity training program is monitored.

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 the 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 organizational, 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 and up to date.

Reviewing BCM Arrangements

A 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.
- enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the enterprise's objectives).
- enterprise' BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control, and coordination of an incident.
- enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise.
- 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.
- 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.
- change control processes are in place and operate effectively.

Stage 5: BCM Training and Awareness

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.

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 listen 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.

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.
- 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.
- 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.
- raising awareness.
- skills training.
- exercising plans.

5.7 TYPES OF PLANS

There are various kinds of plans that need to be designed. They include the following:

5.7.1 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.

5.7.2 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.

5.7.3 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.

mcq tha ..same

5.7.4 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.

5.8 TYPES OF BACK-UPS

Backups should be monitored frequently, and logs should be completed supporting such monitoring and successful completion of the backup. For example, each morning an IS operator should be responsible for checking his/her computer to confirm backup completion or identify any error messages displayed by the system that prevented the backup from completion. Additionally, system generated logs should be examined by IS operations personnel to identify files that might not have been backed up by the system. When exceptions to the backup process are identified, the IS operator should attempt to perform restart procedures to resolve them. If the operator is unable to do so, he/she should escalate the problem for resolution.

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:

(i) **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. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed.

It is commonly used as an initial or first backup followed with subsequent incremental or differential backups. After several incremental or differential backups, it is common to start over with a fresh full backup again. Some also like to do full backups for all backup runs typically for smaller folders or projects that do not occupy too much storage space. The Windows operating system lets us to copy a full backup on several DVD disks. Any good backup plan has at least one full backup of a server.

Refer Table 5.2. Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.

Table 5.2: How does Full Backup work?

Day	Activities performed throughout the day	Full Back up at 9:00 pm at night
Monday	100 photos are stored on the system.	An image file of 100 photos is obtained.

Tuesday	Another 100 photos are stored on the system.	An image file of 200 photos is obtained.
Wednesday	Deletion of any 10 photos out of 200 photos is done.	An image file of 100 photos is obtained.
Thursday	No changes done.	An image file of 100 photos is obtained.
Friday	Another 200 photos are stored on the system.	An image file of 300 photos is obtained.
Conclusion	You get five backup files containing 800 photos. Should a data loss incident occur and you need to recover all the photos, simply restore the last version to get all 800 photos.	

Advantages

- Restores are fast and easy to manage as the entire list of files and folders are in one backup set.
- Easy to maintain and restore different versions.

Disadvantages

- Backups can take very long as each file is backed up again every time the full backup is run.
- Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

(ii) **Incremental Backup:** An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

Refer Table 5.3. For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Table 5.3: How does Incremental Backup work?

Day	Activities performed throughout the day	Incremental Back up (At 9:00 pm at night)
Monday	100 photos are stored on the system and perform full backup.	An image file of 100 photos is obtained.
Tuesday	Another 100 photos are stored on the system resulting to 200 photos in total.	On performing incremental backup, an image file of 100 photos is obtained.
Wednesday	No changes are made.	On performing incremental backup, an empty image file is obtained.
Thursday	100 photos are deleted, and another 100 photos are edited.	An image file of only the edited 100 photos is obtained.
Conclusion	You get three image files containing 300 photos in total. In case you need to recover all the photos, restore all the image files since the last full backup, including the last full backup and the later incremental backups, to get 200 photos (including the deleted 100 photos).	

Advantages

- Much faster backups.
- Efficient use of storage space as files is not duplicated. Much less storage space used compared to running full backups and even differential backups.

Disadvantages

- Restores are slower than with a full backup and differential backups.
- Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.

(iii) Differential Backup: Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made 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.

Refer Table 5.4. For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.

Table 5.4: How does Differential Backup work?

Day	Activities performed throughout the day	Differential Back up (At 9:00 pm at night)
Monday	200 photos are stored on the system and perform full backup.	An image file of 200 photos is obtained.
Tuesday	Another 200 photos are stored on the system resulting to 400 photos in total.	On performing differential backup, an image file of newly added 200 photos is obtained.
Wednesday	No changes are made.	On performing differential backup on existing 400 backups, an image file of newly added 200 photos on Tuesday is obtained.
Thursday	100 photos are deleted, and another 100 photos are edited. (Total of 300 photos).	Image files of 100 photos, 200 photos and 300 photos are obtained.
Conclusion	**Recovering 100 photos:** Both deletion and editing happen to the added 200 photos. The differential backup will back up the edited 100 photos. **Recovering 200 photos:** If you delete 100 photos from the added photos and edit 100 photos from the original photos, the differential backup will back up the edited 100 photos and the 100 added photos (left after deletion). **Recovering 300 photos:** The differential backup will back up the edited 100 photos and the added 200 photos. **When should you use differential backup?** Small and medium-sized organizations that want to process large volumes of valuable data but cannot perform constant backups will find the differential backup method useful.	

Advantages

- Much faster backups than full backups.
- More efficient use of storage space than full backups since only files changed since the last full backup will be copied on each differential backup run.
- Faster restores than incremental backups.

Disadvantages

- Backups are slower than incremental backups.
- Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.
- Restores are slower than with full backups.
- Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.

Refer Table 5.5 for Quick comparison between Full, Differential and Incremental Backups.

Table 5.5: Full vs Incremental vs Differential Backup: Quick Comparison

	FULL	INCREMENTAL	DIFFERENTIAL
Description	Copies the entire Data set	Full Backup + Changes since the previous Backup	Full Backup + Changes since the Full Backup
Backup time	Time-Consuming	Fast to Back Up	Faster than a Full Backup but slower than an Incremental
Recovery time	Fast recovery	Slow recovery	Faster than Incremental but slower than Full Backup
Storage space	Requires lot of storage space	Requires less storage space	Requires less storage space than a Full Backup, but more than an Incremental
Bandwidth	Uses a lot of Bandwidth	Uses less Bandwidth	Uses less Bandwidth than a Full Backup, but more than an Incremental Backup

(iv) **Mirror Backup:** Mirror backups are, as the name suggests, a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually

also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup.

Indeed, a mirror backup is essentially identical to a full backup, differing only in the fact that the files are not compressed into zip files, and there is no option to protect them with a password. The primary purpose of a mirror backup is to generate an exact and uncompressed replica of the backup data.

For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive. Many backup software utilities do provide support for mirror backups.

Advantages

- The backup is clean and does not contain old and obsolete files.

Disadvantages

- There is a chance that files in the source deleted accidentally, by sabotage or through a virus may also be deleted from the backup mirror.

(v) **Cloud Backup:** Cloud backups may offer the perfect and ideal scenario for the future organization. With a cloud backup, files are available everywhere and are no longer dependent on any single computer or server, thereby allowing a quick and smooth restoring of the data in the event of a disaster.

Advantages

- Saves money on storage costs, and the ability to back up more frequently as well as enjoy off-site, redundant storage of critical data.
- Organizations can outsource cloud backup services from third-party entities that specialize in data backup and protection.

Disadvantages

- Speed plays a major role while information is being copied and stored by service provider and the entire process may slow down as per new speed.
- As the service is pay-per-usages basis, the cloud backup can be hafty for organization with enormous data.

5.9 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;
- determine the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- Establishing the priority assigned 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.

5.10 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 that outlines how and when the plan will be tested, as well as the process for ongoing maintenance 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 and 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.

SUMMARY

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 24x7 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.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. ABC Ltd. carries out Fire drills in its company every 6 months whereby fire like situation is simulated and the preparedness of the organization and its personnel for facing disaster is verified. Under Business Continuity Management, which type of plan does this refer to?

   (a) Emergency Plan

   (b) Test Plan

   (c) Back-up Plan

   (d) Recovery Plan

2. Which of the following documents is not classified as being part of the Business Continuity Management System?

   (a) The Risk Assessment Report

   (b) Incident Log

   (c) Local Authority Risk Register

   (d) Performance Analysis Report

3. Which of the following does not form part of the Business Continuity Management (BCM) cycle?

   (a) Information Collection

   (b) Development and Implementation

   (c) Testing and Review

   (d) Recruiting

4. Which of the following statements is incorrect?

   (a) A Full Backup captures all files on the disk or within the folder selected for backup.

   (b) The Mirror backup is clean and does not contain old and obsolete files.

   (c) With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.

(d) Incremental Backup consumes the most storage space as compared to full and differential backups.

5. ABC Ltd. has installed LHJ Backup system whereby the data is backed up almost every second from the live environment to the backup drive. Which type of back-up ABC Ltd. has implemented?

(a) Full Backup

(b) Incremental Backup

(c) Differential Backup

(d) Mirror backup

ANSWERS/SOLUTIONS

1.	**(b)**	**2.**	**(d)**	**3.**	**(d)**	**4.**	**(d)**	**5.**	**(d)**

UNIT – II

INFORMATION SYSTEMS LIFE CYCLE

CHAPTER 6

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- understand the need for a System Development Life Cycle.
- conceptualize the generic phases and associated activities of SDLC.
- understand the importance of testing, implementation, and maintenance of Information Systems.

CHAPTER OVERVIEW

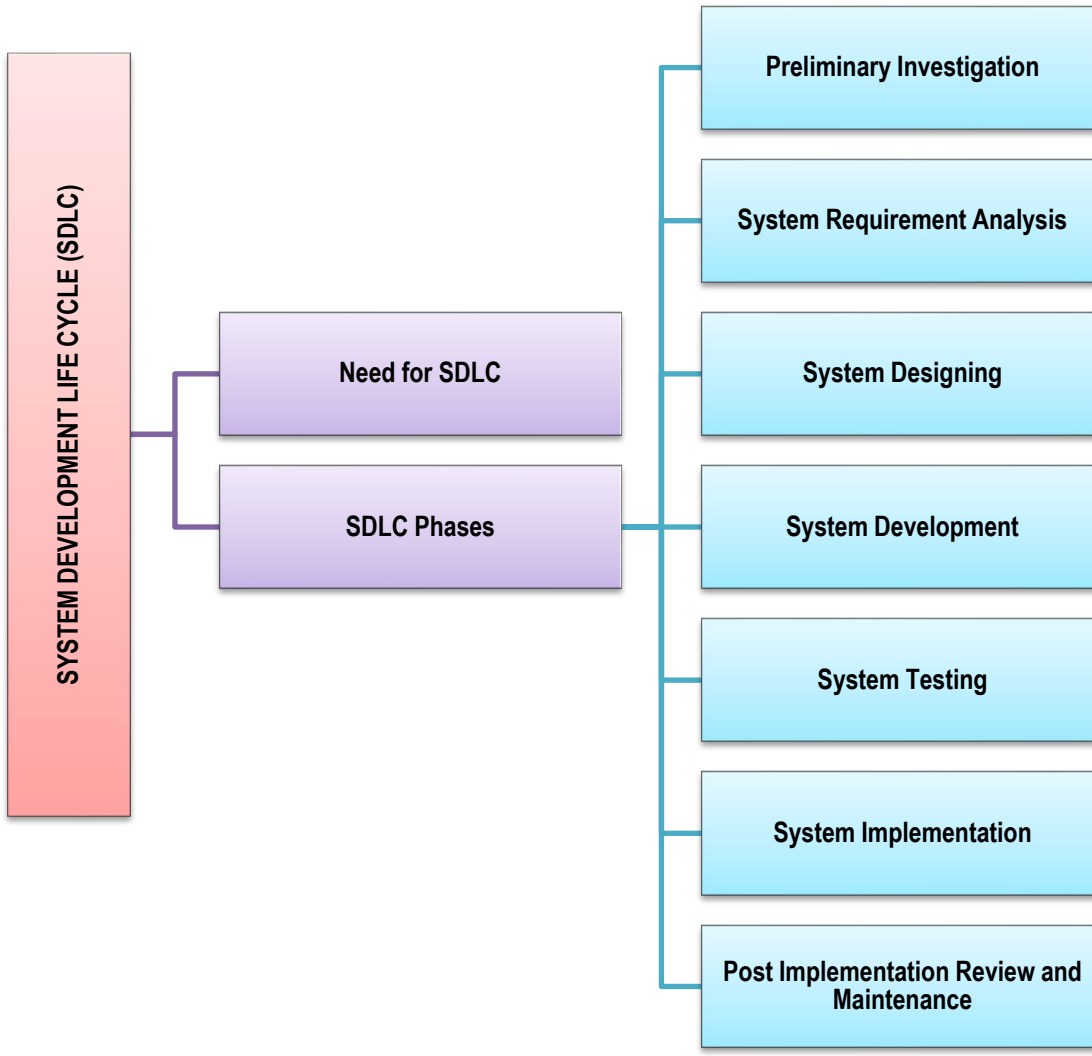


Illustration – Startup for Kid's Apparel

"Delivering the Best" is a new startup owned by four friends as an online e-commerce portal for for kids' apparel. The startup is in the process of developing the web portal that may use the steps for the software development life cycle. The case will represent the practical application of the software development life cycle process.

At the very first step, the Business Analyst/Project Manager collected the details from various stakeholders to know their requirements regarding how the e-Commerce platform will work and

its required features. A detailed Software Requirement Specifications (SRS) of software was prepared then reviewed by the key policymakers and stakeholders.

After this, the SRS document was given to the software development team. The development team carefully reviewed of the SRS document to clearly understand the client's requirements. Accordingly, a well-suited design and architecture of webpages was developed by the development team duly approved by stakeholders.

The development team wrote the coding for various web pages and added API for various functionalities. Once the coding was done, the testing team took over to perform end to end testing to ensure the website worked seamlessly without any bugs. Once the stakeholders approved the platform, it became ready to be deployed. The final version of the e-commerce portal was deployed; however, a similar process was followed to integrate the latest features.

All phases of the Software Development Life Cycle were being used in this case. The startup team knew the criteria for choosing the SDLC which added value to their operations. After considering the SDLC methodology, the requirements of stakeholders, technical capabilities, and constraints of the web portal came into the picture.

It also helped to analyze the suitability of the chosen model of software development w.r.t team's size and their skills, the technology that is going to be used to develop the software. It became helpful to make necessary adjustments that cope with the changes required during the execution of the project.

6.1 INTRODUCTION

The **System Development Life Cycle (SDLC)** provides a sequence of activities for system designers and developers to follow. It consists of a generic sequence of steps or phases in which each phase of the SDLC uses the results of the previous one. SDLC involves acquiring or developing and maintaining application systems that are used in routine business processes. The SDLC is document driven, which means that at crucial stages, the processes documentation is produced.

Every hardware or software system undergoes a thorough development process which can be thought of as an iterative process with multiple steps. SDLC is used to give a rigid structure and framework to define the phases and steps involved in the development of a system.

Barry Boehm suggested the principle of W5HH that talks about the objectives of system, milestone, schedule, responsibility, management, and technical approaches and required resources. The principle outlines a series of questions that can help project managers more efficiently manage

software projects. Each letter in W5HH stands for a question in the series of questions to help a project manager lead as given in Table 6.1.

Table 6.1: W5HH Principle

i. **Why** is the system being developed? ii. **What** will be done? iii. **When** will be done? iv. **Who** is responsible for a function? v. **Where** are they located organizationally?	i. **How** will the job be done technically and managerially? ii. **How** much of each resource is needed?

This principle is applicable to every SDLC regardless of the size and complexity of the system. 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.

6.2 NEED FOR SDLC

There are certain situations that may arises the need for the development or acquisition of a new system, which are explained below:

- If there exists a new service delivery opportunity that relates to a new or existing business processes.
- If there persists an issue or problem with the existing system or business activities.
- If strategic management changes its focus, leading to an opportunity that may provide benefits to the organization. This can be the merger or acquisition of new companies or the starting of a new service delivery channel. For example - opening new ATMs in the case of banks.
- In case organizations get new opportunities due to advancement in their existing technology or replacement of their existing technology with a newer one.
- If the competitors of the organization are using automation to enhance the quality of service.

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 redesign of an existing system. The advantages of this system are as follows:

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

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.

6.3 SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

The process of system development starts when management or sometimes system development personnel realize that a particular business system needs improvement. Refer Fig. 6.1. The System Development Life Cycle (SDLC) method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system. In most business situations, these activities are closely related, usually inseparable and even the order of the steps in these activities may be difficult to determine.

mcq aaya tha..

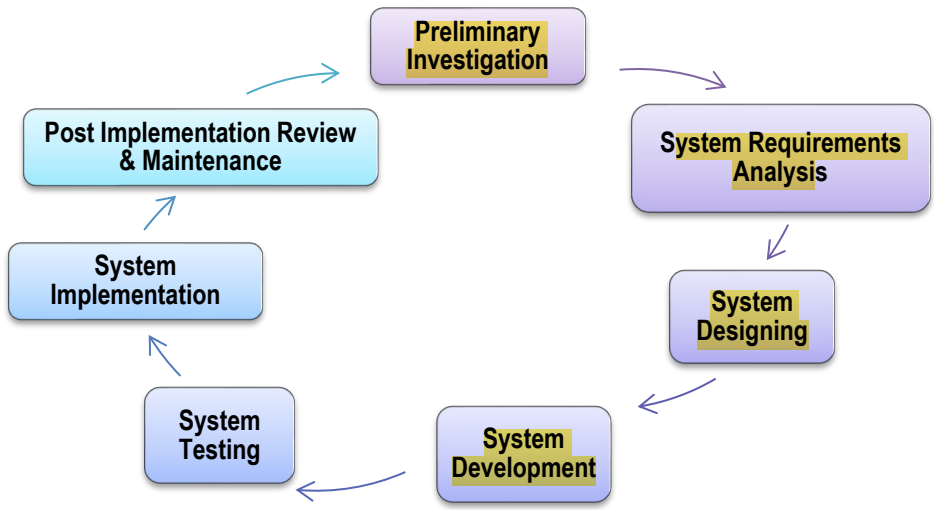


Fig. 6.1: The SDLC Phases

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.

6.3.1 Preliminary Investigation

A **preliminary investigation** is normally initiated by some sort of system request. 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 the morale of employees.

The deliverable of the preliminary investigation includes a report including feasibility study observations. The steps involved in the preliminary investigation phase are given in Fig. 6.2.

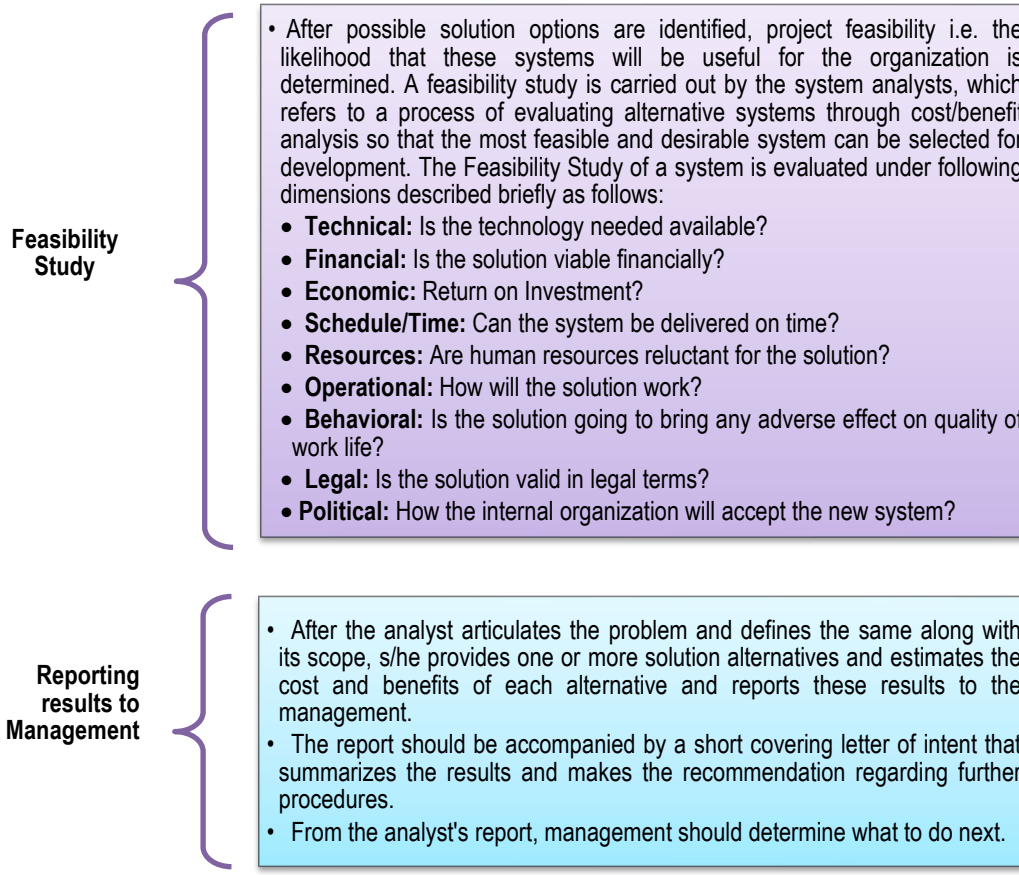


Fig. 6.2: Steps Involved in Preliminary Investigation

6.3.2 System Requirements Analysis

This phase includes a thorough and detailed understanding of the current system, identification of the areas that need modification to solve the problem, the determination of user/managerial requirements and have fair idea about various systems development tools. It assesses the needs of end users and ensures that the newly developed system would fulfill all the requirements of end users. This phase also identifies and documents resources that will be responsible for individual pieces of the system, as well as the timeline expected. The following objectives are performed in this phase to generate the deliverable **Systems Requirements Specification (SRS)**:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts.
- To analyze requirements to detect and correct conflicts and determine priorities.
- To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, and 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, etc.
- To document activities such as interviews, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

To accomplish these objectives, a series of steps are taken that result in process, assuring appropriate systems requirements analysis. A generic set of process is 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 benefit from the system to determine 'what are their actual requirements'.
- Various fact-finding techniques and tools such as documents, questionnaires, interviews, and observations are used by the system analyst to determine these needs/requirements.

(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. The areas including reviewing historical aspects; surveying existing methods; analyzing inputs, reviewing data files, methods, procedures, and data communications; analyzing outputs; reviewing internal controls, modeling the existing system and undertaking overall analysis of the existing system should be intensive to fully understand the present system and its related problems.

(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 shortcomings of the present system. The required systems specifications should be in conformity with the project's objectives articulated and in accordance with the output. After outputs have been determined, it is possible to infer what inputs, databases, methods, procedures, and data communications must be employed.

(iv) **System Development Tools:** Various tools like Structured English, Flowcharts, Data Flow Diagrams, Decision trees and Decision tables, CASE Tools and System Components Matrix etc. are used to help end users and systems analysts in the following areas:

- 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.
- To propose and design new or improved information systems to solve business problems or pursue business opportunities that have been identified.

(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 the development team.

6.3.3 System Designing

After the completion of the 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. This phase describes in detail the specification, features, and operations that will meet the requirement previously defined. 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 guide 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 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 are described briefly in Table 6.2 and the valuable consideration points that are valid for both acquisition of hardware and software are given in Fig. 6.3.

Table 6.2: Design phase activities

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.
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 the objective of the new system; all these have been identified in the analysis phase and documented in Systems Requirements Specification (SRS). In case of failure to produce a high quality design for data/information flow, can seriously undermine a system. For example - Poor timing decisions may result in the capturing of out-of-date data and poor choices about information flows could result in the information being directed to wrong decision makers.
Design of Database	The design of the database involves determining its scope ranging from local to global structure. The scope is decided based on interdependence among organizational units.
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 devices.
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. Some of the issues addressed here are the type of hardware for the 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.
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. 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

	other, subsequent changes will have to be made and resources expended in trying to make the hardware and software compatible with each other.
Internal Design Controls	From an internal control point of view, this phase is also important as all internal controls are placed in the system during this phase. The key control aspects at this stage include the following: • Whether all control aspects have been properly covered? • Whether controls put in place in the system appear in the documentation done at this stage? • Whether a separate review of the design document has been done by the internal auditor?

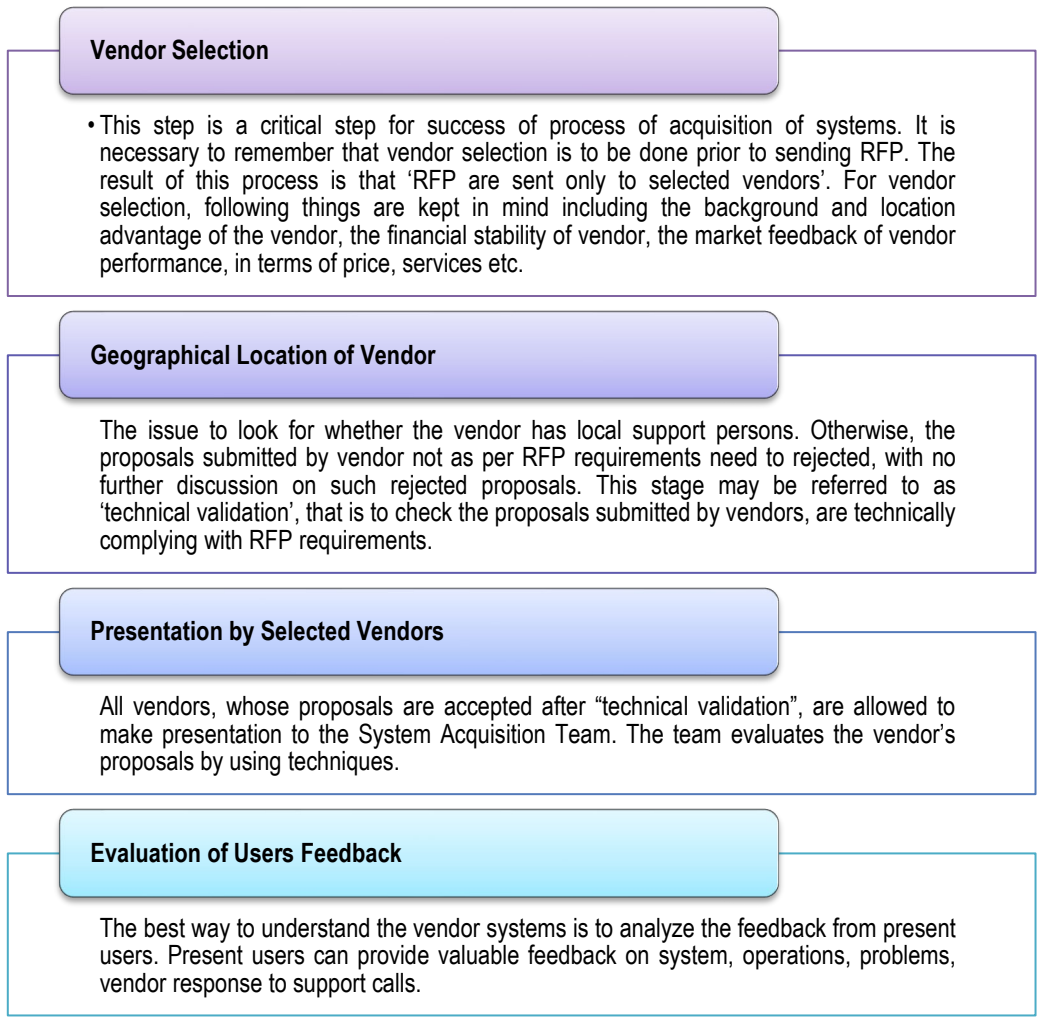


Fig. 6.3: Considerations are valid for both acquisition of Hardware and software.

6.3.4 System Development

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, and conduct system testing. Finally, it results in 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.

mcq .. same qusn tha

- **Robustness:** It refers to the application's strength to uphold its operations in adverse situations by considering all possible inputs and outputs of a program in case of least likely situations.

- **Accuracy:** It refers not only to 'what the 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 by 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 a 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 using any language that has specific rules concerning format and syntax. Syntax means vocabulary, punctuation, and grammatical rules available in the language manuals that the programmer must follow strictly and pedantically. Different programmers may write a program using different sets of instructions but each gives the same results. Therefore, 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 Languages:** 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 High-level general-purpose programming languages such as COBOL and C; Object oriented languages such as C++, JAVA etc.; Scripting languages such as JAVA Script, 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 based on 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 the following four steps shown in Fig. 6.4.

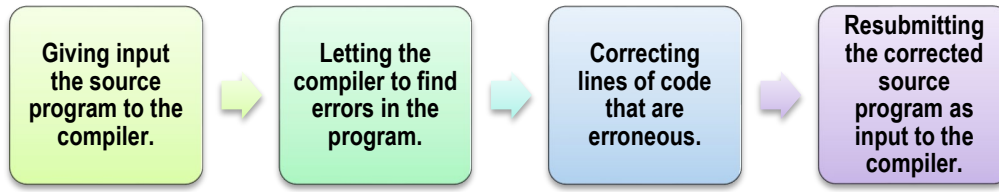


Fig. 6.4: Debugging Process

(d) **Testing the Programs:** 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 the 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 to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. User documentation should also be reviewed for understandability i.e. the documentation should be prepared in such a way that the user can clearly understand the instructions.

(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.

6.3.5 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 effort. The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defects, 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.

(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 to evaluate the validity of the connection of two or more components that pass information from one area to another. Integration testing takes as its input the 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.

(iii) **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. 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.

(iv) **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.

(v) **Final Acceptance Testing:** This 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 (QAT) and User Acceptance Testing (UAT). QAT ensures that new system satisfies prescribed quality standards and UAT ensures that functional aspects expected by users have been well addressed in new system.

It is important to document each test script, its results, and versioning them based on a number of iterations run for the test to pass. Documenting test scripts and running them through the users before Final Acceptance Testing can help them determine if all functional areas and scenarios have been covered or if they need to add more themselves.

6.3.6 System Implementation

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. 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**. Some generic key activities involved in System Implementation include the following shown in Fig. 6.5:

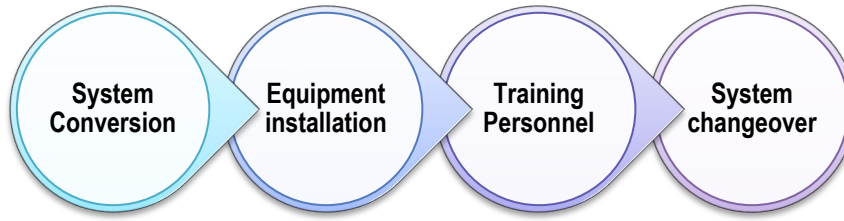


Fig. 6.5: Generic Key Activities involved in System Implementation

Implementation includes all those activities that take place to convert from the old system to the new one. 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 the system implementation stage are described briefly as follows:

(i) System Conversion (Refer Table 6.3)

Table 6.3: Technical activities involved in System Conversion

Procedure Conversion	File Conversion	System Conversion	Scheduling Personnel & Equipment
Operating procedures should be carefully completed with sufficient 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.	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 online files (common database) or offline files. 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 backup. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.	After online 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 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 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 the next period/month should provide sufficient computer time to handle all required processing.

(ii) **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 the 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 not experienced in the installation of the same or similar equipment, adequate time should be scheduled to allow the completion of the following activities:

- **Site Preparation:** An appropriate location/ambience as prescribed and the typical equipment must be used 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 are in actual working conditions.

(iii) **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 the 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 vendors, and through hands-on learning techniques. Such training structure should be highly formalized and be based on business process executions with actual data.

(iv) **System Change-Over Strategies:** Conversion or changeover is the process of changing over or shifting over from the old system (maybe a 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 system change-over strategies are described in the Table 6.4:

Table 6.4: Popular System Change-over Strategies

Direct Implementation / Abrupt Change-Over	Phased Changeover	Pilot Changeover mcq tha	Parallel Changeover
With this strategy, the changeover is done in one operation, completely replacing the old system in one go. The Direct Implementation 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.	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.	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.	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 systems are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and the new system carries on as the only system.

6.3.7 Post-Implementation Review and Maintenance

To assess, review and ensure a 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, the scope of further improvements etc. may be prepared. Such aspects may also be availed in the form of responses to the 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?" This ascertains the degree of success of 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 sometime 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 systems 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:

Table 6.5: Various Types of Evaluation

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 a record of actual performance and cost be maintained.	**Operational Evaluation:** The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable of performing their duties. It tries to answer questions related to functional aspects of the system. Such an evaluation is relatively straightforward if evaluation criteria are established in advance.	**Information Evaluation:** An information system should also be evaluated in terms of the information it provides or generates. This aspect of system evaluation is difficult, and it cannot be conducted quantitatively, as is the case with development and operational evaluations.

(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 (Refer Fig. 6.6):

Scheduled Maintenance	• It 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	• It refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have a 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.
Adaptive Maintenance	• It 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 rules, government policies and work patterns. The need for adaptive maintenance can only be recognized by monitoring the environment.
Perfective Maintenance	• It 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	• It concerns the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

Fig. 6.6: Various types of Maintenance

6.4 OPERATION MANUALS

It is a typical user's guide also commonly known as Operations Manual. Moreover, it may be a technical communication document intended to assist people using a particular 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 associated with electronic goods, computer hardware, and software. The section of an operation manual may include a cover page, a title page, and a copyright page; a preface, containing details of related documents and information on how to navigate the user guide; an index 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; FAQ (Frequently Asked Questions); glossary and, for larger documents, contact list in case of any assistance required etc.

SUMMARY

The objective of the chapter is to describe the key phases involved during the system development process. An effective System Development Life Cycle (SDLC) should result in a high-quality system that meets customer expectations, reaches completion within time and cost evaluations, and works effectively and efficiently in the current and planned Information Technology infrastructure. The System Development Life Cycle (SDLC) is a conceptual model that includes policies and procedures for developing or altering systems throughout their life cycles. SDLC is used by analysts to develop an information system. A detailed discussion of the System Development Life Cycle (SDLC) is provided in the chapter. Accordingly, various stages for the development of the system development life cycle have been discussed.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Which of the following phase of System Development Life Cycle (SDLC) involves the determination of user needs of the Proposed System?

   (a) System Analysis

   (b) System Planning

   (c) System Designing

   (d) System Implementation

2. The following are definitions of various Feasibility Study used in System Development Life Cycle.

   I. Is the solution viable financially?

   II. Does the project provide Return on Investment?

   III. How will the solution work?

   IV. Is the solution permissible?

   The term used for various dimensions of feasibility study is given below:

   A. Legal Feasibility

   B. Operational Feasibility

   C. Economic Feasibility

   D. Financial Feasibility

   Choose the correct option from the following that determine the correct match.

   (a) I-D, II-C, III-B, IV-A

   (b) I-C, II-B, III-A, IV-D

   (c) I-C, II-D, III-B, IV-A

   (d) I-A, II-C, III-D, IV-B

3. In an organization, as most of the Information Systems require some modification after development, the System Maintenance phase becomes one of the important aspects of SDLC. There are different categories of Maintenance which are Scheduled, Adaptive, Corrective, Rescue, Preventive and Perfective. Which of the following statements is not correct about these categories of Maintenance?

   (a) Scheduled Maintenance is planned to ensure operational continuity and avoidance of anticipated risks.

   (b) Rescue Maintenance deals with undetected malfunctions that require immediate troubleshooting solution.

   (c) Adaptive Maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system.

   (d) Corrective Maintenance deals with fixing bugs in the code or defects found during the executions.

4. ABC Ltd. is proposing to introduce the Fitness awareness amongst its employees by gifting FitBit gadget to all employees and then given targets for personal fitness. The Management wants to evaluate the Feasibility of this initiative. Which dimension is tested here?

   (a) Technical Feasibility

   (b) Economic Feasibility

   (c) Operational Feasibility

   (d) Behavioral Feasibility

5. Following are the different types of testing done during System Testing phase of Systems Development Life Cycle (SDLC).

   (A) Regression Testing

   (B) Integration Testing

   (C) System Testing

   (D) Unit Testing

   The activities carried out under these Testing types are mentioned below:

   (i) An activity of software testing in which individual software modules are combined and tested as a group.

(ii) A process in which software and other system elements are tested as a whole.

(iii) Ensures that changes or corrections in the software have not introduced new faults.

(iv) To test if individual units of source code are fit for use.

Pick the correct match:

(a) (A) - (i), (B) - (ii), (C) - (iii), (D) – (iv)

(b) (A) - (iii), (B) - (i), (C) - (ii), (D) – (iv)

(c) (A) - (i), (B) - (iv), (C) - (ii), (D) – (iii)

(d) (A) - (iv), (B) - (ii), (C) - (i), (D) – (iii)

ANSWERS/SOLUTIONS

1.	**(a)**	**2.**	**(a)**	**3.**	**(c)**	**4.**	**(b)**	**5.**	**(b)**

CHAPTER 7

SYSTEM ACQUISITION AND DEVELOPMENT METHODOLOGIES

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- conceptualize a systematic approach to System Acquisition and review its phase-wise activities, methods, tools, controls, etc.
- understand software procurement, acquisition from external sources, evaluation of IT proposals, etc.
- analyze the current system in view of understanding requirements.
- compare different SDLC models and be able to select the most appropriate model best suited for a particular project.
- know the advantages and disadvantages of various system development models.

CHAPTER OVERVIEW

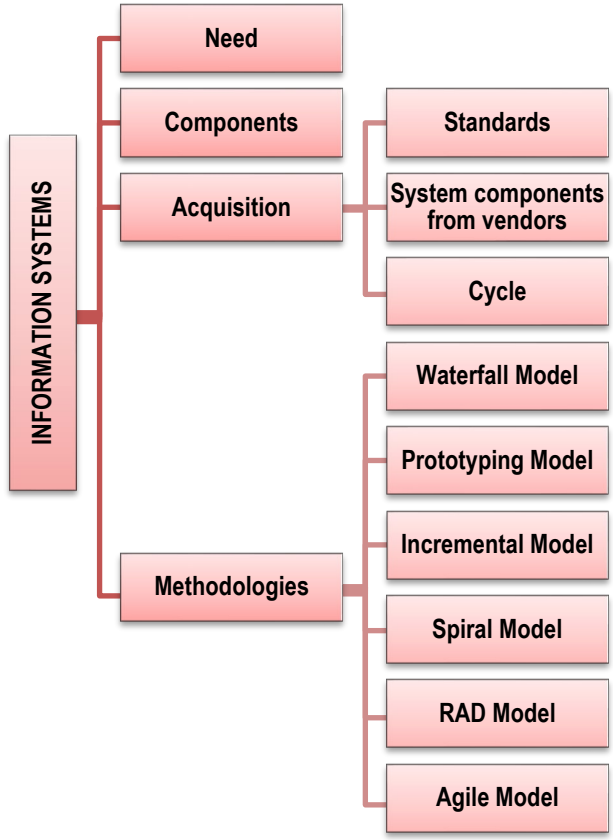


Illustration- Online Ticketing System

Introduction

Mr. Amit waited at the booking window at the PVR, New Delhi. He had reserved center seating tickets for himself and his wife for this concert fifteen days ago and for some reason the box office couldn't find his reservation and sold his tickets to another person. The PVR screen was full and there were no tickets left. That was very disappointing, as he and his wife had been looking to this for a long time as a part of celebration of their 15th wedding anniversary.

The Box Office Manager apologized to Mr. Amit saying that he wrote down his reservation on the phone list, but evidently it somehow wasn't transferred to their master seating chart. However, he arranged two tickets for Mr. Amit and his wife.

Later, Mr. Amit thought of developing an information system to automate the ticketing process as being done manually in the current situation. He fixed a meeting with the PVR manager at the weekend to understand the processes involved and information he required to develop the system.

Later that week Mr. Amit met with the Box Office Manager to develop an overall understanding of their business processes of booking tickets especially for a concert/event, the information they maintain, and the reporting needed. Mr. Amit compiled this information and the detailed requirements are listed below.

Requirements for Systems Analysis and Design

1. Prepare a system proposal that includes an executive summary, the requirements of the system, and identification of the team members.
2. Develop appropriate process models (Use Case Descriptions/Diagrams or Data Flow Diagrams – context level, level 0, level 1) per instructions.
3. Develop the appropriate data model (Class Diagram or Entity-Relationship Diagram) per instructions.
4. Develop preliminary screen and report designs for each user interface identified.
5. Prepare a one-page "pre-implementation review" outlining lessons learned - what went right and what went wrong on this project.

Mr. Amit explained his team that a database system is to be developed which would maintain information about each event and tickets sold, and the patron to whom the tickets are sold. The system should also generate reports on the number of tickets sold/available per performance, and tickets purchased by a specific patron.

After gathering the detailed requirements for the system, Mr. Amit began developing data and process models and designing the user interfaces. He developed an efficient online ticketing system for PVR to keep track of each event and ticket sales much more efficiently.

Requirements for Systems Development

1. Complete the above requirements.
2. Using appropriate development tools, develop a comprehensive, user-friendly, working system that will meet the requirements of PVR.
3. Prepare a user manual describing how to use the system.
4. Prepare a one-page "post-implementation review" outlining lessons learned – what went right and what went wrong on this project.

7.1 INTRODUCTION

Over the past few years, the world has moved on from a connection amongst individuals to more of a connection amongst systems. We now have systems that are constantly exchanging information about various things and even about us, many times without human intervention. This inter-networking of physical devices, vehicles, smart devices, embedded electronics, software, sensors or any such device is often referred to as IoT (Internet of Things).

What is interesting about various emerging technologies is that at their core we have some key elements, namely, People, Computer Systems (Hardware, Operating System and other Software), Data Resources, Networking and Communication Systems. In this chapter, we are going to explore each of those key elements.

Information System is used in almost every imaginable profession. **Information System (IS)** is a combination of people, hardware, software, communication devices, network and data resources that process (can be storing, retrieving, transforming information) data and information for a specific purpose. These interrelated components collect (input), manipulate (process), store and disseminate (output) data and information and provide a feedback mechanism to meet an objective (Refer Fig 7.1). The feedback system helps businesses, entrepreneurs, and organizations achieve their goals, such as increasing profits or improving customer service.

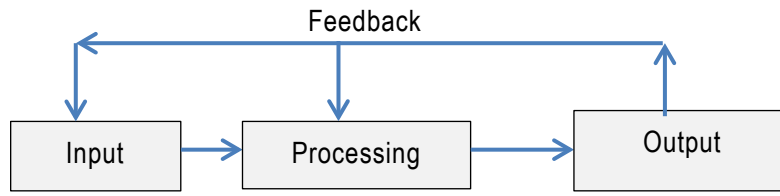


Fig. 7.1: Components of Information System

The system needs inputs from the user (key in instructions and commands, typing, scanning) which will then be processed (calculating, reporting) using technology devices such as computers, and produces output (printing reports, displaying results) that will be sent to another user or other system via a network and a feedback method that controls the operation.

Need of Information System in an organization

Information is the power and information system is used in every sector and profession. Through this system, entrepreneurs and businesses can reach their customers, advertise their projects, manage their employees, communicate with all stakeholders etc. Even for individuals, information system is an indispensable tool that helps them to achieve their goals.

7.2 INFORMATION SYSTEM ACQUISITION

After a system is designed either partially or fully, the next phase of the system development starts, which relates to the acquisition of operating infrastructure including hardware, software, 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 are 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 the 'System Acquisition Committee' is constituted. The sub-committee is mandated to ensure timely and effective completion of this stage.

The next aspect is a 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. The RFP process is the initiation of the final stages for implementation. The requirements analysis and design phase have been completed, before starting this phase. The following considerations as given in Fig. 7.2 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 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.

Fig. 7.2: Considerations are valid for both acquisition of Hardware and Software

Besides these, some specific considerations for hardware and software acquisition are described as follows:

- The benchmark tests to be done for the proposed machine. For hardware, there are specified standard benchmark tests defined based on the nature of hardware. These need to be applied to the 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 buyers to effectively evaluate the 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 effort 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' proposals. The manager can extrapolate in the light of the results of benchmarking problems, and the performance of the vendors' proposals on the entire job mix.

(C) Other Acquisition aspects and practices: In addition to the above, there are several other acquisition aspects and practices also, which are given as follows:

(i) Hardware Acquisition: In the 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, training, etc., and expansion of computer installation for almost an indefinite period; therefore, this is not just buying the machine and paying the vendor for it, but it amounts to an enduring alliance with the supplier.

(ii) Software Acquisition: Once user output and input designs are finalized, the nature of the application software requirements must be assessed by the systems analyst. This determination helps the systems development team to decide 'what type of application software products 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. The 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 exposes organizations to possible litigation.

(iv) **Compliances with Security Protocols and Legal Requirements:** The proposed software should be compliant with the legal provisions (e.g. General Data Protection Regulation (GDPR) and Digital Personal Data Protection (DPDP) Act), wherever applicable. Moreover, they should have minimum security certificates to ensure they are not inherently vulnerable to attacks. These certificates may not be guaranteed protection from cyber-attacks, but they provide reasonable assurance in comparison with unsecured solutions.

(v) **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 cost and benefits of each proposed system.
- ❖ The maintainability of each proposed system.
- ❖ The compatibility of each proposed system with Existing Systems.
- ❖ Vendor Support.

(vi) 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 subjective method for validation and evaluation. The various criteria are put on a checklist 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, backup, 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 7.1 illustrates a Point Scoring Analysis list.

Table 7.1: 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?	7	7	5	6
Are other users satisfied with the software?	8	7	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
Total	**100**	**80**	**86**	**70**

- **Public Evaluation Reports:** Several consultancies as well as independent agencies compare and contrast the hardware and software performance of 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 to 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 workload 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 the 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 judgments can be made. It must be borne in mind, however, that various capabilities to be tested would have to be assigned relative weightage.

- 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 superhighways of information infrastructure. 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 they perform 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 the acquisition of already functional ready-to-use systems or by the development of customized solutions using requisite IT infrastructure, environment and support. System acquisition efforts are put in place due to many reasons:
- Due to the availability of systems at affordable prices subject to satisfactory solutions to the requisite tasks and functionalities.
- Because of the stress in the existing system the system is not able to meet the requirements of system stakeholders and particularly, of its users and thus requires to be changed or modified. There are situations, which can be managed by slight modifications, but there may be situations, which may need complete overhaul. For example: Increased competition, pressure on profits, and customer satisfaction are a few reasons, which have forced many corporations to go for better systems. Many of them have shifted from traditional accounting packages to Enterprise Resource Planning Software.
- 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 to capitalise on such opportunities.

The two cases given below describe the importance and need to automated system development:

Case 1: Manual Billing System: The billing clerk checks the price list of products before s/he bills the same to the 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 the customer. In the above process, the key issue is that the billing clerk needs to possess, an applicable and authorized price list with him. Business Process Design shall need to address the following critical issues:

- Availability of approved price lists with the billing clerk.
- How it shall be ensured that the billing has been done on applicable rates only?
- How is the approval accorded to price lists?
- Whether the price list updating process is pre-defined or need-based?
- How exceptions to the listed price shall be documented?
- How the exceptions shall be submitted to management?

Case 2: Computerized Billing System: In this system, every bill is generated through the system. The 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 database. There is no option available with the billing clerk to modify the 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 the system.
- How it shall be ensured that the price lists in the system cannot be modified?
- How is the approval accorded to price lists?
- Whether the price list updating process is pre-defined or needbased?
- How are the said price lists updated in the system?
- How is the correctness of updates is validated?
- How are exceptions, where the billed price is different from the price in the system authorized?
- How are the exceptions to price reported to management?
- Does the 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 modelling. 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 the following:

- How is the business objective change built into business process change?
- How shall the business processes be documented?

Business Process Modeling is an important step in the process of system development. This step is important and critical for the success of better system development. An offshoot of this process is the term Business Process Re-engineering. The key difference is, 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.

(D) System Acquisition Cycle

It is the activity of modifying an information system. It is important to have a System Acquisition Strategy in place that assists departments with the selection, purchase and, if applicable, implementation of technology-related systems i.e., hardware, software, and services. The goal of this strategy is to ensure that systems to be acquired to -

- align with the objectives and goals of the organization.
- integrate well and are compatible with existing software and technology infrastructure.
- that they result in a positive return on investment.

The key to getting value for organizations is to establish a win–win partnership with the vendor(s). If the partnership doesn't succeed due to inefficiencies with the vendor, etc., then an exit strategy should be exercised that eventually shall allow an organization to select a new vendor with minimized transition costs. The system acquisition process should include the identification and analysis of alternative solutions that are each compared with the established business requirements. In general, the acquisition process involves the following steps as depicted in Fig. 7.3:

1. **Defining System Requirements:** System requirements describe the needs or objectives of the system and define the problems to be solved, business and system goals, system processes to be accomplished, and the deliverables and expectations for the system. System requirements include defining the information being given to the system to process, the information to be processed within the system, and the information expected out of the system. Each requirement should be clearly defined so that later gaps in expectations are avoided.

   System requirements can be captured by interviewing management and those expected to use the information produced by the system to understand their expectations. Gathering requirements can also be accomplished by inspecting existing systems, reviewing related paper and electronic forms and reports, observing related business processes, meeting with IT management and support staff regarding their expectations and constraints for implementing and supporting the system and

researching other companies in a related industry, of similar company size, and with a similar technical environment to identify best practices and lessons learned.

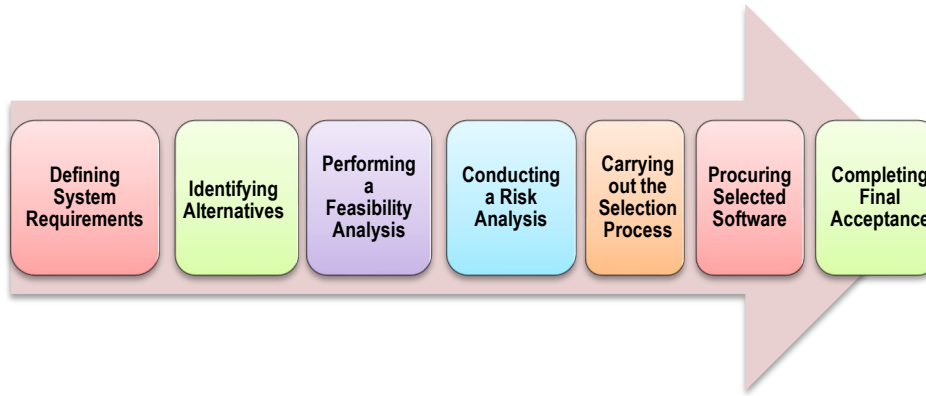


Fig. 7.3: System Acquisition Cycle

2. **Identifying Alternatives:** Many options exist in procuring system solutions (i.e., software), which include any combination of the following: off-the-shelf product, purchased supplier package, contracting for development or developing the system in-house, or outsourcing from another organization.

3. **Performing a Feasibility Analysis:** A feasibility analysis defines the constraints or limitations for each alternative from a technical as well as a business perspective. Feasibility analysis includes the following categories: economic, technical, operational, legal, contractual, and political. These concepts shall be discussed in the next section in detail.

4. **Conducting a Risk Analysis:** A risk analysis reviews the security of the proposed system. It includes an analysis of security threats and potential vulnerabilities and impacts, as well as the feasibility of other controls that can be used to reduce the identified risks.

5. **Carrying Out the Selection Process:** The selection process includes identifying the best match between the available alternatives and the identified requirements. According to KPMG's 2022 State of the Outsourcing, Shared Services, and Operations Industry Survey Report, the top three sourcing trends are Agile based Tendering, API driven integration, streamlined delivery models, AI driven contract Management and workplace Analytics. The survey also showed that smaller organizations place more importance on traditional selection criteria like industry experience and service quality than business outcomes and automation.

6. **Procuring Selected Software:** Once a technical solution has been selected, the procurement process helps ensure that the right terms and conditions are negotiated. One of the integral processes in any project is the procurement of services, hardware, and software. In most cases, organizations consider whether to make or buy systems. In either case, the procurement of external services is usually required. Depending on the extent of the service, a formal RFP or other requirements document needs to be prepared to request competitive bids. The requirements should include service levels with contract penalties and tracking metrics/success criteria.

7. **Completing Final Acceptance:** The procurement process sounds simple but is actually the most complicated of all the acquisition steps. It requires that the purchase price and conditions be stipulated and agreed upon. These agreements take the form of contracts. When procuring software, IT managers may complain about unpredictable license fees, pressured sales methods, poor technical support, and unclear pricing for ongoing maintenance fees.

   Software Contracts and Licenses Agreements are used to document agreements for development, marketing, distribution, licensing, maintenance, or any combination. Contracts can specify a fixed price or a price based on time and materials. Contracts based on time and materials state that the fees charged are directly attributable to actual expenses of time (hourly) or materials. These contracts place more financial risk on the buyer if the initial definition of pricing, the scope, or the desired requirements are unclear or poorly defined. Contract terms and conditions normally include the following:

   - ❖ A functional definition of the work to be performed.
   - ❖ Specifications for input or output designs, such as interfaces, screens, or reports.
   - ❖ Detailed description of the necessary hardware.
   - ❖ Description of the software systems or tools required for development or implementation.
   - ❖ Terms or limitations with the use of any related trademark rights or copyrights.
   - ❖ Requirements for the conversion or transfer of data.
   - ❖ System performance or capacity such as speed, throughput, or storage.
   - ❖ Testing procedures used to identify problems and the results expected to define acceptance.

- ❖ Information and system requirements serve as the basis for defining the acceptance tests.
- ❖ Supplier staffing and specified qualifications.
- ❖ Contact and relationship protocols between the buyer and the supplier.
- ❖ Expected schedules for development, implementation, and delivery.
- ❖ Methods for providing progress reports, such as meetings or reports.
- ❖ Definition of deliverables, which includes a clear description of each item to be delivered or provided by the supplier, when it is to be delivered, and any consequences for missed deliverables.
- ❖ Explicit criteria for defining acceptance of each deliverable as well as for final acceptance.
- ❖ Requirements and expectations for installation.
- ❖ Documentation expected to be provided to the supplier or by the supplier as well as any intellectual property rights needed to maintain or customize the documentation.
- ❖ Training expected to be provided as part of the product or service.
- ❖ Any applicable warranties or maintenance, including provisions for future versions currently in development.
- ❖ Any requirements for indemnity or recovery for losses, such as insurance or bonds.

7.3 INFORMATION SYSTEM DEVELOPMENT METHODOLOGIES

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 several 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 provides 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 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:

sab framewrk read krna

- Waterfall Model-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
- V-Shaped Model
- Agile Methodologies models

I. **Waterfall Model:** The waterfall approach is a traditional development approach in which each phase is carried out in sequence or linear fashion. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release. In this traditional approach to system development, activities are performed in sequence. Fig. 7.4 shows 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.

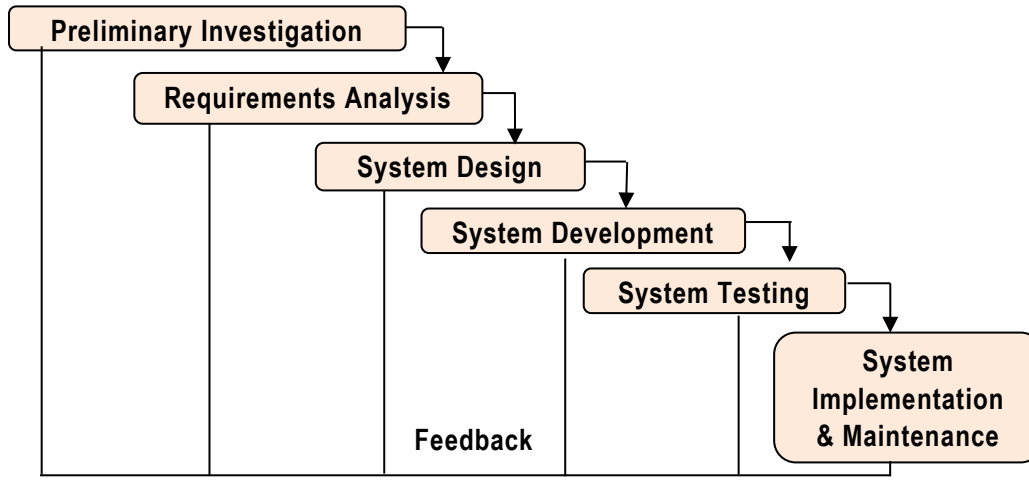


Fig. 7.4: Waterfall Approach

The characterizing features of this model have influenced the development community in a big way. Some of the key characteristics are the following:

- The 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.
- 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 (Refer Fig. 7.5):

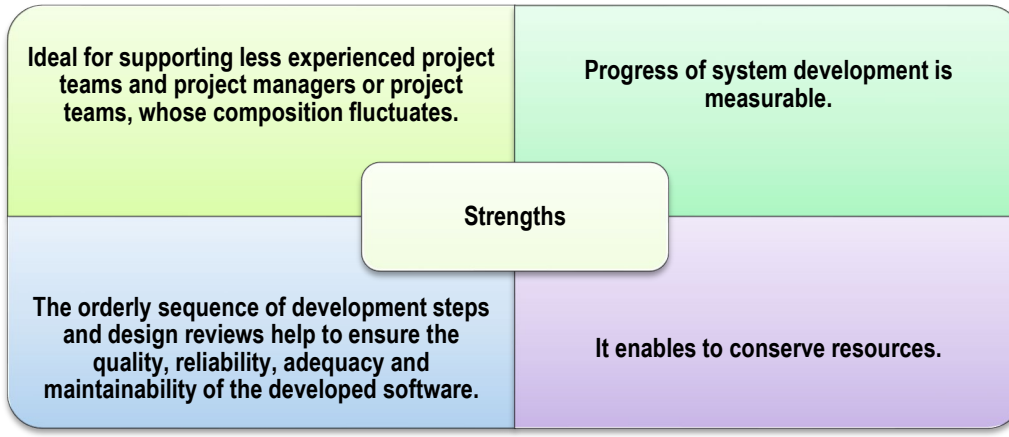


Fig. 7.5: Strength of Waterfall Model

(b) Weaknesses: Though it is a highly useful model, it suffers from various weaknesses too. Experts and practitioners identify number of weaknesses including the following:

- ❖ It is criticized for being inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- ❖ Project progresses forward, with only slight movement backwards.
- ❖ 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 is 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 a clear vision of responsibility.

II. **The Prototyping Model:** The traditional approach sometimes may take years to analyze, design and implement a system. More so, many times we know 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 the 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 with a full-scale and fully operational system. As users work with the prototype, they learn about the system's 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. 7.6 wherein Implementation and Maintenance phases followed by full-blown developments take place once the prototype model is tested and found to be meet the users' requirements. The generic phases of this model are explained as follows:

- o **Identify Information System Requirements:** In the traditional approach, the system requirements are to be identified before the development process starts. However, under the 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.
- o **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 about the information system, judge response times of the system, and issue commands.
- o **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 the iterative process of modification and reevaluation continues until the users are satisfied.

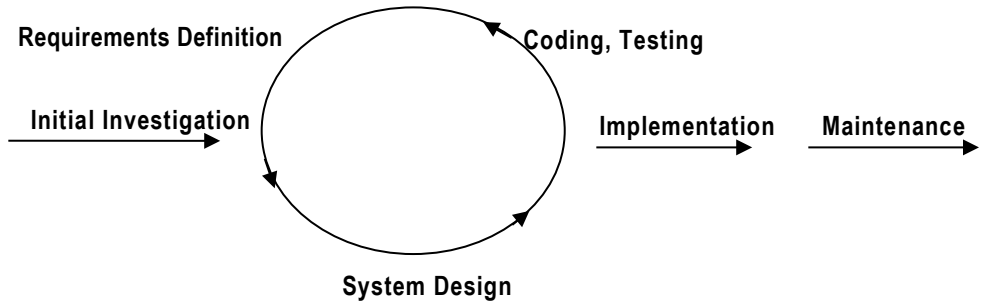


Fig. 7.6: Prototyping Model

- **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 the team 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.
- ❖ The Prototype may not have sufficient checks and balances incorporated.
- ❖ Prototyping can only be successful if the system users are willing to devote significant time to 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 behavioural 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 with the prototype.

In spite of above-listed weaknesses, to some extent, systems analysis and development have 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.

III. **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 7.7.

The product is decomposed into a number of components, each of which is designed and built separately (termed as builds). Each component is delivered to the client when it is complete. This allows partial utilization of the 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 a completely new system all at once. A few pertinent features are listed as follows:

- o 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.
- o Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.
- o 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 the installation of the final prototype (i.e. Working system).

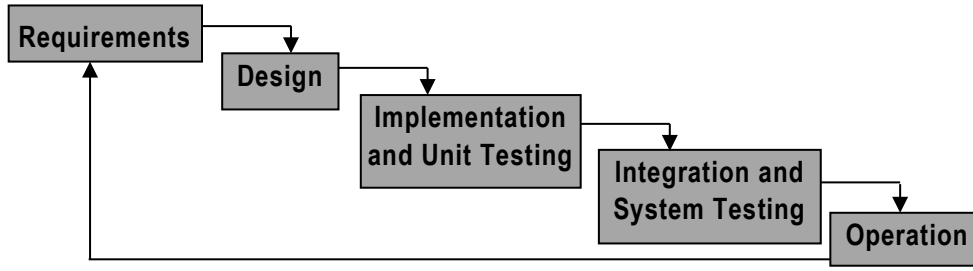


Fig. 7.7: Incremental Model

(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, and 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 on to 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 does 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.

IV. Spiral Model: The Spiral model is a software development process combining elements of both design and prototyping-in-stages. It tries to combine the advantages of top-down and bottom-up concepts. It combines the features of the prototyping model and the waterfall model (given in Fig. 7.8). The spiral model is intended for large, expensive and complicated projects. Game development is the 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:

- o 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.
- o A preliminary design is created for the new system. This phase is the most important part of the "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 especially 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 solutions in order to deal with the potential changes in the requirements.
- o 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.
- o 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.

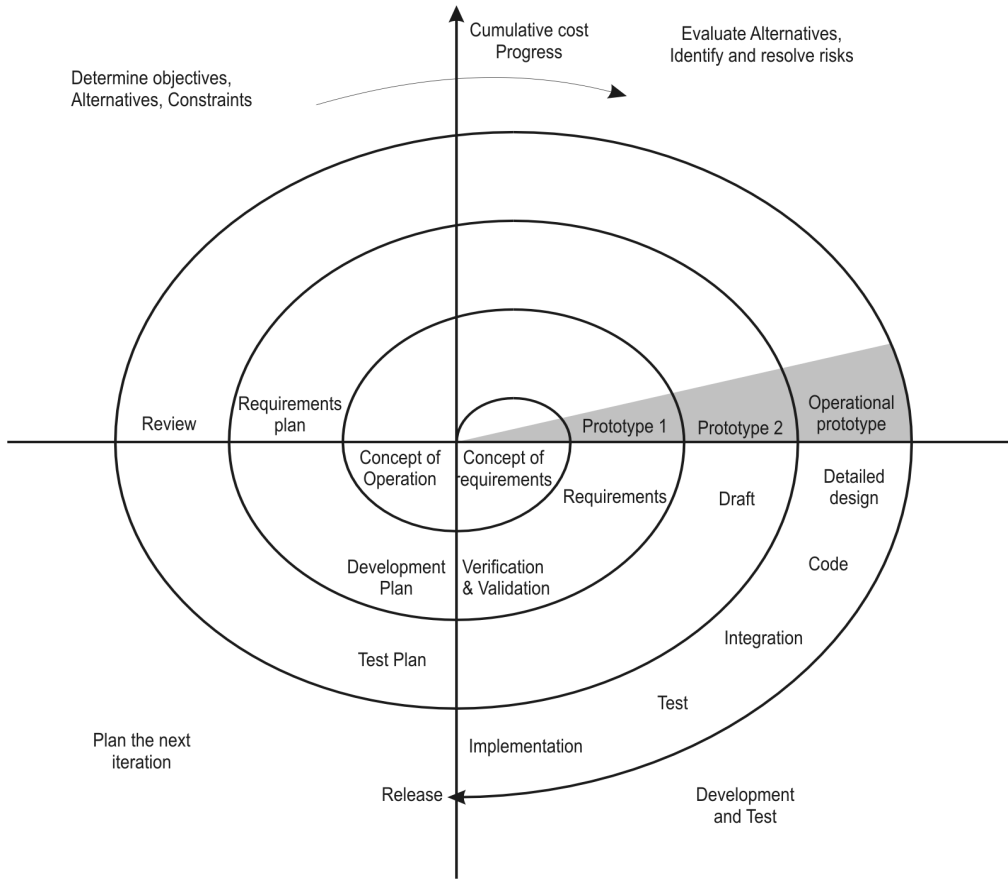


Fig. 7.8: Spiral Model

Refer below Table 7.2 for strengths and weaknesses of the Spiral Model.

Table 7.2: Strengths & Weaknesses of Spiral Model

Strengths	Weaknesses
• It enhances 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 on the type of project risk. For example, a project with a low risk of not meeting user requirements but a	• It is challenging to determine the exact composition of development methodologies used for every 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

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.	generate more work for the next cycle. • There are no firm deadlines, cycles continue with no clear termination condition leading to, the inherent risk of not meeting the budget or schedule.

V. 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:

- The 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, the emphasis is on reducing requirements to fit the timebox, not on 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.

Refer Table 7.3 for strengths and weaknesses of the RAD Model.

Table 7.3: Strengths & Weaknesses of RAD Model

Strengths	Weaknesses
• The operational version of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks. • Because RAD produces systems more quickly and with a business focus, this approach tends to produce systems at a 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, as compared to Waterfall, Incremental, or spiral frameworks. Users are seen as gaining more of a sense of ownership of a system, while developers are seen as gaining more satisfaction from producing successful systems quickly. • It concentrates on essential system elements from a 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.	• Fast speed and lower cost may affect adversely affect 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. • 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 a lack of attention to later system administration needs built into the 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.

VI. Agile Model: This is an organized set of software development methodologies based on ***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 the 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 cooperation 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.

Refer Fig. 7.9 to know about strengths and weaknesses of the Agile Model.

Strengths

- 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.

Weaknesses

- 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.

Fig. 7.9: Strengths and Weaknesses of Agile Model

SUMMARY

Data comprises of raw facts and information is data transformed into meaningful and useful form. The valuable information helps the organization to achieve its goals. Information systems are the set of interrelated elements that are used to collect, manipulate, store and disseminate data and information. Feedback is the output which is used to make modifications to input or processing activities. The development of the system is the key element for most organization that measure and control activities. The various key considerations are discussed for the selection of the method of development. The methods of development such as Waterfall, Prototyping, Spiral, Rapid Application Development (RAD) method, and Agile method are described along with their advantages and disadvantages.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Which of the following is true about Spiral Model?

   (a) It combines features of the prototyping model and waterfall model.

   (b) It combines features of the prototyping model and RAD model.

   (c) It combines features of the waterfall model and RAD model.

   (d) It is intended for small and simple projects.

2. During System Acquisition in SDLC, the top management of an enterprise should establish acquisition standards that address the security and reliability issues as per current state-of-the art development standards. Which of the following is not considered while focusing on acquisition standards?

   (a) Ensuring security, reliability, and functionality already built into a product.

   (b) Ensuring managers' complete reviews of appropriate vendor, contract and licensing.

   (c) Request for proposals soliciting bids when acquiring off-the-shelf or third-party software.

   (d) To select the programming techniques and languages to be used for systems development.

3. Softtech, a software development company, has clients in many fields like pharmaceuticals, educational institutes, health industry, etc. The company follows an approach to develop the software by releasing multiple versions, wherein the product is decomposed into the number of components and each component is delivered to client on its completion. Identify the System development approach adopted by Softtech.

   (a) The Waterfall Model

   (b) The Prototyping Model

   (c) The Spiral Model

   (d) The Incremental Model

4 Amongst various System Development Methodologies, a software development model that combines iterative and incremental methods is _____.

   (a) Spiral

   (b) Agile

   (c) Prototype

   (d) Rapid Application Development (RAD)

5. Which of the following is not a strength of RAD model?

   (a) Possibility of quick initial review.

   (b) Constant integration isolates problems and encourages customer feedback.

   (c) Provides the ability to rapidly change system design as demanded by users.

   (d) Enhances the risk avoidance.

ANSWERS/SOLUTIONS

1.	(a)	2.	(d)	3.	(d)	4.	(b)	5.	(d)

UNIT – III

INFORMATION SYSTEMS' CONTROLS

CHAPTER 8

INFORMATION SYSTEMS' CONTROL AND ITS CLASSIFICATION

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- establish an understanding of the Internal Control Framework and its components.
- build a detailed understanding of various types of controls classified under different parameters.
- comprehend controls based on "Objective of Controls".
- classify the controls based on "Nature of information system resources".
- know the categorization of controls based on "Audit perspective".
- understand the controls based on "Control Activities".
- know the role of auditors while inspecting these controls.

CHAPTER OVERVIEW

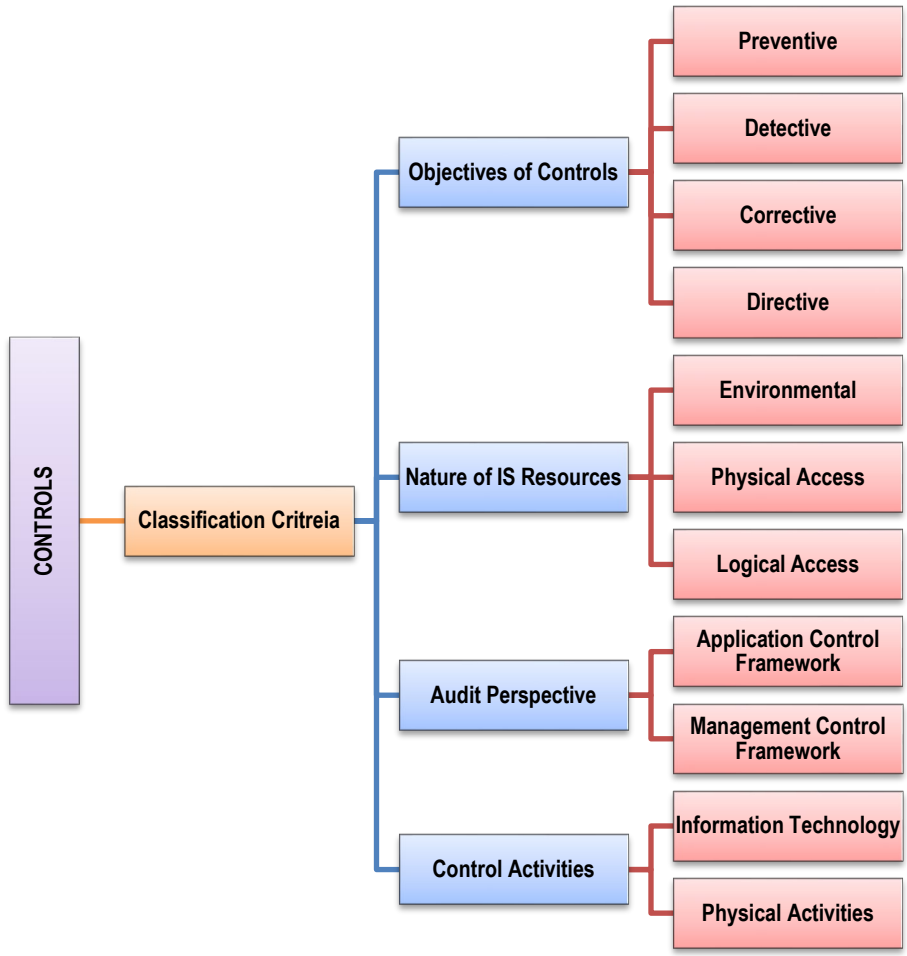


Illustration: ABC Multispecialty Hospital

- ABC Multispecialty Hospital is one of the prominent hospitals and medical college with national reputation having 250 patient beds and over 3000 employees inclusive of doctors and administrative staff.
- The hospital has long been the market leader in several service lines such as critical care, ambulatory care, and home health care.
- In the early 90's, the hospital started using specific software for recording its daily financial transactions and has been upgraded and customized on a regular basis.

Problem Raised

- The hospital was doing well, however recent changes in regulatory compliances, and market factors have resulted in falling annual profits.
- The hospital embarked on a dramatic Business Process Re-engineering effort. With the increasing competition, the hospital sought to reduce its annual operating cost by 10% of its total operating expenses.

Solution Found

- This initiative was taken by the hospital's **Chief Executive Officer**, Mr. Rajesh who sought to change the way the organization viewed its patients, employees, and other stakeholder groups. Hence, ten groups were formed namely finance, information systems, nursing, ancillary services, laboratory, administrative, pharmacy, radiology, supportive services and physician services to review the overall operation of hospital.
- These groups were given a three-day orientation and training session by the management consulting company hired by the hospital for assistance in this project.
- The administrative work group initiated a study on the working of the Financial Accounting System used by the Accounts department. After the completion of their study, the administrative group proposed removal of two clerk positions which were no longer necessary due to a decrease in the overall number of medical supply vendors. However, Certified Public Accountant (CPA) and Accounts Manager of hospital opposed the staff reduction, it may affect the general performance concerns and a continuous high turnover rate in the accounts department. However, the other stakeholder approved the same, hence both positions were eliminated from accounts department.
- The hospital vendors had raised various complaints about slow payments from the accounts department. Vendors were upset as they were not timely paid and had raised numerous complaints about their slow payments, and therefore, used to threaten the management to stop fully the supply of critical care equipment and accessories to the hospital. This generates the requirement of staff, when this news was shared among the people, one of the employee suggested the name of his son Mr. Mahesh Johri who would be interested in this job and his qualification also matched with this profile.
- Mr. Mahesh was found to be personable, curious and eager to work at the hospital, therefore hired as a temporary staff without interviewing any other candidate. Since, he is the son of present staff, and hired as temporary staff, therefore no background investigation was required. Though, it was one of the hospital's standard operating procedure for employees in sensitive department such as IT and Finance.

Issues found by stake holder in solution provided

- The hospital has an internal audit department with Certified Information Systems Auditors. This department performs the internal audit on various business processes of hospital for hassle free working. During a routine audit of the finance division, Mr. Pankaj, Internal Audit Manager, was introduced to Mr. Mahesh.
- Mr. Pankaj came to know Mahesh's father is also working in the hospital, he immediately checked for the hospital's policies regarding nepotism and found that the general administrative policies of hospital was prohibits the members of the same family to work in a sensitive department. It was done to avoid the impact on the integrity or safekeeping of corporate assets or documents.
- The situation in the accounts department appeared to conflict with hospital's policies and was considered a red flag, indicating a situational environment which is conducive to a potential management.

Discovery of Fraud

- After six months, CFO discovered some very unsettling information and identified six cash disbursements totalling ₹ 80,000 that had been made to Mr Mahesh. He immediately contacted Mr Pankaj, the company's Internal Audit Manager asking him about the primary job responsibilities of Mr. Mahesh and his employment relationship.
- Mr. Pankaj analysed the copies of relevant information system reports, cancelled cheques from the hospital's bank, supporting cash disbursement authorization forms, did a thorough review of the accounts payable department's operating procedures and found that Mr. Mahesh appeared to have forged six cash disbursement authorization forms, which contained vendor invoice data (e.g. vendor name, vendor address, invoice number, and invoice amount).
- It was found that Mr. Mahesh input the data contained on the fraudulent accounting forms into the accounts payable accounting module under his own vendor account.
- Furthermore, while Mr. Mahesh's supervisor was away on vacation, he was assigned responsibility for performing the semi-weekly cash disbursement run. It was hospital's standard operating procedure to require a second signature on all cheques over ₹ 15,000. Mr. Mahesh was very savvy, so in order to avoid creating suspicion by management, each of the individual cheques processed by Mr. Mahesh was for less than ₹ 15,000.
- At the conclusion of the fraud investigation, Mr. Mahesh was now to be interrogated. After investigation he confessed to the crime and explained that he was forced to steal from

hospital. Mr. Mahesh then signed a written confession and was immediately suspended without pay.

Observations/Result

- This case illustrated a variety of risks and corresponding controls that are normally found in a Financial Accounting system.
- It illustrates how a well-designed information system, can still have weaknesses in it. Then, once a system weakness is discovered by an employee; he/she can exploit it to take personal advantage.
- Another important issue brought out in the case is that company management can override policies and procedures at their discretion.
- While sometimes justified, the corresponding risk needs to be fully understood. It also provides an interesting example of how Information Systems auditors can work with other employee groups to improve internal controls, governance and protect against future fraudulent activities.

8.1 INTRODUCTION

The increasing use of Information Technology (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.

Control is defined as policies, procedures, practices, and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented, detected, and corrected.

The main objectives of information controls are safeguarding of assets, maintenance of data integrity, effectiveness in achieving organizational objectives, and efficient consumption of resources to ensure that the business objectives are achieved. To manage the risks, businesses need to set up internal control systems which can be applied to all activities and process of business.

This is achieved by designing and effective internal control framework which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

8.2 CONTROLS

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 access the records and make amendments, some of which could remain undetected.

Today's dynamic global enterprises need information integrity, reliability, and validity for timely availability of accurate information throughout the organization. The goals are to reduce the probability of organizational costs of data loss, computer loss, computer abuse, incorrect decision making and to maintain the privacy; To achieve the required goals, an organization's management must set up a system of internal controls within IT environment. 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's Information System (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; Qualify Assurance Procedures; Physical access controls; network and communication; Database Administration; protective and detective mechanisms against internal/external attacks etc.

8.3 CLASSIFICATION OF CONTROLS

A **control** is a system that is used to prevent, detect, or correct unlawful events or errors. 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. The common classification of controls is represented in the Fig. 8.1.

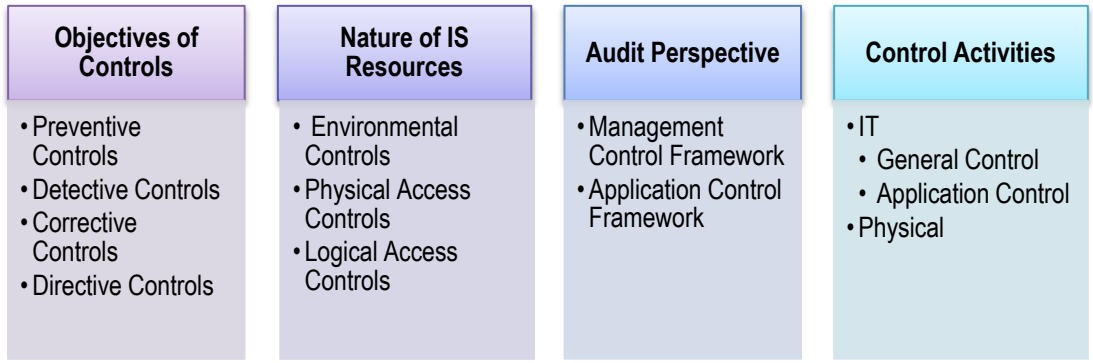


Fig. 8.1: Classification of Controls

8.3.1 Classification based on "Objectives of Controls"

The controls applied to risks can be represented with a hierarchy of options of **Preventive, Corrective, Directive and Detective (PCDD)** which are described as follows through an illustration highlighted in the Fig. 8.2:

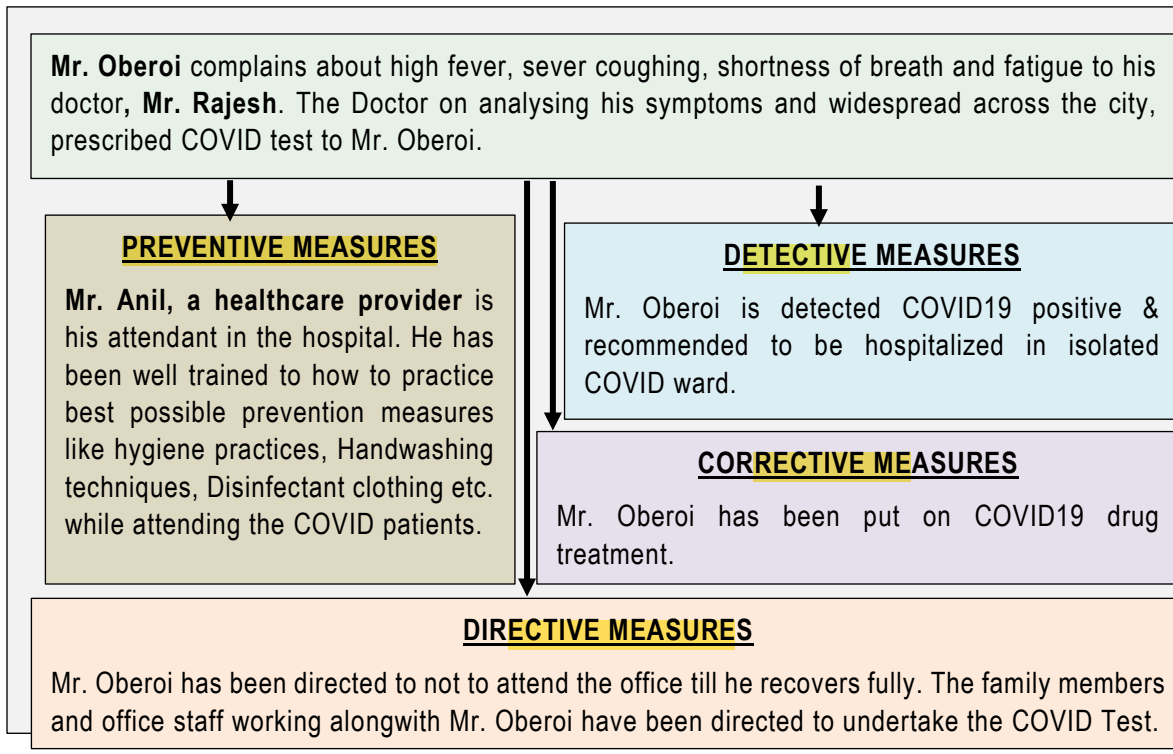


Fig. 8.2: ILLUSTRATION

(A) Preventive Controls: These controls are designed to prevent errors, omissions, or security and malicious incidents from occurring. Preventive controls can be implemented in both

manual and computerized environments. The implementation methodology may differ from one environment to the other.

The main characteristics of Preventive controls are as follows:

- A clear-cut understanding about the vulnerabilities of the asset.
- Understanding of probable threats.
- Provision of necessary controls for probable threats from materializing.
- They are basically proactive in nature.
- These are more cost-effective than detection and correction of errors when they occur.

Refer Table 8.1 to know about advantages, disadvantages, and examples of Preventive Controls.

Table 8.1: Preventive Controls

Advantages	Disadvantages	Examples
These controls eliminate the risk; and therefore, no further consideration is required.	Not a cost-effective operation, moreover not possible for operational reasons. Elimination of beneficial activities, activities may be either outsourced or replaced with something less effective and efficient.	Employing qualified personnel; Segregation of duties; Access control that protect sensitive data/ system resources from unauthorized people; 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 act like a corrective control also) etc., Intrusion Prevention and Passwords. The above list contains both manual and computerized, preventive controls.

(B) Detective Controls: These controls are designed to detect errors, omissions or malicious acts that has occurred and report the occurrence. In other words, Detective Controls detect errors or incidents that elude preventive controls.

The main characteristics of Detective controls are given as follows:

- These controls required to have clear understanding of lawful activities so that deviation is reported as unlawful, malicious, etc.
- These controls require an established mechanism to refer the reported unlawful activities to the appropriate person or group, whistle blower mechanism.

- These controls interact with preventive control to prevent such acts from occurring and may lead to change in structure of preventive controls.
- Surprise checks by supervisor.
- These controls are designed to be of investigative in nature that reveals errors by making a comparison with actual occurrence based on prescribed standards.
- These controls provide evidence after the event such as loss/error has occurred but do not prevent them from recurring.

Refer Table 8.2 to know about advantages, disadvantages, and examples of Detective Controls.

Table 8.2: Detective Controls

Advantages	Disadvantages	Examples
Simple to administer and gives early warning if any of other risk has materialize	Risks generally occur before they are detected.	Review of payroll reports; identification of account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities Compare transactions on reports to source documents; Monitor actual expenditures against budget; Use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend; Hash totals; Check points in production jobs; Echo control in telecommunications; Duplicate checking of calculations; Past-due accounts report; internal audit functions; Intrusion Detection System; Cash counts and bank reconciliation and Monitoring expenditures against budgeted amount. For sensitive electronic communications, detective controls indicate that a message has been corrupted or the sender's secure identification cannot be authenticated.

(C) **Corrective Controls:** It is desirable to correct errors, omissions, or incidents once they have been detected. These corrective processes also should be subject to preventive and detective controls because they represent another opportunity for errors, omissions, or falsification.

The main characteristics of the Corrective controls are as follows:

- 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 errors on account of unlawful/wrong event.
- Most efficient to prevent errors or detect them as close as possible to their source to simplify correction.
- Designed to reduce the impact or correct an error once it has been detected.
- Modifying the processing systems to minimize future occurrences of incidents.

Refer Table 8.3 to know about advantages, disadvantages, and examples of Corrective Controls.

Table 8.3: Corrective Controls

Advantages	Disadvantages	Examples
• Reactive in nature. • Simple and cost effective. • Do not replace or eliminate the existing practices.	• The design and implementation of these controls sometimes may cause potential disagreement. • These are put in place because of regulatory requirement; hence the organization has to confirm their acquiescence with minimum requirement of legislation.	Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. For example- "Complete changes to IT access lists if individual's role changes" is an example of corrective control. If an accounts clerk is transferred to the sales department as a salesman, his/her access rights to the general ledger and other finance functions should be removed and he/she should be given access only to functions required to perform his sales job. Some other examples of Corrective Controls are submitting corrective journal entries after discovering an error, to identifying and removing unauthorized users or software from systems or networks to recovery from incidents, disruptions, or disasters; A

		Business Continuity Plan (BCP); Contingency planning; Backup procedure; Rerun procedures; System reboot; Change input value to an application system; and report violations.

(D) Directive Controls: These controls generally give directions to people or employees to follow and make them understand to limit the damage and loss. Directive controls ensure the achievement of a specific outcome. As an important control, these are likely to be used for most risks irrespective of existence of other types of control. The management of the organization identified the risk and their integration; prepares the relevant directive; ensures that these are approved for compliance purposes.

The main characteristics of the Directive controls are as follows:

- Ensures that all identifieds risks are managed by providing formal directions to staff of the organization.
- Requires inter departmental indulgent which may include embedded regulatory requirements.
- Ensures the compliance of regulatory requirements.
- These controls will be the first to response to a risk if it occurs.
- These controls are easy to implement as compared to directive control than preventive and corrective to reduce the risk by direction.

Refer Table 8.4 to know about advantages, disadvantages, and examples of Directive Controls.

Table 8.4: Directive Controls

Advantages	Disadvantages	Examples
• The requirement or policies and procedures to control the risk can be explained in a normal training session for employees.	• Training can give impression implementation of control. • May cause chaos as decentralized operations are integrally divided.	The directive controls can be in the task having a risk, training, and instruction, together with information and documented procedure; provide training the employee to wear personal protective equipment while working on dangerous operation; supervision of enforced procedures; providing training manual to driver for defensive driving and use of

• Result oriented. • Safeguarding of asset.		protocols in case of emergency, SOP for process, and Internal circulars.

8.3.2 Classification based on "Nature of Information System Resources"

(A) **Environmental Controls:** These are the controls relating to IT environment such as power, air-conditioning, Uninterrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers etc. Table 8.5 lists all the controls against environmental exposures like Fire, Electrical Exposures, Water Damage, and Pollution damage and others with their corresponding controls respectively.

Table 8.5: Environmental Controls

Fire It is a major threat to the physical security of a computer installation.	**Smoke Detectors:** These should be positioned at places above and below the ceiling tiles and should produce an audible alarm and must be linked to a monitored station. **Reduction in Electric firing:** The location of the computer room should be strategically planned. Wiring should be placed in the fire-resistant panels and conduit. **Fire Extinguishers:** Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon-dioxide based fire extinguishers should be well placed and maintained. **Fire Alarms:** Place both automatic and manual fire alarms at strategic locations. Install control panel and master switches for power and automatic fire suppression system. On activation of fire alarm, a signal may be sent automatically to permanently manned station. **Regular Inspection:** Regular inspection by Fire Department Officials. Proper documentation of the procedure should follow during emergency. **Raising awareness:** Fire exits should be clearly marked, and all the staff members should be trained to use the system in case of emergency. Periodic Mock Drills should be conducted to create awareness. **Documented and Tested Emergency Evacuation Plans:** Saving human life should be given paramount importance. Proper procedure to controlled shutdown of the computer should be documented and tested.
Electrical Exposure	**Electrical Surge Protectors:** The risk of damage due to power spikes can be reduced using Electrical Surge Protectors.

These include the risk of damages that may be caused due electrical faults such as non-availability of electricity, spikes (temporary very high voltages), fluctuations of voltage and other such risks.	**Un-interruptible Power System (UPS)/Generator:** The UPS provides the backup by providing electrical power from the battery to the computer for a certain span of time, in case of power failure. **Voltage regulators and circuit breakers:** These protect the hardware from temporary increase or decrease of power. **Emergency Power-Off Switch:** An emergency power-off switch at the strategic locations should be easily accessible and to be secured from unauthorized people. **Power Back up and alignment:** Redundant power links should be available at data centre so that interruption of one power supply does not adversely affect availability of system.
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, floods tornadoes, etc.	**Water Detectors:** These should be placed under the raise floor, near drain holes and near any unattended equipment storage facilities. **Strategically locating the computer room:** To reduce the risk of flooding, the computer room should not be located in the basement of the ground floor of a multi-storey building. 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-prone areas, have the installation above the upper floors but not at the top floor. • Water proofing and water leakage Alarms.
Pollution Damage The major pollutant in a computer installation is dust. Dust caught between the surfaces of storage devices may cause either permanent damage to data or read/write errors.	**Prohibitions against eating, drinking and smoking within the information processing facility** • These activities should be prohibited from the information processing facility and such instructions should be displayed at appropriate places such as - a sign on the entry door.

(B) **Physical Access Controls:** The Physical Access Controls are the controls relating to physical security of the tangible 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. The details of these controls are given in Table 8.6.

Table 8.6: Controls for Physical Exposures

Heena and Neha are two friends who started their startup of candle making and home decorative items. To secure their IT systems, they need to implement controls for physical exposures. What are the possible options for the same?

Lock the Doors

- **Cipher locks (Combination Door Locks)** are used in low security situations or when many entrances and exits must be usable all the time. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period, usually 10 to 30 seconds.
- **In Bolting Door Locks,** a special metal key is used to gain entry and to avoid illegal entry, the keys should not be duplicated.
- **Electronic Door Locks** can be used wherein a magnetic or embedded chip-based plastics card key or token may be entered into a reader to gain access in these systems.

Physical Identification Medium

- **Personal Identification Number (PIN)** is a secret number assigned to an individual, in conjunction with some means of identifying the individual that 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. Entry of individual will be matched with the PIN number available in the security database.
- The **Plastic Cards** are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.
- **Identification Badges** are special identification badges that can be issued to personnel as well as visitors. For easy identification purposes, the color of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys.

Logging on facilities

- **Manual Logging:** All visitors should be prompted to sign a visitor's log indicating their name, date and time of visit, company represented, their purpose of visit, and person to meet. Logging may happen at both fronts office - reception and at Server room. A valid and acceptable identification proof 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.

Other means of controlling physical access

- **Video Cameras** should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video footage must be retained for longer period for future audit/investigations if any thing may happen.
- Extra security can be provided by appointing **Security Guards** aided with CCTV feeds. Guards supplied by an external agency should be made to sign NDA (Non-Disclosure Agreement) / bond to protect the organization from loss due to theft of data.
- A responsible employee should escort all visitors to ensure **Controlled Visitor Access** wherein visitors may be friends, maintenance personnel, computer vendors, consultants, and external auditors.
- All **service contract personnel**, such as cleaning people and off-site storage services, should be asked to sign a bond / NDA. This can help in minimizing the financial exposure of the organization.
- **Dead Man Doors/Man trap-based** systems encompass 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. It helps to manage traffic and prohibits the intruder from escaping the facility quickly.
- There should be **non-exposure of sensitive facilities** such as the presence of windows of directional signs hinting at the existence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.
- **Computer Terminal Locks** ensure that the device to the desk is turned off or not accessed by unauthorized persons.
- All incoming personnel can use **Controlled Single-Entry Point** unnecessary or unused entry points should be eliminated or deadlocked.
- Illegal entry can be avoided by linking the **Alarm System** to inactive entry point and the reverse flows of enter or exit doors, to avoid illegal entry. Security personnel should be able to hear the alarm when activated. Periodic mock drill should cover testing of alarms.
- **Perimeter Fencing** at boundary of the facility may also enhance the security mechanism.
- **Control of out of office during the working hours of employees** should be monitored carefully and movements of such employees must be logged and reported to the concerned officials periodically by geo tagging.
- **Secured Report/Document Distribution Cart** must be covered and locked and should always be attended.

(C) Logical Access Controls: Logical Access Controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. It restricts the use of information to authorized individulas, groups, or organizations.

The characteristics of these controls are as follows:

- These are the controls related to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc.
- These are implemented to ensure that access to systems, data and programs is restricted to authorized users 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.

Table 8.7 highlights various controls for technical exposures.

Table 8.7: Controls for Technical Exposures

I. User Access Management: This involves the system administrator for giving individual users access to the application/Menu/Sysstem required as per the role in the organization . This is an important function and involves the following activities: ○ **User Registration:** There should be form for user registration which will provide the information about user such as Name, designation, Department, date of joining, access rights to be given, approval of access rights by Head of Department Standard forms should also be used for de-registration/transfer of user rights. ○ **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities are to be minimal w.r.t their job function. For example, an operator at the order counter shall have direct access to order processing activity of the application system. Similarly, a business analyst could be granted access to view the report but should not allow to modify the report. Modification can be be done by the developer. ○ **User password management:** 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.

- **Review of user access rights:** A user's need for accessing information may change due to change in job profile due to promotions / transfer / rotation. Periodic review of access rights should be done to check inconsistencies in the user's current job profile, and the privileges granted.

II. **User Responsibilities**: User awareness and responsibility are also important factors and include followings :

- **Password use:** This includes mandatory use of strong passwords to maintain confidentiality. Controls can be built in system for use of strong password. The definition of strong password should be displayed to user while creation / change of passwords.
- **Sharing of Password:** User should never share the password with anyone.
- **Writing of Password:** Password should not be written on paper / desk while operating it should be kept secured by user.
- **Unattended user equipment:** 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. Control should be built in IT system so that users are automatically logged off after certain period of inactivity. While leaving the premises from work, care should be taken to always lock the system.

III. **Network Access Control:** Network Access controls refers to the process of managing access for use of network-based services like shared resources, access to cloud based services, remote login, intranet wireless network and internet access. The protection can be achieved through the following means:

- **Policy on use of network services:** An enterprise-wide policy applicable to internet and other network aligned with the business need is the first step. Selection of appropriate services and approval to access them should be part of this policy.
- **Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks e.g. internet access by employees will be routed through a firewall and proxy.
- **Segregation of networks:** 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 thereby providing a secure remote connection.
- **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.

- **Security of network services:** Network devices should be accessed through authentication and authorization policy should be implemented across the organization's network.
- **Firewall:** 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 that will allow only authorized traffic between the organization and the outside to pass through it. The firewall must be immune to penetrate from both outside and inside the organization. In order to insulate the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access as per the organization's network usage policy. The firewall rules should be reviewed periodically to address new threats.
- **Network Encryption:** Network encryption is defined as the process of encrypting data and messages transmitted or communicated over a computer network. Encrypting data means the conversion of data into a secret code for storage in databases and transmission over networks. Two general approaches - Private key and Public key encryption are used for encryption.
- **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 measures 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 limit 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.

IV. Operating System Access Control: Operating System (O/S) is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database, and printers. Major tasks of O/S are Job Scheduling; Managing Hardware and Software Resources; Maintaining System Security; Enabling Multiple User Resource Sharing; Handling Interrupts and Maintaining Usage Records. 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'. Hence, protecting operating system access is extremely crucial and can be achieved using the following steps.

- **Automated terminal identification:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.
- **Terminal log-in procedures:** A log-in procedure is the first line of defense against unauthorized access as it does not provide unnecessary help or information, which could be misused by an intruder. 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 and accordingly authorizes the log-in.

- **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:** Access Control Lists (ACLs) provide a method for controlling access to objects on a computer system. ACLs aim to protect operating system resources, including directories, files, and devices. An ACL is a list of users and groups, alongwith the permissions they have for an object, such as a file or directory. hese permissions include read, write, execute, delete, list directory contents, and change permissions.
- **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.
- **User identification and authentication:** 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.
- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should be stored in encrypted form and not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. This utility should be accessible to system administrator only. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. The design of the duress alarm should be simple enough to be operated under stressful situations.
- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in the absence of legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time. For example, System access should not be allowed after 8.00 p.m. and before 8.00 a.m. or on a Saturday / Sunday or Holidays.

V. **Application and Monitoring System Access Control:** Applications are the most common assets that access information. Users invoke the or modules of application to access, process and communicate information. Hence, it is necessary to control the accesses to application. Some of the controls are as follows:

- **Information Access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. Controls are implemented on access rights like read, write, delete, and execute to users, and further to ensure that sensitive output is sent only to authorized terminals and locations.
- **Sensitive System isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect/report any unauthorized activities.
- **Event logging:** 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. 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 and, IP address from where the request has been originated.
- **Monitor System use:** Based on the risk assessment, 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. Considering the cyber risk, organization can outsource the continuous monitoring of key logging activities.
- **Clock Synchronization:** Event logs maintained across an enterprise network play a significant role in correlating an event and generating reports on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

VI. **Controls when mobile:** In today's organizations, computing facilities are not restricted to a certain data center alone. Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security. Theft of data carried on the disk drives of portable computers is a high-risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features. VPN (Virtual Private Network) should be implemented for sharing data with employees / vendors who have opted for work from home option.

8.3.3 Classification based on "Audit Perspective"

There can be several approaches for audit in IT environment . Auditors have found two ways to be especially useful when conducting information systems audits, as discussed below. Fig. 8.3 and Fig. 8.4 provide an overview of The Management Control Framework and Application Control Framework respectively.

A. **The Management Control Framework (Refer Fig. 8.3):** Managerial functions must be reviewed to ensure the development, implementation, operation, and maintenance of information systems in a planned and controlled manner in an organization. These functions provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

I. **Top 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 their enterprise system has put in place are sufficient so 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 will operate. The controls flow from the top of an organization to the bottom; the responsibility still lies with the senior management. Top management is responsible for planning for the information systems function. The major functions that a senior management must perform are **Planning, Organizing, Leading** and **Controlling**.

II. **Systems Development Management Controls:** Systems Development Management has responsibility for the functions associated with analyzing, designing, building, altering, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentation and authorizations are available for each phase of the system development process. It includes controls required for new system development activities. Therea are various activities involved that deal with system development controls in IT setup.

III. **Programming Management Controls:** Program development and implementation is a major phase within the system's development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. Refer Fig. 8.3 for the details of each phase of the Program Development Life cycle.

IV. **Data Resource Management Controls:** In organizations, data is a critical resource that must be managed properly accordingly, centralized planning and control are implemented. For effective data management , 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 easily if the change is required and the integrity of the data must be preserved.

If data repository system is used properly, it can enhance data and application system reliability. Data definition should be controlled carefully, as 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, segregating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities. Data integrity is defined as maintenance, assurance, accuracy, consistency of data and the control activities that are involved in maintaining it are highlighted in Fig. 8.3.

V. **Security Management Controls:** Information security administrators are responsible for ensuring that information systems assets categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software are secure. Assets are secure when the expected losses that may occur are kept at an acceptable level. Environmental Controls, Physical Controls and Logical Access Controls are all security measures against the possible threats. However, despite the controls on place, there could be a possibility that a control might fail. Disasters are events/incidents that are so critical that has capability to hit business continuity of an entity in an irreversible manner.

When disaster strikes, it should be possible to recover operations and mitigate losses using the controls of last resort - A **Disaster Recovery Plan (DRP)** and **Insurance**, as referred in Fig. 8.3.

VI. **Operations Management Controls:** Operations management is responsible for the daily running of hardware and software facilities so that production application systems can accomplish their work and development staff can design, implement, and maintain application systems. Operations management typically performs controls over the functions as discussed in Fig. 8.3.

VII. **Quality Assurance Management Controls:** Quality Assurance management is concerned with ensuring that the –

- ❖ Information systems produced by the information systems function achieve certain quality goals.
- ❖ Development, implementation, operation, and maintenance of Information systems comply with a set of quality standards.

Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –

- ❖ Quality goals are established and understood clearly by all stakeholders.
- ❖ Compliance occurs with the standards that are in place to attain quality information systems.

Best practices in the industry are also incorporated during the production of information systems including detailed knowledge transfer sessions, quality matrix.

Fig. 8.3: The Management Control Framework

Top Mgt. Controls: Functions performed by Senior Management that includes **Planning** to determine goals of information systems function and means of achieving goals; **Organizing** to gather, allocate, coordinate the resources needed to accomplish goals, **Leading** to include activities like Motivate, guide, and communicate with personnel; and **Controlling** to compare actual with planned performance.

Systems Development Management Controls: Responsible for functions like analyzing, designing, building, implementing, maintaining IS. This includes **Problem definition and Feasibility Assessment** to find possible solutions and their economic justification to resolve problems, **Analysis of existing system** to study the existing structure, culture of the system, existing product & information flows, **Information processing system design** involving elicitation of detailed requirements, design of data flow, database, user interface, physical design, h/w and s/w platform etc., **H/w & S/w acquisition & procedures development** wherein vendors are selected based on evaluation criterion, **Acceptance testing & conversion** to identify deficiencies in the system before its release, **Operation and Maintenance** in which new system run as production system & maintenance activities monitored carefully.

Programming Mgt. Controls: To acquire & implement high-quality programs. Includes phases **Planning** that estimates the required resources for s/w development, **Design** involves systematic approach to program design, **Coding** use Top-down, Bottom-up approach, **Testing** to ensure developed program achieves its goals, **Operation & Maintenance** to monitor status of operational programs so that maintenance can be identified on timely basis & **Control** phase that monitors progress against all phases using WBS, Gantt Charts, PERT.

Data Resource Management Controls: Data must be available to users at a location and form in which it is needed, data is modifiable & data integrity is preserved etc. Includes controls like **Definition Controls** to comply with database definition standards, **Existence Controls** to ensure existence of database after data loss, **Access Controls** prevent unauthorized access, **Update Controls** to restrict update of database to authorized users only, **Concurrency controls** to overcome data integrity problems **& Quality Controls** to ensure accuracy, completeness, & data consistency.

Security Management Controls: Ensure that IS assets are secure, recoverable after disaster occurs. Includes **DRP** (how to recover from disaster & returns to normalcy) & **Insurance** (protection against losses).

Quality Assurance Management Controls: To achieve quality goals & IS comply with set of quality standards.

Operations Management Controls: Responsible for daily running of h/w and software computer, n/w operations, file library etc. Includes **Computer Operations** to directly support daily execution of test or production systems on h/w or s/w platform, **Network Operations** involve functioning of n/w operations, monitoring communication channels, devices etc., **Data Preparation & Entry** include keyboard environments designed to promote speed/accuracy to maintain wellbeing of operators, **Production Controls** include functions like receipt/dispatch of I/O; job scheduling; mgt. of SLAs etc., **File Library** includes mgt. of storage media, **Documentation and Program Library** ensures documentation stored securely; up-to-date & adequate backup exists, **Technical support** assist end-users to employ h/w & s/w, **Capacity Planning & Performance Monitoring** to identify resource deficiencies and **Management of Outsourced** Operations to carry out day-to-day monitoring of outsourcing contracts.

Fig. 8.4: The Application Control Framework

Boundary Controls: Involves access control mechanism. This involves **Cryptographic Controls** to transform data into codes that are meaningless for a non-authenticated person, **Access Controls** that involves 3 steps: Identification, Authentication, Authorization**; PIN** is a random number stored in database, **Digital Signatures** to establish authenticity of e-documents, **Plastic Cards** to store information required in an identification process.

Input Controls: Ensure accuracy of data to be inputted into application system. This includes **Data Code Controls** to reduce user error during data feeding, **Batch Controls** to prevent/detect errors in batch, **Validation of Data input Controls** detect errors in transaction data before data are processed.

Processing Controls: To compute classify, sort and summarize data. This includes **Processor Controls** to reduce expected losses from errors & irregularities associated with processors, **Real Memory Controls** to detect/correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access, **VM Controls** that maps VM addresses into real memory addresses, **App. S/w Control** to validate checks to identify errors during data processing.

Database Controls: To protect integrity of database when app. s/w act as interface b/w user & database. This includes **Access Controls** to prevent unauthorized access & use of data, **Integrity Controls** to ensure accuracy, completeness, and uniqueness of instances, **Application S/w Controls** that involve Update and Report Controls, **Concurrency Controls** that handles cases of concurrency and deadlock, **Cryptographic Controls** used to maintain data integrity**, File Handling Controls** to prevent accidental data destruction on storage medium.

Communication Controls: Discuss exposures in communication subsystem, controls over physical components, & channel access controls. **Physical Component Controls** to mitigate effects of exposures, **Line Error Controls** to detect/correct error of attenuation/distortion, **Flow Controls** to control rate at which data flows b/w users, **Link Controls** to manage link b/w two nodes in a network, **Topological Controls** to specify location & way nodes are linked, **Channel Access Controls** to handle contention in channel, **Control over Subversive threat** require data to be rendered useless in case of intrusion, **Internetworking Controls** to control network connecting devices.

Output Controls: Ensure data delivered to users is presented, formatted, delivered consistently. It includes **Inference Controls** to prevent compromise of statistical database, **Batch output production and distribution controls** include controls over file spooling, printing controls, report distribution controls, storage controls etc., **Batch Report Design controls** to ensure compliance with control procedures laid during the output, **Online output production and Distribution Controls** deal with establishing the output at source, distributing, communicating, receiving, viewing, retaining and destructing output.

B. The Application Control Framework: The objective of application controls is to ensure that data remains complete, accurate and valid at all levels including input, updation, 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. For example, a counter clerk at a bank is required to enter user master data in system, will not be allowed to exit unless all mendatory fields are captjred in application system.

Application 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. Boundary Controls: The major controls of the boundary system are the access control mechanisms that link the authentic users to the authorized resources they are permitted to access. The boundary subsystem establishes the interface between the would-be user of a computer system and the computer itself. Major Controls at the Boundary subsystem is shown in Fig. 8.4.

II. Input Controls: Data that is presented to an application as input data must be validated for authorization, reasonableness, completeness, accuracy, and integrity. These controls are designed to ensure the accuracy and completeness of data and instruction entered into an application system. Input controls are important and critical since substantial time is spent on input of data, and when data is entered manually through human intervention is prone to error and fraud. Its types are shown in the Fig. 8.4.

III. Communication Controls: These controls are designed at 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, and audit trail controls. Some communication controls are shown in the Fig. 8.4.

IV. 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. Some of these controls are shown in Fig. 8.4.

V. **Database Controls :** These controls are used within application software to maintain the integrity of data, to prevent integrity violations when multiple programs have concurrent access to data, and the ways in which data privacy can be preserved within the database subsystem. Various types of database controls are shown in Fig. 8.4.

VI. **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. Various Output Controls are shown in Fig. 8.4.

8.3.4 Classification based on "Control Activities"

As discussed earlier, control activities are the policies and procedures used to ensure that appropriate actions are taken to deal with the organization's identified risks. These can be grouped as shown in the Fig. 8.5.

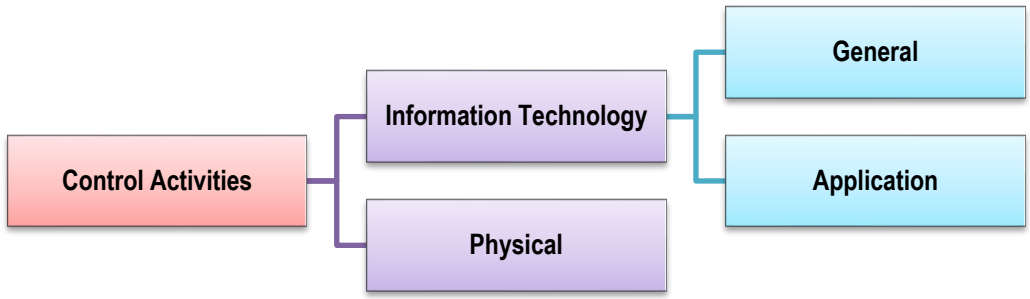


Fig. 8.5: Classification based on "Control Activities"

General controls apply to all system across the organization and, not related to any specific application. These controls are designed to ensure the system integrity, and are not designed to control specific transaction. General controls are basic controls which will be required to support the functioning of all other application control.

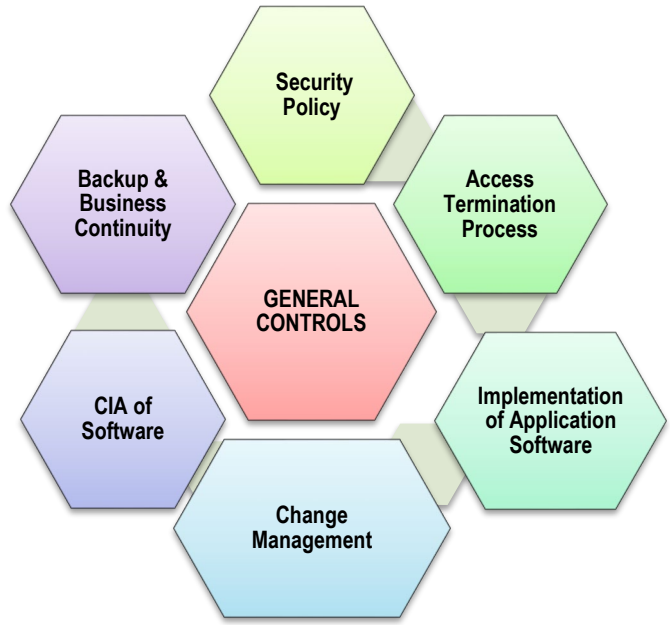


Fig. 8.6: General Controls

General IT controls include following, but are not limited to the following:

- **Information Security Policy:** An Information Security policy is the statement of intent by the senior management about how to protect a company's information assets. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization. The security policy is approved by the senior management and encompasses all areas of operations and drives access to information across the enterprise and other stakeholders.
- **Administration, Access, and Authentication:** Access controls are measures taken to ensure that only the authorized persons have access to the system and the actions they can take. IT should be administered in line of approved security policies and procedures clearly defining the levels of access to information and authentication of users.
- **Separation of key IT functions:** Secure deployment of IT requires the organization to have separate IT Department with key demarcation of duties for different personnel within IT department and to ensure that there are no Segregation of Duties (SoD) conflicts.
- **Management of Systems Acquisition and Implementation:** Management should establish acquisition standards that address the security, functionality, and reliability issues related to systems acquisition. Hence, the process of acquisition and implementation of systems should be properly controlled.

- **Change Management:** Deployed IT solutions and their various components undergo change due to changes in technology environment, business processes, regulatory, requirements, compliance requirements and changing needs of the users. These changes impact the IT environment of the organization. Hence, a change management process should be implemented to ensure smooth transition to new environments covering all key changes including hardware, software, and business processes. All changes must be properly approved by the management and tested before implementation.
- **Backup, Recovery and Business Continuity:** Heavy dependence on IT and criticality makes it imperative that resilience of the organization operations should be ensured by having appropriate business continuity including backup, recovery, and off-site data center. Business continuity controls ensure that an organization can prevent interruptions (violations) and processing can be resumed in an acceptable period of time.
- **Proper Development and Implementation of Application Software:** Application software drives the business processes of the organizations. These solutions in case developed and implemented must be properly controlled by using standard software development process. Controls over software development and implementation ensure that the software is developed according to the established policies and procedures of the organization. These controls also ensure that the systems are developed within budgets, within budgeted time, security measures are duly incorporated, and quality and documentation requirements are maintained.
- **Confidentiality, Integrity and Availability of Software and data files:** Security is implemented to ensure Confidentiality, Integrity, and Availability (CIA) of information. **Confidentiality** refers to protection of critical information to ensure that information is only available to persons who have right to see the same. **Integrity** refers to ensuring that no unauthorized alterations are made in data in all stages of processing. **Availability** refers to ensuring availability of information to users when required.
- **Incident response and management:** Thereare various incidents in system due to failure of any IT controls. These incidents need to be appropriately responded to and managed as per pre-defined policies and procedures.
- **Monitoring of Applications and supporting Servers:** The Servers and applications running on them are monitored to ensure that servers, network connections and application software along with the interfaces are working continuously without downtime.
- **Value Added areas of Service Level Agreements (SLA):** SLA with vendors is regularly reviewed to ensure that the services are delivered as per specified performance parameters.

- **User training and qualification of Operations personnel:** The personnel deployed have required competencies and skillsets to operate and monitor the IT environment. These competencies should be consistent with the defined roles. Moreover, training may be used as a tool to develop the competencies and skillsets to work in an IT environment.

It is important to note that proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls. In later sections, detailed risk, and control matrix for various types of general controls are provided.

Application Controls and Physical Controls are explained earlier in this context.

8.4 ROLE OF AUDITORS WHILE INSPECTING THE CONTROLS

The attack on the World Trade Centre in 2001 and COVID 19 outbreak has created a worldwide alert bringing focus on business continuity planning and environmental controls. Inspection 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.

I. **Inspecting Environmental Controls:** Inspection of environmental controls requires the IS auditor to conduct physical inspections and observe practices. Reviewing environmental controls requires knowledge of building mechanical and electrical systems as well as fire codes. The IS auditor needs to be able to determine if such controls are effective and if they are cost-effective and are operative throughout the period. Auditing environmental controls requires attention to these and other factors and activities, including:

   - **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, line conditioners, surge protectors, or motor generators, are used, inspected, and maintained and if this is performed by qualified personnel.
   - **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. S/he should examine maintenance records to see how frequently these components are maintained and if this is done by qualified personnel.
   - **Heating, Ventilation, and Air Conditioning (HVAC):** The IS auditor should determine if HVAC systems are providing adequate temperature and humidity levels, and if they

are monitored. Also, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.

- **Water detection:** The IS auditor should determine if any water detectors are used in rooms where computers are used. He or she should determine how frequently these are tested and if they are monitored.
- **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if they are tested. S/he should determine how frequently fire suppression systems are inspected and tested, and if the organization has emergency evacuation plans and conducts fire drills. The IS auditor may also check refilling status of fire extinguishers installed around Data center / DR site.
- **Cleanliness:** The IS auditor should examine data centers to see how clean they are. IT equipment air filters and the inside of some IT components should be examined to see if there is an accumulation of dust and dirt.

II. **Inspecting Physical Access Controls:** The inspection of 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 activities:

- **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.
- **Review of Documents:** The auditor may examine relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams to check that they are in compliance with the organizations policies.
- **Controls Assessment:** The auditor should check whether risk assessment is done by management which would evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks. This may include the following activities:
  - **Sitting and Marking:** Auditor may review building layout, sitting arrangements and location of data center and Disaster recovery site. This will require attention to several key factors and features, including natural and manmade hazards to dams; rivers, lakes, and canals; natural gas and petroleum pipelines; water mains and pipelines; earthquake faults; areas prone to landslides; volcanoes; severe weather such as hurricanes, cyclones, and tornadoes; flood zones; military bases; airports; and railroads.

- ❖ **Physical barriers:** This includesreview of fencing, walls, barbed/razor wire, and crash gates which are used to control access to the facility and determination of their effectiveness.
- ❖ **Surveillance:** This includes review of video and human surveillance which are used to control and monitor access, and if it is effective in preventing or detecting incidents or not.
- ❖ **Guards and dogs:** This includes examination of processes, policies, procedures, and records to understand the required activities used to evaluate the effectiveness of security guards and guard dogs and how they are carried out.
- ❖ **Key-Card systems:** This includes review of card systems which are used to control access to the facilities like work zones and answers the questions like - whether the facility is divided into security zones and which persons are permitted to access which zones whether key-card systems record personnel movement or not; what processes and procedures are used to issue keycards to employees, etc.

III. Inspecting Logical Access Controls

- ○ **Network Access Paths:** This includes an independent review of the IT infrastructure to map out the organization's logical access paths. This will require considerable effort and may require the use of investigative and technical tools, as well as use of external specialized experts on IT network architecture.
- ○ **Documentation:** This will include review of any discrepancies that may exist and to identify all the documented and undocumented access paths to functions and data.
- ○ **User Access Controls:** Inspecting user access controls requires attention to several factors like authentication mechanism, access violations, use account lockout, intrusion prevention and detection system logs, dormant and shared accounts, usage, and system admin accounts logs, etc.
- ○ **Password Management:** This will include review of password configuration settings on information systems as to determine how passwords are controlled. Some of the areas requiring examination include determination of how many characters must a password have and whether there is a maximum length defined; how frequently passwords to be changed; whether old passwords can be used again; whether the password is masked when logging in or when creating a new password,etc.

- **User Access Provisioning:** The review of the user access provisioning process requires attention to several key activities, including access request processes and approvals, new employee provisioning, segregation of duties, access reviews, etc.
- **Employee Terminations:** This will include review of removal of access to all IT system, NOC from various departments. Back up of personal data stored on system, etc.
- **User Access Logs:** This will include review of user access logs to check what events are recorded in access logs, are the logs aggregated or are stored in individual systems, can access logs be modified / altered, destroyed or attacked to cause the system to stop logging events, how and when the access logs are reviewed and who review them, are the access logs retained by the organization or are backed up and what actions are take when necessary.
- **Investigative Procedures:** In some cases, if auditors is assigned with investigation role then auditor needs to identify non-compliance of any IT policies and procedures, use techniques to identify computer crime investigations, and computer forensics.
- **Internet Points of Presence:** The IS auditor who is performing a comprehensive review of an organization's system and network system needs to perform a "points of presence" audit to discover what technical information is available about the organization's Internet presence. Some of the aspects of this intelligence gathering include search engines, social networking and online sales sites, domain names, etc.

IV. Inspecting Management Control Framework (Refer Table 8.8)

Table 8.8: Inspecting Top Management Controls

Planning	Whether top management has formulated a high-quality information system plan and Policies that are appropriate to the scale of organization.
Organizing	Whether proper organization chart is prepared assigning roles and responsibilities at each level.
Leading	Whether top management are prompt in dealing with any technical development in industry and how it is responded including the latest cyber threats.
Controlling	Focus on subset of the control activities to be performed by top management to evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

Systems Development Management Controls	
Concurrent Audit	As a member of the system development team, the auditors need to assist the team in improving the quality of systems development for the specific system they are building and implementing. The Auditor may guide that required controls are built into the system at development stage.
Post - implementation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating the current status of the system in terms of attaining asset safeguarding, data integrity, system effectiveness and system efficiency objectives so that the decision on whether the system needs to be scrapped, continued, or modified in some way can be taken.
General Audit	To check whether there is continuous system of IS audit once the system is developed to evaluate the quality of overall systems development process. This review allows them to make judgments on the likely quality of individual application systems developed by the system development management subsystem, the control risk associated with this subsystem, and to determine whether the extent of substantive testing needed to form an audit opinion about management's assertions relating to the systems effectiveness and efficiency, can be reduced or not. An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. Organisation may use resources from their own Internal auditors team or generally participate in the development of material application systems or undertake post-implementation review of the system.
Programming Management Controls	
Planning	♦ They should evaluate whether nature of and extent of planning are appropriate to different types of software that are developed or acquired. ♦ They must evaluate how well the planning work is being undertaken.
Control	♦ This will include review of control activities undertaken are appropriate for the different types of software that are developed or acquired. ♦ They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current software development and acquisition projects carried out at different locations in the organization, they are auditing.
Design	♦ Auditors should find out whether programmers use some type of systematic approach to design.

	♦ Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	♦ Auditors should seek evidence – • On the level of care exercised by programming management in choosing a module implementation and integration strategy. • To determine whether programming management ensures that programmers follow structured programming conventions. • To check whether programmers employ automated facilities to assist them with their coding work.
Testing	♦ Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. ♦ Auditors are primarily concerned with the quality of integration testing work carried out by information systems professionals rather than end users. ♦ Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	♦ Auditors need to ensure effective and timely reporting of maintenance needs that occur so that maintenance is carried out in a well-controlled manner. ♦ Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.
Data Resource Management Controls	
♦ Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls. ♦ Auditors might employ test data to evaluate whether access controls and update controls are working. ♦ Auditors might interview the Data Administrator (DA) and Database Administrator (DBA) to determine the procedures used by them to monitor the database environment. ♦ Auditors need to assess how well the DA and DBA carry out the functions of database definition, creation, redefinition, and retirement.	
Security Management Controls	
♦ Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; ♦ Auditors need to evaluate the performance of BCP controls. The BCP 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 to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. ♦ Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place or not; and ♦ Auditors check whether the organizations have opted for an appropriate insurance plan or not. ♦ Auditor needs to check how security incidents are identified, handled and reported to regulating authorities such as SEBI/RBI as per the requirement of CERT-In
Operations Management Controls
♦ Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel. ♦ Auditors can use interviews, observations, and review of documentation to evaluate- o the activities of documentation librarians; o how well operations management undertakes the capacity planning ad performance monitoring function; o the reliability of outsourcing vendor controls; o whether operations management is monitoring compliance with the outsourcing contract; and o Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.
Quality Assurance Management Controls
♦ Auditors might use interviews, observations, and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role. ♦ Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation. ♦ Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

V. Inspecting Application Control Framework (Refer Table 8.9)

Table 8.9: Inspecting Application Control Framework

Boundary Controls
♦ To determine how well the safeguard assets are used and preserve data integrity by verification of PAM – Privilege Access Management. ♦ To determine whether the access control mechanism implemented in that system is sufficient or not by review of Access control matrix. ♦ To ensure that careful control must be exercised over maintenance activities, in case of hardware failure by ensuring proper session log in and log out during maintenance.

- To address three aspects to assess cryptographic key management - how keys will be generated and distributed to users, and how they will be installed in cryptographic facilities?
- To ensure that rules in Firewall and network architecture is adequate.

Input Controls

- To analyze what and how the data will be captured and by whom, how the data will be prepared and entered into the computer systems and how the document will be handled, stored and filed.
- To examine the data-entry screens used in an application system and validation rules for data entered. Auditor should check validation made in application for auto correct/ rejection option provided while entering the data. For example PIN code field should only have 6 digit numeric field only.
- To evaluate the quality of the coding systems used in application system to determine their likely impact in the data integrity, effectiveness, and efficiency objectives.
- To comprehend various approaches used to enter data into an application system and their relative strengths and weaknesses. Auditor may review system user manual or SOP to identify gaps if any.
- To check whether input files are stored securely and backup copies of it are maintained at an offsite location so that recovery remains unaffected in case system's master files are destroyed or corrupted. Ensure that auto backup is scheduled in system without manual intervention.

Communication Controls

- To adopt a structured approach to examine and evaluate various controls in the communication subsystem.
- To collect enough evidence to establish a level of assurance that data transmission between two nodes in a wide area network is being accurate and complete by review of Downtime records maintained by IT department.
- To check whether adequate network backup and recovery controls are practiced regularly or not. These controls may include automatic line speed adjustments by modems based on different noise-levels, choice of network topology, alternative routes between sender and receiver, etc., to strengthen network reliability. Auditor should also ceck whether alternate back up network communication lines are available and periodically switching is done between network line.
- To assess the implementation of encryption controls to ensure the protection of privacy of sensitive data.
- To assess the topological controls to review the logical arrangement of various nodes and their connectivity using various internetworking devices in a network.

Processing Controls

- To determine whether user processes can control unauthorized activities like gaining access to sensitive data or not.
- To evaluate whether the common programming errors that can result in incomplete or inaccurate processing of data have been taken care or not.

♦ Auditor may enter data in test server to ensure desired output is received after processing the data. ♦ To assess the performance of validation controls to check for any data processing errors. ♦ To check for the checkpoint and restart controls that enable the system to recover itself from the point of failure. The restart facilities need to be implemented well so that restart of the program is from the point the processing has been accurate and complete rather than from scratch.
Database Controls
♦ To check for the mechanism if a damaged or destroyed database can be restored in an authentic, accurate, complete, and timely way. To check controls at Disaster Recovery (DR) site and ensure replica of database is available on real time basis. ♦ To comprehend backup and recovery strategies for restoration of damaged or destroyed database in the event of failure that could be because of application program error, system software error, hardware failure, procedural error, and environmental failure. Auditor can also check whether operation is shifted periodically to DR site. ♦ To evaluate whether the privacy of data is protected during all backup and recovery activities. Auditor can check privacy policy. ♦ To check for proper documentation and implementation of the decisions made on the maintenance of the private and public keys used under cryptographic controls. ♦ To address the concerns regarding the maintenance of data integrity and the ways in which files must be processed to prevent integrity violations.
Output Controls
♦ To determine what report programs are sensitive, who all are authorized to access them and that only the authorized persons are able to execute them. ♦ Auditors should review that the action privileges that are assigned to authorized users are appropriate to their job requirement or not. Auditor can check the job profile and relevant report menu access provided in Application. ♦ Auditors must evaluate how well the client organizations are provided controls in terms of alteration of the content of printer file, number of printed copies etc. Auditor can check whether external emails outside organization network are restricted. ♦ Auditors should determine whether the report collection, distribution and printing controls are well executed in an organization or not. Auditor can check whether all prints are directed to centralized printer.

SUMMARY

In this chapter, the Internal control framework has been discussed in detail. An internal control framework is a structured guide that organizes and categorizes expected controls or control topics.

Furthermore, the chapter deals with controls and their classification based on various parameters. The importance of these controls and how these are to be implemented to safeguard the information systems in an organization are covered vastly in the chapter. Furthermore, how these controls are to be inspected to ensure the proper implementation of these controls in an organization's working environment.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Identify from the following controls of Information System that deals with framing of high-level IT policies, procedures, and standards on a holistic view.

   (a) Management Controls

   (b) Environmental Controls

   (c) Access Controls

   (d) Physical Controls

2. Mr. Amit is an auditor of a company XYZ Ltd. While evaluating controls over ERP systems, he had to audit the controls which were administered through the computer center/computer operations group and the built-in operating system controls. Which of the following controls are referred here?

   (a) Environmental Controls

   (b) Application controls

   (c) Management Controls

   (d) Audit Controls

3. Mr. Y used duplicate keys to enter in prohibited area zone of JKH Ltd. company and stole some important documents of the company. Which of the following controls you think has been compromised to make such an incident happen?

   (a) Environmental Control

(b) Physical Access Control

(c) Network Access Control

(d) Logical Access Control

4. Output Controls are responsible to ensure that the data delivered to users will be presented, formatted, and delivered in a consistent and secured manner. Which of the following activity does not fall under the purview of Output Control?

(a) Spooling

(b) Report Distribution Control

(c) Asset Safeguarding

(d) Control over printing

5. The Quality Assurance Management controls involve various functions that ensure that the development, implementation, operation and maintenance of information systems conform to quality standards. With such scope of the controls in mind, what do you think is not true about Quality Assurance Management Controls?

(a) Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.

(b) Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.

(c) Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

(d) Auditors check whether the organizations that have been audited have appropriate, high-quality disaster recovery plan in place or not.

ANSWERS/SOLUTIONS

1.	(a)	2.	(a)	3.	(b)	4.	(c)	5.	(d)

CHAPTER 9

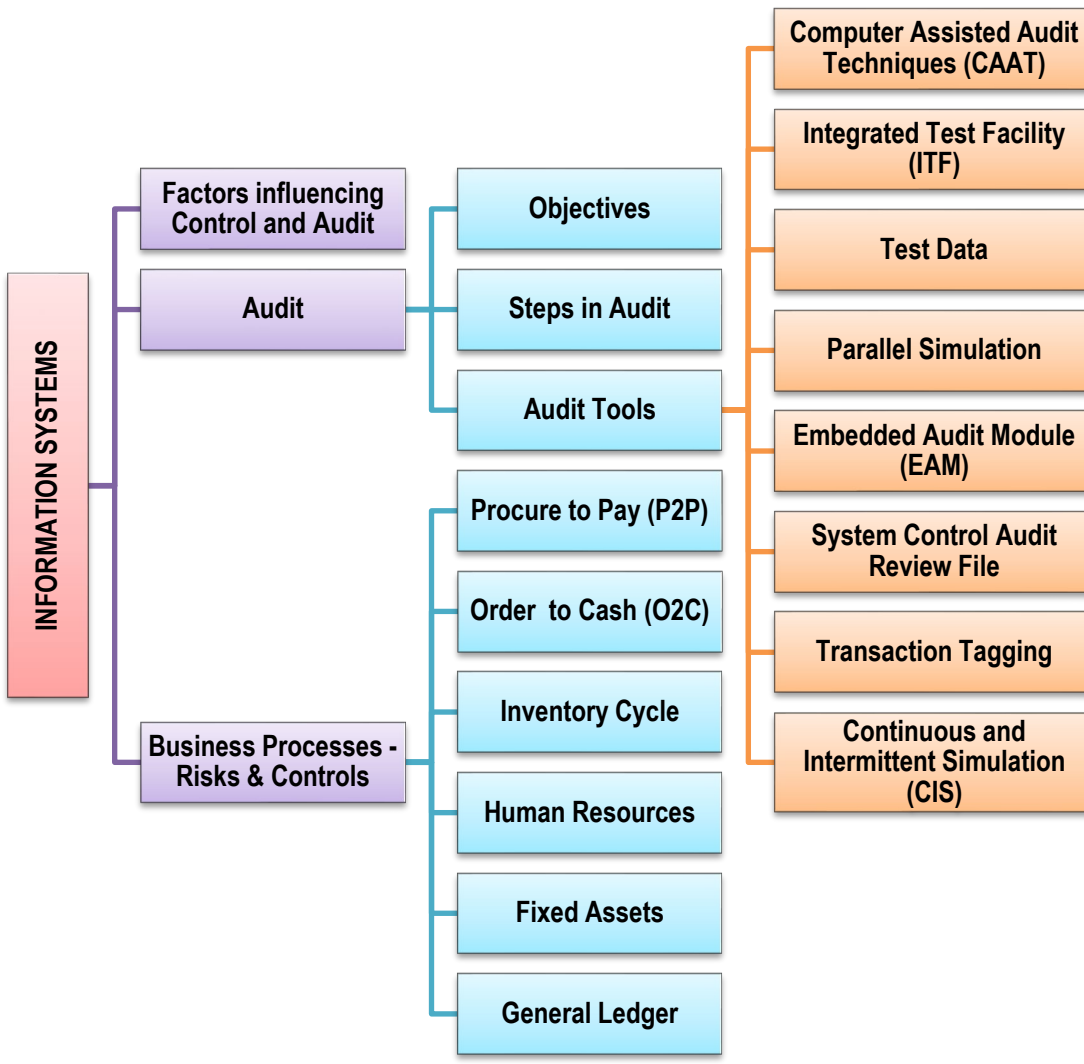
INFORMATION TECHNOLOGY TOOLS

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- distinguish between Information Systems and Information Technology.
- understand the factors influencing Information systems Audit and its objectives.
- understand all the steps involved in an Information Systems Audit (ISA).
- gain an overview of Information Technology Tools.
- comprehend about working of several Information Technology Tools.
- understand about various risks and their controls through illustrations on several business processes.
- comprehend the risks and controls of specific business processes like Procure to Pay (P2P), Order to Cash (O2C), Current Account and Savings Account (CASA) of Core Banking Systems (CBS).

CHAPTER OVERVIEW



9.1 INTRODUCTION

Information Technology (IT) has improved its control and influence every area of business inclusive of processing and auditing of information.

- IT enhanced the ability to store, process and analyse the information and to expand the power of business decision maker.
- IT has impact on the control process of business environment. The control objectives of business processes remain constant however the technology has changed the way in which systems should be controlled.
- IT has also influenced the Chartered Accountancy profession in every manner, for example it influences how the audit is being conducted including drawing of samples and generation of system report, verification of internal controls and efficiency and effectiveness of system alon with integrity of adit report.

Information technology has become an integral part of most organizational functions. It is likely that many organization either have eliminated or will eliminate a substantial portion of their paper documents and replace them with electronic documents stored on system in computerized form. An auditor who is unable to use computerized audit tools and techniques effectively will be at a disadvantage.

Before proceeding further, it is essential to understand the difference between Information System and Information Technology. The Information System comprises of people, process, and Technology whereas IT component of an Information system include hardware, software, communication, and other components required to generate, process and transfer data / information.

IT tools are generally used in IT audit which is considered as independent, formal, and objective examination of IT infrastructure of an organization. IT auditing is required to evaluate the capability of application system that fulfil the processing requirement, capability of internal control and ensure the safety of assets that are controlled by these systems. Tools for auditing help to identify controls and determine their effectiveness including the standard auditing tools of internal control questionnaires, interviews, observation, and document review.

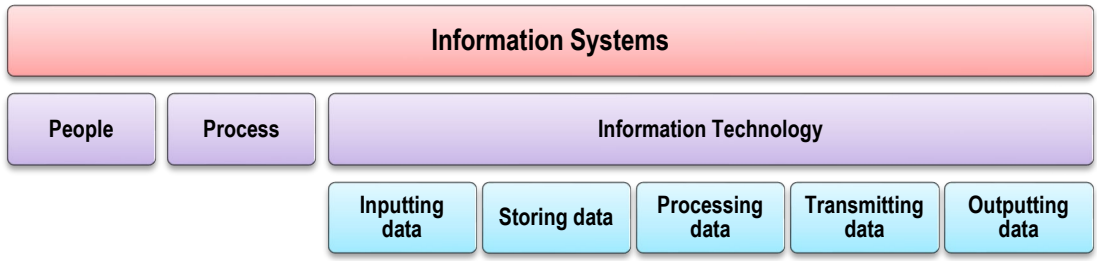


Fig. 9.1: Information Systems vs Information Technology

Information Systems comprise of various activities such as strategic, managerial, and operational that work together to gather, processing, storing, and distributing of data and information. In today's era, the IT auditor requires to have advanced knowledge and skills for continue growth progressing up the external and internal audit paths. Today almost every organization has IT audit department that assist in financial auditing, internal security auditing, internet security, etc.

9.2 CONTROL AND INSPECTION OF INFORMATION SYSTEM

It is necessary to understand the techniques and tools used to test and evaluate the application for auditing purposes. An evaluation of network reliability makes the auditor to get the answer of following:

- Who monitors performance?
- Who corrects problems?
- Who examines the network periodically?
- What problems have occurred?
- What action was taken?
- How is the network kept up-to-date?

As discussed above information system are used in every function of business. The management needs assurance that the system is functioning as per the expectation and all internal controls are operating as designed.

Design of Internal controls are dependent on many factors. Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in Fig. 9.2.

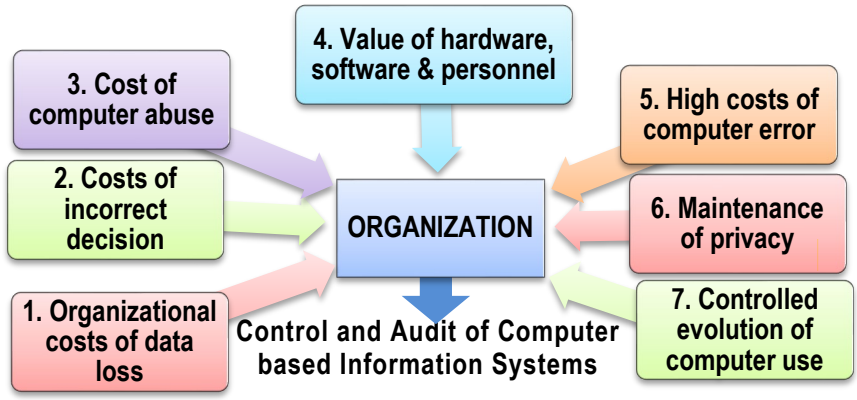


Fig. 9.2: Factors influencing an organization toward Control and Audit of computer-based Information Systems

Let us now discuss these reasons in detail (Refer Fig. 9.2):

1. **Organizational Costs of data loss:** Data is a critical resource of an organization. If the data is accurate, its ability to adapt and survive in a changing environment increases significantly. If such data is lost, an organization can incur substantial losses.

2. **Cost of Incorrect Decision making:** Making high-quality decisions are dependent on both – the reliability and integrity of the data. Decision is taken at highest levels based on MIS reports provided by middle management. The Middle management relies on the output generated by system. Any incorrect data at any level can have adverse impact on the organization as well as other stakeholders having an interest in the organization.

3. **Costs of computer abuse:** Computer abuse is defined as any incident associated with computer technology in which the user suffered or could have suffered loss and a perpetrator by intention made or could have made gain. Unauthorized access to computer systems, malwares, and unauthorized physical access to computer facilities, unauthorized copies of sensitive data, viruses, and hacking can lead to destruction of assets (hardware, software, data, information, etc.). The cost of data leakage can impact the reputation of any organization.

4. **Value of computer hardware, software and personnel:** In today's environment management has substantial investment in creating and maintaining IT infrastructure which include Hardware software and people. These are critical resources of an organization, which has a credible impact on its infrastructure and business competitiveness. The intentional or unintentional loss of hardware, the destructions or corruption of software, and non-availability of skilled computer professionals in any organization may lead to disruption of business operations.

5. **High Costs of Computer Error:** In a computerized enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage. For example -ABC trader punched an order to buy 17 lakh NIFTY 50 units instead of punching order to sell ₹ 17 lakh worth of NIFTY 50 units. The sell orders were converted into a transaction because ABC trader placed unrealistic buy order to buy NIFTY 50 stocks at price far away from the market price, without adequate margin money.

6. **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual. This data were also collected before computers but now, there are many instances in which privacy of individuals has been eroded beyond acceptable levels. Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (5) of section 8 of Digital personal data protection Act 2023 have penalty provisions of maximum up to 250 Crores.

7. **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. Governments, professional bodies, pressure groups, organizations and individual persons all must be concerned with evaluating and monitoring how we deploy computer technology. For example, MCX (Multicommodity exchange) India Limited was an associate company of 63 Moons, which held 26% of its equity. MCX was using the software platform provided by 63 Moons. MCX was forced to sell its stake in MCX following the scandal that surfaced at its subsidiary spot exchange NSEL in 2013. Due to this scam MCX was required to change the core trading platform due to non-reliability of earlier system.

9.3 INFORMATION SYSTEMS AUDITING

Information systems are the backbone of any organization; therefore, their auditing is also very important to work on. **Information Systems Auditing** is defined as the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both. Information Systems Auditing (ISA) enables organizations to better achieve some major objectives that are depicted in the Fig. 9.3:

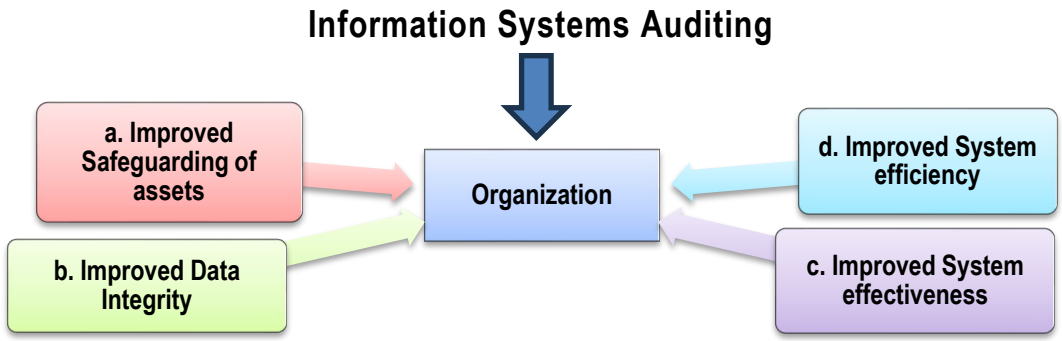


Fig. 9.3: Information Systems Auditing

a. **Improved Safeguarding of Assets:** The information system assets like hardware, software, facilities, people, data files, system documentation, information, etc. must be protected from unauthorized access. These assets are often concentrated in one or a small number of locations, such as single server. Therefore, asset safeguarding is an important objective for many organizations to achieve.

b. **Improved Data Integrity:** It is a fundamental attribute of Information System Auditing. Data has certain attributes – completeness, reliability, transparency, and accuracy. The integrity of data is to be maintained throughout data life cycle such as from capturing of the data till destruction of data as per the policy of the organizations; else an organization may suffer loss of competitive advantage. It is also important from the business perspective of the decision maker, competitive and the market environment.

c. **Improved System Effectiveness:** Evaluating effectiveness implies matching the user needs. Effectiveness of a system means whether a system reports information in a way that facilitates its users in decision- making or not. Auditors must be aware of users' requirements and decision-making environment at various levels of users to have an assurance on effectiveness of system .

d. **Improved System Efficiency:** An efficient information system uses minimum resources to achieve its required objectives, therefore the use of various information system resources like machine time, peripherals, system software and labor must be optimally utilized along with the impact on its computing environment. Before upgradation of the any systems or at implementation of new system, auditors may assist management by giving recommendation for improvement in system efficiency.

9.4 AUDITING AROUND THE COMPUTER VERSUS AUDITING THROUGH THE COMPUTER

Auditing around the computer (Blackbox auditing approach) and auditing through the computer (Whitebox auditing approach) are the two different concepts. When the automated applications are simple and straightforward, then auditing around computer is more adequate than auditing through computer.

- In the **auditing around the computer**, the auditor obtains the source document related to a particular transaction and reconciles these documents against output result. Hence, audit supporting documentation is drawn and conclusions are reached without considering how inputs are being processed to provide outputs.
- The **auditing through the computer approach** includes a variety of techniques to evaluate how the application and their embedded controls respond to various types of transactions that can contain errors. The techniques most commonly use include Integrated Test facility, Test data, Parallel Simulation, Embedded Audit Module, Systems Control Audit Review File (SCARF), and transaction tagging, etc. Again, many of these techniques should be embedded into the application for use by auditors and information security personnel. These techniques provide continuous audit and evaluation of the application or systems and provide management and the audit or security personnel assurances that controls are working as planned, designed, and implemented.
- The major weakness of the **auditing around the computer** approach is that it does not verify or validate whether the program logic of the application being tested is correct, which is the main characteristics of the **auditing through the computer** approach.

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. 9.4.

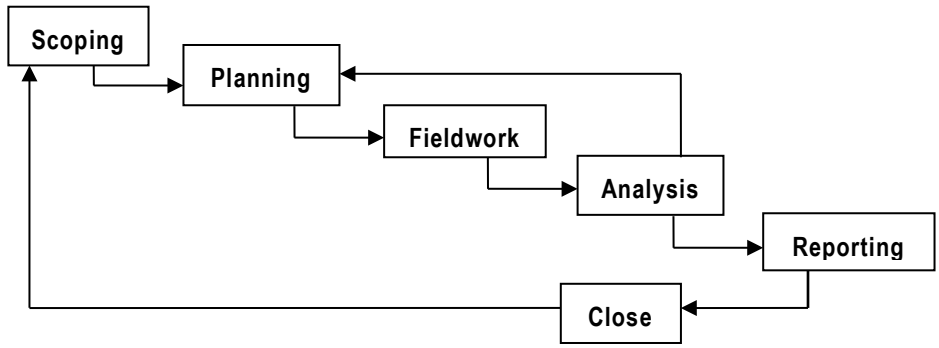


Fig. 9.4: Steps in Information Systems Audit process

(i) **Scoping and pre-audit survey:** Auditors determine the significant area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. This may includes collecting background through various sources such as from web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) **Planning and preparation:** At this stage, the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) **Fieldwork:** This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

(iv) **Analysis:** This step involves sorting out, reviewing and to arrive at conclusion from the 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 evidences and first level discussion with auditee for explanation on identified observations.

(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.

9.5 INFORMATION TECHNOLOGY TOOLS

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 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 is 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. Auditors should understand all tools and techniques that can be used to test all the business processes of a computerized system by processing and analyzing the data of these computerized files.

In today's world, it is a necessity that an auditor should understand alternative tools and techniques to test the operations of computerized systems and gather and analyse data contained in computerized files. While dealing with large volume of information, these automated techniques have proven to be better than manual. Automation helps to evaluate greater volumes of data and quickly perform analysis on data to gather a broader view of a process. The person who inspects or checks can take advantage of these tools to be more efficient and effective while performing audit work.

Some common tools used for analysing data are Microsoft Access, Microsoft Excel and SAP Audit Management, etc.

- **Microsoft Access** can be used to analyze data, create reports, and query data files.
- **Microsoft Excel** also analyzes data, generates samples, creates graphs, and performs regression or trend analysis.
- **SAP Audit Management** facilitates the documentation of evidence, organization of working papers, and creation of audit reports. This technique also provides analytical capabilities to shift the focus of audits from basic assurance to providing insight and advice.

I. **Computer Assisted Audit Techniques (CAATs):** When adequate application controls are identified in an Information System, the IT auditor performs tests to verify their design and effectiveness. When controls are not adequate, IT auditors perform extensive testing to verify the integrity of the data. To perform tests of applications and data, an auditor may use CAAT. CAATs are the practice of using computers to automate the IT audit processes.

CAAT is useful to both IT and financial auditors in a variety of ways to evaluate the integrity of an application, determine compliance with procedures, and continuously monitor processing results. IT auditors can review applications to expand an understanding of the controls in place to ensure the accuracy and completeness of the information generated.

Common CAATs such as Audit Command Language (ACL) and Interactive Data Extraction and Analysis (IDEA) can be used to select a sample, analyse the characteristics of a data file, identify trends in data, and evaluate data integrity.

A large part of the professional skills required to use CAATs lies in planning, understanding, and supervising. The computer has a broad range of capabilities. There is a variety of CAATs that are useful when auditing applications and data integrity. For example - Generalized audit software can be used to analyse the spreadsheet logic and calculations for accuracy and completeness, evaluate data produced from applications, and produce logical data flowcharts. The activities involved under generalized audit software are to:

- analyze and compare files;
- select specific records for examination;
- conduct random samples;
- validate calculations;
- prepare confirmation letters; and
- analyze aging of transaction files.

IT auditors also use these software techniques for testing and/or documentation of selected processes within the IT environment in the form of flowcharts, and data flow diagrams, for instance. Example of the most popular software packages includes Audit Analytics by Arbutus Software, CaseWare Analytics IDEA Data Analysis, Easy2Analyse, TeamMate Analytics, etc.

Refer Table 9.1 to know about Traditional audit vs CAATs.

Table 9.1: Traditional audit vs CAATs on specific risks

Consider an example of an insurance company.

Using traditional audit techniques, the risk of paying any claims even after a policy is terminated would be very difficult to test. The auditor would "randomly select" a "statistically valid" sample of 30-50 claims which would provide a clear understanding of the situation is highly unlikely.

Using CAATs, the auditor can select every claim that had a date of service after the policy termination date. Using CAATs, the auditor is able to identify every claim that was paid,

and the exact amount incorrectly paid by the insurance company. The auditor can then figure out why the controls to prevent this failed.

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 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 must 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. This technique can be used on large scale to serve multiple locations of the organization. Auditors can submit transactions to test the system throughout the financial period. The test facility is composed of a fictitious company or branch, set up in the application and file structure to accept or process test transactions as though it was an actual operating entity. Fig. 9.5 provides an outline about the advantages and disadvantages of ITF and Table 9.2 provides its example.

Advantages

- This facility is designed into the application during system development.
- Designed into the application during system development.

Disadvantages

- Expertise is required to design the audit modules (built-in test environments) into the application and to ensure that test transactions do not affect actual data.
- Since the audit module is set up in the organization or client application, the risk of disrupting the data is high.
- Controls must be adequately designed and implemented to identify and remove the effects of test transactions.

Fig. 9.5: Advantages and Disadvantages of ITF

Table 9.2: Example of ITF Implementation

ABC Ltd. is a company having a team of Information Systems Auditors and deal with assignments related to IS Auditing. One of the major clients of ABC Ltd. is ManuTree dealing in mutual fund services.

To audit ManuTree's accounting system, Mr. Suresh, an IS Auditor provided an audit facility consisting of program, code, or additional data to be embedded and incorporated into the computer element of the client's accounting system.

Using ITF, a fictitious entity was created, for example a customer, within the context of the regular application. Transactions are then posted to the fictitious entity together with regular transactions and the results produced by the normal processing cycle are

then compared with predetermined results. Such entries should be reversed at defined cut-off dates to ensure that they are not included in the financial reports.

Conclusion: The ITF enabled Mr. Suresh, the auditor and the client's management to check continuously on the internal processing functions.

III. **Test Data:** This technique involves methods of providing test transactions to a system for processing by existing applications. Test data provides a full spectrum of transactions to test the processes within the application and system. Both valid and invalid transactions should be included in the test data as the objective is to test how the system processes both correct and erroneous transaction input. Let us consider the consumer credit card service. Many transactions in this case may involve invalid account numbers, accounts that have been suspended or deleted, and others. If reliance is placed on program, application, or system testing, some form of intermittent testing is essential. Test data generators are very good tools to support this technique but should not be relied on entirely for extreme condition testing. Fig 9.6 highlights the advantages and disadvantages of Test Data and Table 9.3 provides its example.

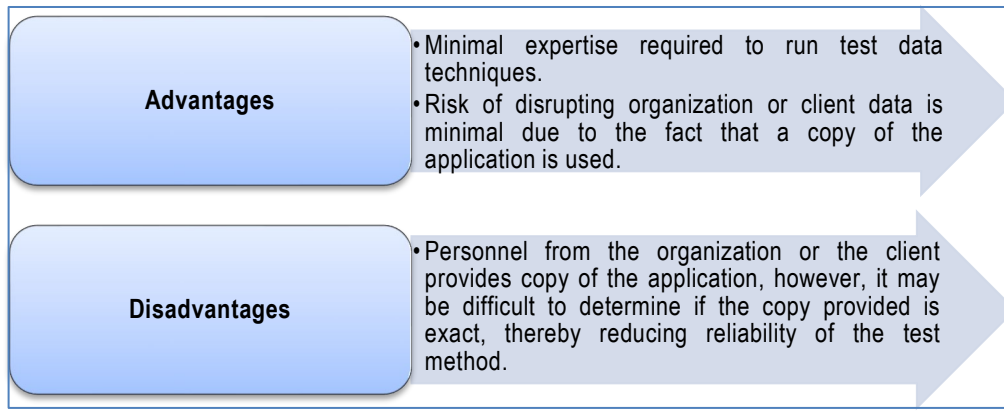


Fig. 9.6: Advantages and disadvantages of Test Data

Table 9.3: Example of Test Data

In an organization, if two dummy transactions are being processed with the probability that the transaction within the purview of parameters would be accepted else it would be rejected. If any of the transaction does not produce the expected result, them the auditor must ponder upon the requirement of applicable procedures in the area being reviewed.

IV. **Parallel Simulation:** Parallel simulation involves the separate maintenance of two presumably identical sets of programs. The original set of programs is the production copy used in the application under examination. The second set could be a copy secured by auditors at the same time that the original version was placed into production.

As changes or modifications are made to the production programs, the auditors make the same updates to their copies. If no unauthorized alteration has taken place, using the same inputs, comparing the results from each set of programs should yield the same results. Another way is for the auditor to develop pseudocode using higher-level programming languages such as SQL, JAVA, etc. from the base documentation following the process logic and requirements. For audit purposes, both software applications (test versus actual) would utilize same inputs and generate independent results that can be compared to validate the internal processing steps. Refer Fig. 9.7 to know about several advantages and disadvantages of Parallel Simulation and Table 9.4 provides its example.

Advantages	Risk of disrupting organization or client data is minimal. Simulation does not affect processing.
	Auditor obtains output information directly without intervention from organization or client personnel.
Disadvantages	Extent of to which expertise is required depends upon the complexity of the organization or client's processing being simulated.

Fig. 9.7: Advantages and Disadvantages of Parallel Simulation

Table 9.4: Example of Parallel Simulation

Let us consider an example of invoice processing. Collect a set of invoices from client's data and simulate to arrive at the expected accounting entries on invoice processing. Now compare the simulated results with that of client's system. If the results are same, the client's system control is intact. Suppose there are exceptions in the comparison, additional test procedures should be performed to identify the impact of exception.

V. Embedded Audit Module (EAM): It is the programmed audit module that is added to the application under review. The embedded module allows auditors to monitor and collect data for analysis and to assess control risks and effectiveness. The level of expertise required in this module is considered medium to high, as auditors require knowledge and skills in programming to design and implements the module. The risk of disrupting client data may be high. Because all transactions would be subjected to the module's screening algorithm, it can significantly affect the speed of processing.

For example - A company wants to ensure that all sales transactions over ₹10 lakhs are required to be authorized by a manager. An embedded audit module could be programmed into the company's sales system to flag all such transactions. Whenever a sales transaction

over ₹ 10 lakh occurs, the module records the transaction details and whether it was appropriately authorized. The auditors can then periodically review this information to identify any transactions that did not receive proper authorization.

Advantages: By providing real-time or near real-time monitoring of transactions, embedded audit modules can help detect errors, fraud, or non-compliance more quickly than traditional audit methods.

Disadvantages: However, they need to be carefully managed and secured, as they have access to sensitive system and transaction data.

Refer Table 9.5 to understand example of Embedded Audit Module.

Table 9.5: Example of an Embedded Audit Module

Suppose there's a company called "TrialFin" that processes thousands of financial transactions on daily basis. As the volume of the transactions is very high, it is impossible for internal auditors to manually check each transaction for inconsistencies or errors.

To address this, TrialFin decides to incorporate an embedded audit module in its transaction processing system. This module is programmed to look for certain indicators of fraud or error, such as:

- Transactions that exceed a certain amount, say ₹ 10 crores because these could represent a higher risk if they are incorrect or fraudulent.
- Transactions that are processed outside of normal business hours, which could be a sign of unauthorized activity.
- Transactions processed by certain high-risk or high-privilege user accounts, to ensure these are being used appropriately.

The embedded audit module tracks these transactions in real time as the system processes them. If it detects any that meet the criteria, it flags them and records relevant details in a special audit log.

The auditors periodically review the audit log to check for any flagged transactions. For each one, they would verify whether it was correct and authorized. If any issues are found, they can investigate further to understand what went wrong and how to prevent it in the future.

Through this process, TrialFin can effectively monitor its high-volume transaction processing, detect potential issues more quickly, and provide assurance that its financial

controls are working properly. The embedded audit module aids in efficient and effective auditing without disrupting the normal operations.

VI. **System Control Audit Review File (SCARF):** The SCARF technique is real time technique that 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 file. This technique may collect specific transactions that violate certain predetermined pattern like transactions that exceed a specified limit; involve inactive accounts; deviate from company policy; or contain write-downs of asset values.

To review and examine, computer forensic specialist may collect data from log files. Auditors then examine the information contained in this file to see if some aspect of the application system needs follow-up.

Usually, SCARF is used to collect the following information - Application System errors, Policy and procedural variances, System exceptions, Statistical samples, Snapshots and extended records, Data profiling, Data for performance measurement. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities. Fig. 9.8 illustrates the advantages and disadvantages of SCARF and Table 9.6 provides its example.

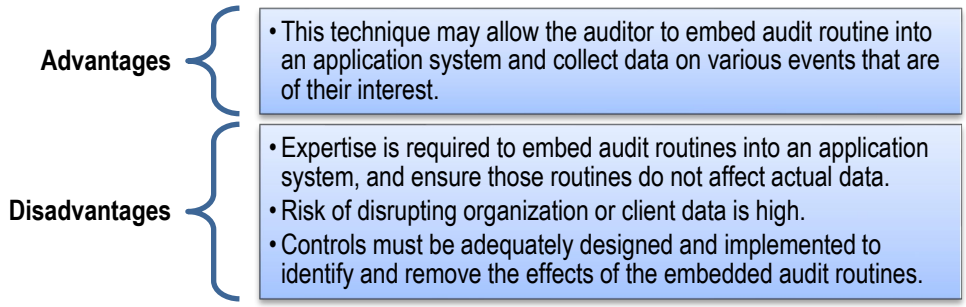


Fig. 9.8: Advantages and disadvantages of SCARF

Table 9.6: Example of SCARF

For Life insurance Company, criteria have been set that if below two conditions are satisfied, then transaction should be recorded In SCARF for subsequent review of Auditor:

- Change in the address of the customer.
- Withdrawal of fund within 7 days of change in address.

VII. **Transaction Tagging:** Transaction tagging follows a selected transaction through the application from input, transmission, processing, and storage to its output to verify the

integrity, validity, and reliability of the application. Some applications have a trace or debug function, which can allow one to follow the transaction through the application. This may be a way to ensure that the process for handling unusual transactions is followed within the application modules and code. Table 9.7 highlights the advantages and disadvantages of Transaction Tagging and Table 9.8 provides its example.

Table 9.7: Advantages/Disadvantages of Transaction Tagging

Advantages	Disadvantages
Allows auditors to log all the transactions or snapshot of activities.	Expertise required to add special designation (or tag) to the transaction record.
Tags transactions from beginning to end.	Risk of disrupting client data may be medium to high. Controls must be adequately designed and implemented to identify and remove the tag or special designation added to the transaction being.

Table 9.8: Example of Transaction Tagging

Imagine yourself to be an interior designer working with ten real estate agents that refer business to you. You might know off the top of your head which agent refers the most business, but you are not sure which clients pay the most. Let us say Mr. Amit refers an average of twenty clients per month, whereas Mr. Monty refers an average of seven clients per month. It might seem like it is most worthwhile to focus on building your relationship with Mr. Amit. However, by tagging your transactions, you discover that clients referred by Mr. Amit pay around ₹ 50K, whereas clients that come from Mr. Monty pay around ₹ 80K. The numbers speak for themselves—by tagging transactions with client name, you discover that you can make more money by building closer ties with Mr. Monty.

Thus, we can see that how transaction tagging can help us get more strategic and be instrumental in any business growth.

VIII. **Continuous and Intermittent Simulation (CIS):** This is a variation of the SCARF continuous audit technique which can be used to trap exceptions whenever the application system uses a Database Management System (DBMS). CIS is an auditing technique that simulates the instruction execution of the application at the time the application is processing a transaction. All data and input to the application is accessible by and shared with the simulation. This means that the simulation is notified about each transaction that is entered to the application and accesses to database by the DBMS.

Advantages: The CIS does not require modifications to the application system and yet provides an online auditing capability.

Disadvantages

- 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.

Refer Table 9.9 to understand example of CIS.

Table 9.9: Example of CIS

During application system processing, CIS executes in the following way:

- The DBMS reads an application system transaction which 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 DBMS.
- 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. Serious exceptions may prevent the DBMS from executing the update.

9.6 BUSINESS PROCESSES

A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal. Depending on the organization, industry and nature of work; business processes are often broken up into different categories as shown in the Fig. 9.9.

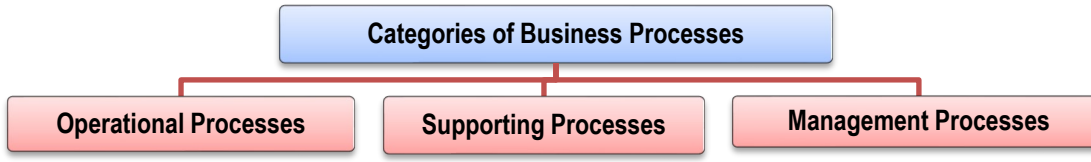


Fig. 9.9: Categories of Business Processes

I. **Operational Processes (or Primary Processes): Operational** or **Primary Processes** deal with the core business and value chain. These processes deliver value to the customer by helping to produce a product or service. Operational processes represent essential business activities that accomplish business objectives e.g. purchasing, manufacturing, and sales. Also, Order to Cash cycle (O2C) and Purchase to Pay (P2P) cycles are associated with revenue generation.

II. **Supporting Processes (or Secondary Processes): : Supporting Processes** back core processes and functions within an organization. Examples of supporting or management processes include Accounting, Human Resource (HR) Management and workplace safety. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. However, it should be noted that hiring the right people for the right job has a direct impact on the efficiency of the enterprise.

III. **Management Processes: Management Processes** measure, monitor and control activities related to business procedures and systems. Examples of management processes include internal communications, governance, strategic planning, budgeting, and infrastructure or capacity management. Like supporting processes, management processes do not provide value directly to the customers. However, it has a direct impact on the efficiency of the enterprise.

9.6.1 Business Processes - Risks and Controls

Suitable controls should be implemented to meet the requirements of the control objectives. These controls can be manual, automated, or semi-automated provided the risk is mitigated. In computer systems, controls should be checked at three levels, namely **Configuration**, **Masters,** and **Transactions** level (Table 9.10).

Table 9.10: Various levels to check control

Configuration	Masters	Transactions
Configuration refers to the way a software system is set up. Configuration is the process of defining options that are provided. When any software is installed, values for various parameters should be set up (configured) as per policies and business process workflow and rules of the enterprise. Configuration will define how software will function and what menu options are displayed to various users. Configuration can be modified based on user requirements with the use of administrative rights only.	**Masters** refer to key business data that provides context for business transactions and operations. Data designated as master data will be different for various industries. The transactions are processed based on programming done with master data The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed.	**Transactions** refer to the entries recorded in system through menus and functions in the application software. Transaction can be system generated or user generated from any specific modules. The processing of transactions in system involves initiation, authorization, or approval based on design of system.
The various modules of the enterprise such as Purchase, Sales, Inventory, Finance, User Access etc. must be configured.	Examples are Vendor Master, Customer Master, Material Master, Accounts Master, Employee Master etc.	For example: Sales transactions, Purchase transactions, Stock transfer transactions, Journal entries and Payment transactions.

9.6.2 Procure to Pay (P2P) – Risks and Controls

Procure to Pay (Purchase to Pay or P2P) is the process of obtaining and managing the materials required for manufacturing a product or providing a service. It involves the transactional flow of data that is sent to a supplier as well as the data that surrounds the fulfillment of the actual order and payment for the product or service. Using automation, it should be possible to have a seamless procure to pay process covering the complete life-cycle from point of order to payment. Figure 9.10 depicts P2P process

Fig.9.10: Procure to pay process

Masters

Table 9.11: Risks and Control Objectives (Masters-P2P)

Risk	Control Objective
Unauthorized changes to supplier master file.	Only valid changes are made to the supplier master file.
All valid changes to the supplier master file are not input and processed.	All valid changes to the supplier master file are input and processed.
Changes to the supplier master file are not correct.	Changes to the supplier master file are accurate.
Changes to the supplier master file are delayed and not processed in a timely manner.	Changes to the supplier master file are processed in a timely manner.
Supplier master file data is not up to date.	Supplier master file data remain up to date.
System access to maintain vendor masters has not been restricted to the authorized users.	System access to maintain vendor masters has been restricted to the authorized users.

Transactions

Table 9.12: Risks and Control Objectives (Transactions-P2P)

Risk	Control Objective
Unauthorized purchase requisitions are ordered.	Purchase orders are placed only for approved requisitions.
Purchase orders are not entered correctly in the system.	Purchase orders are accurately entered.
Purchase orders issued are not input and processed.	All purchase orders issued are input and processed.
Amounts are posted in accounts payable for goods or services not received.	Amounts posted to accounts payable represent goods or services received.
Amounts posted to accounts payable are not properly calculated and recorded.	Accounts payable amounts are accurately calculated and recorded.
Amounts for goods or services received are not input and processed in accounts payable.	All amounts for goods or services received are input and processed to accounts payable.
Amounts for goods or services received are recorded in the wrong period.	Amounts for goods or services received are recorded in the appropriate period.

Accounts payable amounts are adjusted based on unacceptable reasons.	Accounts payable are adjusted only for valid reasons.
Credit notes and other adjustments are not accurately calculated and recorded.	Credit notes and other adjustments are accurately calculated and recorded.
All valid credit notes and other adjustments related to accounts payable are not input and processed.	All valid credit notes and other adjustments related to accounts payable are input and processed.
Credit notes and other adjustments are recorded in the wrong period.	Credit notes and other adjustments are recorded in the appropriate period.
Disbursements are made for goods and services that have not been received.	Disbursements are made only for goods and services received.
Disbursements are distributed to unauthorized suppliers.	Disbursements are distributed to the appropriate suppliers.
Disbursements are not accurately calculated and recorded.	Disbursements are accurately calculated and recorded.
All disbursements are not recorded.	All disbursements are recorded.
Disbursements are recorded for an inappropriate period.	Disbursements are recorded in the period in which they are issued.
Adjustments to inventory prices or quantities are not recorded promptly and not done in the appropriate period.	Adjustments to inventory prices or quantities are recorded promptly and in the appropriate period.
System access to process transactions has not been restricted to the authorized users.	System access to process transactions has been restricted to the authorized users.

9.6.3 Order to Cash (O2C) – Risks and Controls

Order to Cash (OTC or O2C) is a set of business processes that involve receiving and fulfilling customer requests for goods or services. Refer Fig. 9.11 to understand O2C process.

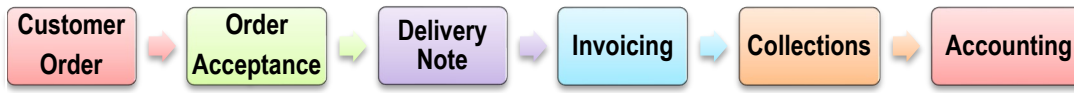


Fig. 9.11: Order to Cash Process

i. **Customer Order:** Customer order is received.

ii. **Order Acceptance:** Order is accepted as per agreed terms including delivery or service timelines .

iii. **Delivery Note:** Order is shipped to customer or service is performed.

iv. **Invoicing:** Invoice is prepared created and sent to the customer.

v. **Collections:** Funds are collected from customer for sale of goods/service .

vi. **Accounting:** Payment is recorded in General ledger.

Table 9.13: Risks and Control Objectives (Masters-O2C)

Risk	Control Objective
The customer master file is not maintained properly, and the information is not accurate.	The customer master file is maintained properly, and the information is accurate.
Invalid changes are made to the customer master file.	Only valid changes are made to the customer master file.
All valid changes to the customer master file are not input and processed.	All valid changes to the customer master file are input and processed.
Changes to the customer master file are not accurate.	Changes to the customer master file are accurate.
Changes to the customer master file are not processed in a timely manner.	Changes to the customer master file are processed in a timely manner.
Customer master file data is not up-to-date and relevant.	Customer master file data is up to date and relevant.
System access to maintain customer masters has not been restricted to the authorized users.	System access to maintain customer masters has been restricted to the authorized users.

Transactions

Table 9.14: Risks and Control Objectives (Transactions-O2C)

Risks	Control Objectives
Orders are processed exceeding customer credit limits without approvals.	Orders are processed only within approved customer credit limits.
Orders are not approved by management as to prices and terms of sale.	Orders are approved by management as to prices and terms of sale.
Orders and cancellations of orders are not entered accurately.	Orders and cancellations of orders are input accurately.
Order entry data are not transferred completely and accurately to the shipping and invoicing activities.	Order entry data are transferred completely and accurately to the shipping and invoicing activities.
All orders received from customers are not entered and processed.	All orders received from customers are input and processed.
Invalid and unauthorized orders are entered	Only valid and authorized orders are input and

and processed.	processed.
Invoices are generated using unauthorized terms and prices.	Invoices are generated using authorized terms and prices.
Invoices are not accurately calculated and recorded.	Invoices are accurately calculated and recorded.
Credit notes and adjustments to accounts receivable are not accurately calculated and recorded.	Credit notes and adjustments to accounts receivable are accurately calculated and recorded.
Goods shipped are not invoiced.	All goods shipped are invoiced.
Credit notes for all goods returned and adjustments to accounts receivable are not issued in accordance with organization policy.	Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy.
Invoices are raised for invalid shipments.	Invoices relate to valid shipments.
Credit notes do not pertain to a return of goods or other valid adjustments.	All credit notes relate to a return of goods or other valid adjustments.
Invoices are not recorded in the system.	All invoices issued are recorded.
Credit notes issued are not recorded in the system	All credit notes issued are recorded.
Invoices are recorded in the wrong period.	Invoices are recorded in the appropriate period.
Credit notes are recorded in the wrong accounting period.	Credit notes issued are recorded in the appropriate accounting period.
Cash receipts are not recorded in the period in which they are received.	Cash receipts are recorded in the period in which they are received.
Cash receipts data are not entered correctly.	Cash receipts data are entered for processing accurately.
Cash receipts are not entered in the system for processing.	All cash receipts data are entered for processing.
Cash receipts data are not valid and are not entered in the system for processing more than once.	Cash receipts data are valid and are entered for processing only once.
Cash discounts are not accurately calculated and recorded.	Cash discounts are accurately calculated and recorded.
Collection of accounts receivable is delayed and not properly monitored.	Timely collection of accounts receivable is monitored.
System access to process transactions has not been restricted to the authorized users.	System access to process transactions has been restricted to the authorized users.

9.6.4 Inventory Cycle – Risks and Controls

The **Inventory Cycle** is a process of accurately tracking the on-hand inventory levels for an enterprise. An inventory system should maintain accurate record of all stock movements to calculate the correct balance of inventory including raw material, in process stock and finished goods.

The typical phases of the Inventory Cycle for Manufacturers are as follows:

i. **The Ordering phase:** The amount of time it takes to order and receive raw materials.

ii. **The Production phase:** The work in progress phase relates to time it takes to convert the raw material to finished goods ready for dispatch to customer.

iii. **The finished goods and delivery phase:** The finished goods that remain in stock and the delivery time to the customer. The inventory cycle is measured in number of days.

Risks and Control Objectives (Masters-Inventory) and Risks and Control Objectives (Transactions-Inventory) are provided below in Tables 9.15 and 9.16 respectively.

Masters

Table 9.15: Risks and Control Objectives (Masters-Inventory)

Risks	Control Objectives
Invalid changes are made to the inventory management master file.	Only valid changes are made to the inventory management master file.
Invalid changes to the inventory management master file are entered and processed.	All valid changes to the inventory management master file are input and processed.
Changes to the inventory management master file are not accurate.	Changes to the inventory management master file are accurate.
Changes to the inventory management master file are not promptly processed.	Changes to the inventory management master file are promptly processed.
Inventory management master file data is not up to date.	Inventory management master file data remain up to date.
System access to maintain inventory masters has not been restricted to the authorized users.	System access to maintain inventory masters has been restricted to the authorized users.

Transactions

Table 9.16: Risks and Control Objectives (Transactions-Inventory)

Risks	Control Objectives
Adjustments to inventory prices or quantities are not recorded accurately.	Adjustments to inventory prices or quantities are recorded accurately.
Raw materials are received and accepted without valid purchase orders.	Raw materials are received and accepted only if they have valid purchase orders.
Raw materials received are not recorded accurately.	Raw materials received are recorded accurately.
Raw materials received are not recorded in system.	All raw materials received are recorded.
Receipts of raw materials are not recorded promptly and not in the appropriate period.	Receipts of raw materials are recorded promptly and in the appropriate period.
Defective raw materials are not returned promptly to suppliers.	Defective raw materials are returned promptly to suppliers.
Transfers of raw materials to production are not recorded accurately and are not in the appropriate period.	All transfers of raw materials to production are recorded accurately and in the appropriate period.
Direct and indirect expenses associated with production are not recorded accurately and are posted in an inappropriate period.	All direct and indirect expenses associated with production are recorded accurately and in the appropriate period.
Transfers of completed units of production to finished goods inventory are not recorded completely and accurately and are posted in an inappropriate period.	All transfers of completed units of production to finished goods inventory are recorded completely and accurately in the appropriate period.
Finished goods returned by customers are not recorded completely and accurately and are posted in an inappropriate period.	Finished goods returned by customers are recorded completely and accurately in the appropriate period.
Finished goods received from production are not recorded completely and accurately and are posted in an inappropriate period.	Finished goods received from production are recorded completely and accurately in an appropriate period.
Shipments are not recorded in the system.	All shipments are recorded in the system.
Shipments are not recorded accurately.	Shipments are recorded accurately.
Shipments are not recorded promptly and are in an inappropriate period.	Shipments are recorded promptly and in the appropriate period.

Inventory is reduced when goods are not shipped and made based on unapproved customer orders.	Inventory is reduced only when goods are shipped with approved customer orders.
Costs of shipped inventory are not transferred from inventory to cost of sales.	Costs of shipped inventory are transferred from inventory to cost of sales.
Costs of shipped inventory are not accurately recorded.	Costs of shipped inventory are accurately recorded.
Amounts posted to cost of sales does not represent those associated with shipped inventory.	Amounts posted to cost of sales represent those associated with shipped inventory.
Costs of shipped inventory are not transferred from inventory to cost of sales promptly and not done in the appropriate period.	Costs of shipped inventory are transferred from inventory to cost of sales promptly and in the appropriate period.
System access to process inventory related transactions has not been restricted to the authorized users.	System access to process inventory related transactions has been restricted to the authorized users.

9.6.5 Human Resources – Risks and Controls

The **Human Resources (HR)** cycle refers to human resources management and covers all the stages of an employee's time within a specific enterprise and the role the human resources department plays at each stage. Typical stage of HR cycle includes the following:

1. **Recruiting and On-boarding:** Recruiting is the process of hiring a new employee. The role of the human resources department in this stage is to assist in hiring. This might include placing the job ads, shortlisting the candidates based on resumes, conducting interviews and administering assessments such as personality profiles to select the most suitable applicant for the position. In a small business where the owner performs these duties personally, the HR person would assist in a support role. In some organizations, the recruiting stage is referred to as "hiring support." On-boarding is the process of getting the successful applicant set up in the system as a new employee.

2. **Orientation and Career Planning:** Orientation is the process by which the employee becomes a member of the company's work force through learning his/her new job duties, establishing relationships with co-workers and supervisors and developing a niche. Career planning is the stage at which the employee and his/her supervisors work out her long-term career goals with the company. The human resources department may make additional use of personality profile testing at this stage to help the employee determine his/her best career options with the company.

3. **Career Development:** Career development opportunities are essential to keep an employee engaged with the company over time. After an employee, has established himself/herself at the company and determined his long-term career objectives, the human resources department should try to help him/her meet his/her goals, if they are realistic. This can include professional growth and training to prepare the employee for more responsible positions within the company. The company also assesses the employee's work history and performance at this stage to determine whether he has been a successful hire.

4. **Termination or Transition:** Some employees will leave a company through retirement after a long and successful career. Others may choose to move on to other opportunities or be laid off. Whatever the reason, all employees will eventually leave the company. The role of HR in this process is to manage the transition by ensuring that all policies and procedures are followed, carrying out an exit interview if that is company policy and removing the employee from the system. These stages can be handled internally or with the help of enterprises that provide services to manage the employee life cycle.

Configuration

Table 9.17: Risks and Control Objectives (Configuration-Human Resource)

Risks	Control Objectives
Employees who have left the company continue to have system access.	System access to be immediately removed when employees leave the company.
Employees have system access in excess of their job requirements.	Employees should be given system access based on a "need to know" basis and to perform their job function.

Masters

Table 9.18: Risks and Control Objectives (Masters-Human Resources)

Risks	Control Objectives
Additions to the payroll master files do not represent valid employees.	Additions to the payroll master files represent valid employees.
New employees are not added to the payroll master files.	All new employees are added to the payroll master files.
Terminated employees are not removed from the payroll master files.	Terminated employees are removed from the payroll master files.
Employees are terminated without following statutory requirements.	Employees are terminated only within statutory requirements.

Deletions from the payroll master files do not represent valid terminations.	Deletions from the payroll master files represent valid terminations.
Invalid changes are made to the payroll master files.	Only valid changes are made to the payroll master files.
Changes to the payroll master files are not accurate.	Changes to the payroll master files are accurate.
Changes to the payroll master files are not processed in a timely manner.	Changes to the payroll master files are processed in a timely manner.
Payroll master file data is not up to date.	Payroll master file data remain up to date.
Payroll is disbursed to inappropriate employees.	Payroll is disbursed to appropriate employees.
System access to process employee master changes has not been restricted to the authorized users.	System access to process employee master changes has been restricted to the authorized users.

9.6.6 Fixed Assets – Risks and Controls

Fixed Assets process ensures that all the fixed assets of the enterprise are tracked for the purposes of financial accounting, preventive maintenance, and theft deterrence. Fixed assets process ensures that all fixed assets are tracked and fixed asset record maintains details of location, quantity, condition, and maintenance and depreciation status. Typical steps of fixed assets process are as follows:

1. **Procuring an asset:** An asset is entered into the accounting system on receipt of ; approved invoice for the asset; into the accounts payable; or purchasing module of the system. In some case, for long term projects, assets procured are accounted as capital work in progress and transferred to Assets on completion of the project.

2. **Registering or adding an asset:** Most of the information needed to set up the asset for depreciation is available at the time the invoice is entered. Information entered at this stage could include; acquisition date, placed-in-service date, description, asset type, cost basis, depreciable basis, location, etc.

3. **Adjusting the Assets:** Adjustments to existing asset may be made when it adds value to the useful life of assets. Events may occur that can change the depreciable basis of an asset. Further, there may be improvements or repairs made to asset that either adds value to the asset or extend its economic life. For example, in case of immovable property revaluation of assets may impact the value of recorded assets in the records of company.

4. **Transferring the Assets:** A fixed asset may be sold or transferred to another subsidiary, reporting entity, or department within the company. These inter-company and intra-company transfers may result in changes that impact the asset's depreciable basis, depreciation, or other asset data. This needs to be reflected accurately in the fixed assets management system.

5. **Depreciating the Assets:** The decline in an asset's economic and physical value is called depreciation. Depreciation is an expense which should be periodically accounted on a company's books, and allocated to the accounting periods, to match income and expenses. Sometimes, the revaluation of an asset, may also result in appreciation of its value.

6. **Disposing the Assets:** When a fixed asset is no longer in use, becomes obsolete, is beyond repair; the asset is disposed. When an asset is taken out of service, depreciation cannot be charged on it. There are multiple types of disposals, such as abandonments, sales, and trade-ins. Any difference between the book value, and realized value, is reported as a gain or loss.

Tables 9.19 and 9.20 given below provide Risks and Control Objectives (Masters-Fixed Assets) and Risks and Control Objectives (Transactions-Fixed Assets) respectively.

Masters

Table 9.19: Risks and Control Objectives (Masters-Fixed Assets)

Risks	Control Objectives
Invalid changes are made to the fixed asset register and/or master file.	Only valid changes are made to the fixed asset register and/or master file.
Valid changes to the fixed asset register and/or master file are not input and processed.	All valid changes to the fixed asset register and/or master file are input and processed.
Changes to the fixed asset register and/or master file are not accurate.	Changes to the fixed asset register and/or master file are accurate.
Changes to the fixed asset register and/or master file are not promptly processed.	Changes to the fixed asset register and/or master file are promptly processed.
Fixed asset register and/or master file data are not kept up to date.	Fixed asset register and/or master file data remain up to date.
System access to fixed asset master file / system configuration is not restricted to the authorized users.	System access to fixed asset master file / system configuration is restricted to the authorized users.
System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has not been correctly defined.	System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has been correctly defined.

Transactions

Table 9.20: Risks and Control Objectives (Transactions-Fixed Assets)

Risks	Control Objectives
Fixed asset acquisitions are not accurately recorded.	Fixed asset acquisitions are accurately recorded.
Fixed asset acquisitions are not recorded in the appropriate period.	Fixed asset acquisitions are recorded in the appropriate period.
Fixed asset acquisitions are not recorded.	All fixed asset acquisitions are recorded.
Depreciation charges are not accurately calculated and recorded.	Depreciation charges are accurately calculated and recorded.
Depreciation charges are not recorded in the appropriate period.	All depreciation charges are recorded in the appropriate period.
Fixed asset disposals/transfers are not recorded.	All fixed asset disposals/transfers are recorded.
Fixed asset disposals/transfers are not accurately calculated and recorded.	Fixed asset disposals/transfers are accurately calculated and recorded.
Fixed asset disposals/transfers are not recorded in the appropriate period.	Fixed asset disposals/transfers are recorded in the appropriate period.
Records of fixed asset maintenance activity are not accurately maintained.	Records of fixed asset maintenance activity are accurately maintained.
Unusable Fixed Assets are not recorded at disposable value	Assets should be periodically tested for impairment
Software not in use are not removed from Gross block of assets.	Software gross block to be periodically verified to identify discarded software
Fixed asset maintenance activity records are not updated in a timely manner.	Fixed asset maintenance activity records are updated in a timely manner.
Accounting entries pertaining to acquisition, disposals, transfers, retirement are not recorded in the correct GL account.	Accounting entries pertaining to acquisition, disposals, transfers, retirement are recorded in the correct GL account.
System access to process fixed asset transactions has not been restricted to the authorized users.	System access to process fixed asset transactions has been restricted to the authorized users.

9.6.7 General Ledger – Risks and Controls

General Ledger (GL) process refers to the process of recording the transactions in the system to generate the reports from financial transactions entered in the system. The input for GL Process

Flow is the financial transactions and the outputs are various types of financial reports such as balance sheet, profit and loss a/c, funds flow statement, ratio analysis, etc.

The typical steps in general ledger process flow are as follows:

1. Entering financial transactions into the system
2. Reviewing Transactions
3. Approving Transactions
4. Posting of Transactions
5. **Generating Financial Reports**

Risks and Control Objectives (Configuration-General Ledger); Risks and Control Objectives (Masters-General Ledge) and Risks and Control Objectives (Transactions-General Ledger) are provided below in Tables 9.21, 9.22 and 9.23 respectively.

Configuration

Table 9.21: Risks and Control Objectives (Configuration-General Ledger)

Risks	Control Objectives
Unauthorized general ledger entries could be passed.	Access to general ledger entries is appropriate and authorized.
System functionality does not exist to segregate the posting and approval functions.	System functionality exists to segregate the posting and approval functions.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliations to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliations to confirm accuracy of such accounts.
Systems do not generate reports of all recurring and non-recurring journal entries for review by management for accuracy.	Systems generate reports of all recurring and non-recurring journal entries for review by management for accuracy.
Non-standard journal entries are not tracked and are inappropriate.	All non-standard journal entries are tracked and are appropriate.
Out-of-balance entries are not prohibited.	Out-of-balance entries are prohibited.
Enterprise-wide consolidation, including standard inter-company eliminations, is not automated and not performed.	Enterprise-wide consolidation, including standard inter-company eliminations, is automated and performed.
Variance reports are not generated for use to identify posting errors/out-of-balance conditions.	Variance reports are generated for use to identify posting errors/out-of-balance conditions.

System controls are not in place for appropriate approval of write-offs.	System controls are in place for appropriate approval of write-offs.
Journal entries of exceptional amount that were posted to the general ledger during the month are not flagged by the system and not subsequently reviewed for accuracy and approved by the controller or CFO after month-end.	Journal entries of exceptional amount that were posted to the general ledger during the month are flagged by the system and subsequently reviewed for accuracy and approved by the controller or CFO after month-end.
Automated amortization timing, periods and methods are not appropriate and not accurately entered.	Automated amortization timing, periods and methods are appropriate and accurately entered.
Standard, recurring period-end journal entries submitted from subsidiary ledger systems are not automated, not appropriately approved and not entered accurately.	Standard, recurring period-end journal entries submitted from subsidiary ledger systems are automated, appropriately approved and entered accurately.
Transactions can be recorded outside of financial close cut-off requirements.	Transactions cannot be recorded outside of financial close cut-off requirements.
The sources of all entries are not readily identifiable.	The sources of all entries are readily identifiable.
Transactions are not rejected, accepted and identified, on exception reports in the event of data exceptions.	Transactions are rejected, or accepted and identified, on exception reports in the event of data exceptions.
Account mappings are not up to date.	Account mappings are up to date.
Adding to or deleting general ledger accounts are not limited to authorize accounting department personnel.	Adding to or deleting general ledger accounts are limited to authorized accounting department personnel.

Masters

Table 9.22: Risks and Control Objectives (Masters-General Ledger)

Risks	Control Objectives
General ledger master file change reports are not generated by the system and are not reviewed as necessary by an individual who does not input the changes.	General ledger master file change reports are generated by the system and reviewed as necessary by an individual who does not input the changes.
A standard chart of accounts has not been approved by management and is not utilized within all entities of the corporation.	A standard chart of accounts has been approved by management and is not utilized within all entities of the corporation.

Transactions

Table 9.23: Risks and Control Objectives (Transactions-General Ledger)

Risks	Control Objectives
General ledger balances are not reconciled to sub ledger balances and such reconciliation are not reviewed for accuracy and not approved by supervisory personnel.	General ledger balances reconcile to sub ledger balances and such reconciliation are reviewed for accuracy and approved by supervisory personnel.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliation to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliation to confirm accuracy of such accounts.
Account codes and transaction amounts are not accurate and not complete, and exceptions are not reported.	Account codes and transaction amounts are accurate and complete, with exceptions reported.
A report of all journal entries completed as part of the closing process is not reviewed by management to confirm the completeness and appropriateness of all recorded entries.	A report of all journal entries completed as part of the closing process is reviewed by management to confirm the completeness and appropriateness of all recorded entries.
Actual-to-actual, actual-to-budget and yield reports are not produced from the general ledger system monthly prior to the final close of the general ledger. Reports are not distributed to and reviewed by the controller and CFO. Unusual amounts or variances are not investigated and reclassified when applicable.	Actual-to-actual, actual-to-budget and yield reports are produced from the general ledger system monthly prior to the final close of the general ledger. Reports are distributed to and reviewed by the controller and CFO. Unusual amounts or variances are investigated and re-classified when applicable.
Entries booked in the close process are not complete and accurate.	Entries booked in the close process are complete and accurate.

9.6.8 CASA at CBS - Risks and Controls

Banks carry out a variety of functions across the broad spectrum of products offered by them. Some of the key products that are provided by most commercial banks are Current and Savings Accounts (CASA), Credit Cards, Loans and Advances, Treasury and Mortgages.

Below is a high-level overview (illustrative and not exhaustive) of some of these processes with its relevant flow and indicative key risks and controls across those processes. The flow and process as well as relevant risk and control may differ from bank to bank however below information should give a basic idea to students about these processes where Core Banking System (CBS) and other relevant applications are used and what specific risk and controls might be relevant in such cases.

I. Business Process Flow of Current & Savings Accounts (CASA)

- Either the customer approaches the relationship manager to apply for a CASA facility or will apply the same through internet banking, the charges/ rates for the facility are provided by the Relationship Manager (RM) on basis of the request made by the customer.
- Once the potential customer agrees to avail the facilities/products of the bank, the RM request for the relevant documents i.e. KYC and other relevant documents of the customer depending upon the facility/product. KYC (Know Your Customer) is a process by which banks obtain information about the identity and address of the customers. KYC documents can be Passport, Driving License, etc.
- The documents received from the customers are handed over to the Credit team / Risk team for sanctioning of the facilities/limits of the customers.
- Credit team verifies the documents, assesses the financial and credit worthiness of the borrowers and updates facilities in the customer account.
- Current Account /Saving Account along with the facilities requested are provided to the customer for daily functioning.
- Customers can avail facilities such as cheque deposits/ withdrawal, Cash deposit/ withdrawal, Real Time Gross Settlement (RTGS), National Electronics Funds Transfer System (NEFT), Electronic Clearing Service (ECS), Overdraft Fund Transfer services provided by the bank.

Table 9.24: Risks and Control. Objectives around the CASA Process

Risks	Control Objectives
Credit Line setup is unauthorized and not in line with the bank's policy.	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk Policy and that the Client can be given the Credit Line.
Credit Line setup in CBS is unauthorized and not in line with the bank's policy.	Access rights to authorize the credit limit in case of account setup system should be restricted to authorized personnel.
Customer Master defined in CBS is not in accordance with the Pre- Disbursement Certificate.	Access rights to authorize the customer master in CBS should be restricted to authorized personnel.
Inaccurate interest / charge being calculated in CBS.	Interest on fund-based facilities is automatically calculated in the CBS as per the defined rules.

Unauthorized personnel approving the CASA transaction in CBS.	Segregation of Duties (SoD) to be maintained between the initiator and authorizer of the transaction for processing transaction in CBS.
Inaccurate accounting entries generated in CBS.	Accounting entries are generated by CBS basis the facilities requested by the customer and basis defined configurations for those facilities in CBS.

SUMMARY

In the present contemporary world, apart from change the thought-provoking terminology is business which is a driving force behind change and how to insight into trade is a dynamic called integration. Organizations of the 1990's were concentrated on the re-engineering and redesign of their business processes to endorse their competitive advantage. To endure in the 21st century, organizations have started paying attention on integrating enterprise-wide technology solutions to progress their business processes called Business Information Systems (BIS). Now, every organization integrates part or all of its business functions together to accomplish higher effectiveness and yield. The thrust of the argument was that Information Technology (IT), when skilfully employed could in various ways differentiate an organization from its competition, add value to its services or products in the eyes of its customers, and secure a competitive advantage in comparison to its competition. This Chapter has provided an overview on the importance of information systems in an IT environment and how information is generated. There has been a detailed discussion on Information System Audit, its need, and the method of performing the same. Afterwards, the chapter discusses the tools to perform an Information system audit is discussed. The idea of pre-audit survey and planning of an audit for effective execution of an audit has also been elaborated in the chapter. It also covers various automated business processes. This chapter throws a light on how Digitization of business processes impact the modern enterprises and leads to new risks which should be mitigated by implementing appropriate controls.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. An IS Auditor is using an audit tool that involves embedding audit software modules within a host application system to provide continuous monitoring of system's transactions. Which audit tool does this refer to?

   (a) Audit hooks

   (b) System Control Audit Review File (SCARF)

   (c) Integrated Test Facility (ITF)

   (d) Continuous and Intermittent Simulation (CIS)

2. In an organization ABC Ltd.; the adherence of policies, procedures and standards as defined by the management are required to be followed. An accountant Mr. X, due to enmity, misused his access rights and made changes in the credit points earned by the salesperson Mr. A on every sale of his customer. During the audit, the auditor Mr. B suspected this discrepancy and preferred to embed an audit software module into the accountant Mr. X's host application software to determine the frequency with which he had made the changes in the credit points of Mr. A. Which of the following audit tool is used by Mr. B in this case?

   (a) Integrated Test Facility (ITF)

   (b) System Control Audit Review File (SCARF)

   (c) Snapshots

   (d) Audit Hooks

3. Which of the following is not an advantage of continuous assisted audit techniques?

   (a) Evaluate the integrity of an application

   (b) Timely, Comprehensive and Detailed Auditing

   (c) Analyze aging of transaction files

   (d) No need of prior knowledge and experience of working with CAAT

4. An IS auditor used concurrent audit technique to check whether the accounting system of an organization restricting the cash payment in excess of ₹ 10,000/- or not by creation of dummy entity. Identify from the following concurrent audit techniques which will be useful in this case.

   (a) Use of System Control Audit Review File (SCARF)

(b) Use of Integrated Test Facility (ITF)

(c) Use of Continuous and Intermittent Simulation (CIS)

(d) Use of Snapshot

5. Mr. Ankit an IS auditor of ABC Ltd., wants to collect evidence based on system user profiles. To perform this activity, he has collected data from log files.Which of the following audit technique is being used by the IS auditor to achieve this objective?

(a) Continuous and intermittent Solution (CIS)

(b) Audit Hooks

(c) System Control Audit Review File (SCARF)

(d) Integrated Test Facility (ITF)

ANSWERS/SOLUTIONS

1.	**(b)**	**2.**	**(b)**	**3.**	**(d)**	**4.**	**(b)**	**5.**	**(c)**

UNIT – IV

DIGITAL DATA AND ANALYSIS

CHAPTER 10

DIGITAL DATA AND PRIVACY

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- develop an understanding about the concepts of data protection and its related principles.
- comprehend the concepts related to Data Analysis and the tools employed for data security.
- know the basics about the Digital Personal Data Protection Act, 2023 and its major highlights.

CHAPTER OVERVIEW

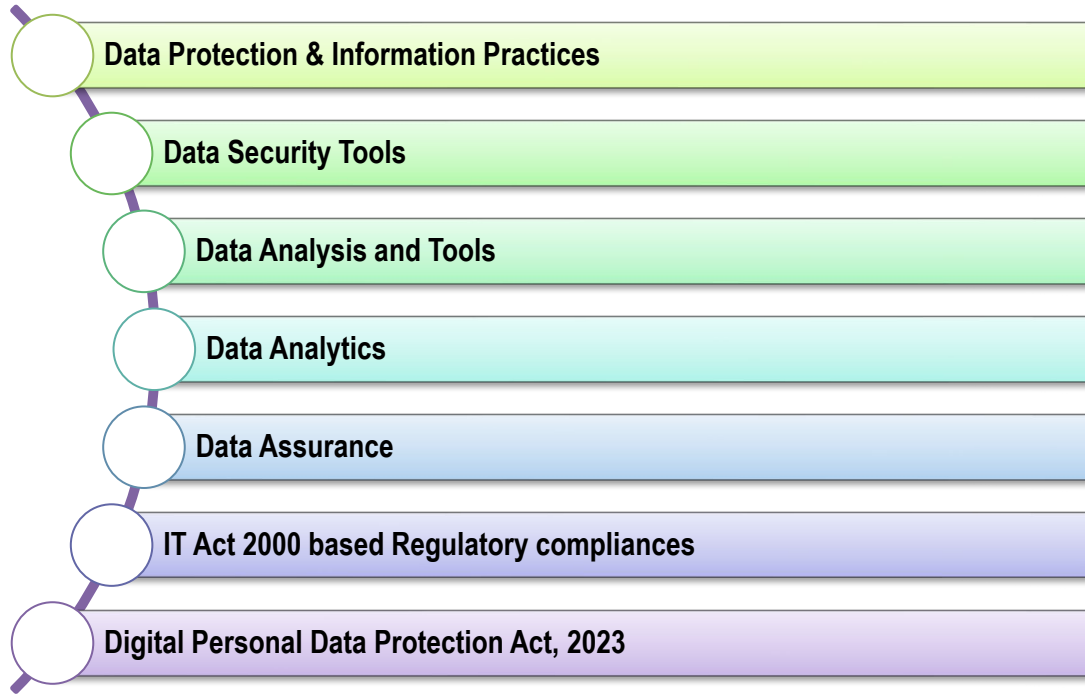


Illustration: Aviation Industry

Headlines about the increase in cyberattacks across different industries, companies, and infrastructures, and the aviation industry have become dangerously common. There has been a significant rise in cyber-attacks in the last decade in the aviation industry. The aviation industry has access to a huge volume of sensitive information including passport and payment information, making it a prime target for cybercriminals. The aviation industry is a largely interconnected network, spanning across various sectors and stakeholders, and each one is a potential entry point for attackers. Key elements like the reservation systems, digital air traffic controls, navigation, anti-collision systems, in-flight entertainment devices, cabin crew devices, cockpit instruments, cargo handling, amongst others, are all highly vulnerable to attacks. A breach of any of these could be disastrous, potentially leading to hijacking or even a crash.

Furthermore, airlines are increasingly looking for ways to reduce costs and improve efficiency by adopting advanced technologies across all functions. This leads to the outsourcing of IT departments and systems to third-party vendors and relying on Commercial Off-The-Shelf (COTS)

software. But third-party systems and software do not always have reliable and robust security, leaving them more prone to attacks.

Major cyberattacks on Aviation Industry world-wide.

No company is immune from falling victim to a cyberattack. The number of security breaches grew exponentially during the COVID-19 pandemic and the aviation industry has experienced a wave of cyberattacks. Let's consider the recent high-profile attacks that have threatened critical infrastructures.

In 2022, a low-cost airline in India fell prey to a ransomware attack that led to the delayed departures of several flights. While the airline was able to contain and rectify the situation and resume operations within a few hours, it left many passengers stranded at different airports. Some passengers took to social media to point out the chaos caused at the airports. The situation also threw light on the fact that while IT teams try to resolve the issue at the back end, it is equally crucial to train the ground staff and in-flight staff to handle such situations effectively.

- In April 2022, a renowned airline faced a cyberattack that caused flight delays and operational glitches for five days. The attack was reportedly due to a data breach at the company's third-party service provider, which provides passenger management software solutions (e.g. check-in and boarding) for the airlines. Without the check-in systems in place, the airlines were forced to process flights, fill out boarding passes, and check in passengers manually.
- In February 2021, one of the largest aviation IT companies that caters for nearly 90% of airlines globally with its in-house Passenger Service System, was hit by a massive cyberattack in which hackers targeted servers containing personal data records of passengers dating back to a decade. The IT company revealed that several major airlines were affected, including an Indian airline company that reported the personal data of nearly 4.5 million passengers were compromised.
- A British airline company fell prey to one of the biggest cyberattacks in 2020, when the personal data of nearly 9 million customers, including the credit card information of 2,000+ customers, was compromised.
- In 2018, the largest British airline company had a major data breach in which the personal data of over 400,000 customers and staff were compromised. The breached data included names, addresses, and credit card information.

The consequences of these cyberattacks span from minor inconveniences to severe operational disruptions, encompassing the breach of personal data for both customers and staff. Additionally,

these attacks result in substantial financial losses for the airlines and, in the gravest scenarios, pose a threat to life through potential hijacks or crashes.

What Needs to be done to protect Business and Customer Data?

The question is whether companies are doing enough from a data security and data privacy point of view to protect themselves and their customers that put their trust in them. It is of the utmost importance that organizations take further steps to bulletproof their data from cyberattacks, especially if they are using external third-party services.

Compliance with best-practice data security guidelines and international standards is a significant step to prevent future breaches. Additionally, to mitigate the potential damage of breaches that may occur, it is of utmost importance that an organization employs a strong encryption strategy and operational processes. To prevent unencrypted data being accessed by unauthorized parties, the companies must take steps to ensure that:

- Its data remains encrypted while at rest in its databases.
- Its data remains encrypted while in transit while it migrates between clients, applications, and the personnel of the company.
- The Hardware Security Module (HSMs) must not be accessible by the third-party data processor.
- Its encryption keys must never be with its third-party data processor and must remain stored in company's vaulted data center.
- Third parties will not have access to readable data.
- The mandatory multifactor authentication of clients is implemented to generally limit the access to data to only authorized persons like passengers who can only view their personal data.

10.1 INTRODUCTION

Every organization runs various operations which involve various kinds of data collection and data processing activities. Data across these activities needs to be collected properly and stored in an effective manner so that it can be used for analysis purposes in an easy way. For example, an organization may have many employees and their records and data need to be maintained as part of the human resource process. Similarly, under the accounting process, transactions related to payroll and other expenses need to be maintained. But so far, the data that we have maintained is in a passive state. If we can analyze this data, we can develop insights which may help us in

transforming and restructuring existing operations to achieve optimum utilization of resources. The HR department can analyze the data and can identify the productivity. Employee leave records and patterns of people joining and leaving organizations can help in building a better HR policy. The accounts department can analyze transactional data to observe spending patterns. Restructuring the expenses policy based on this analysis may lead to better utilization of funds and the minimization of money wastage

10.2 DATA PROTECTION

Data is a representation of facts and can be presented in many forms using characters, digits, and special symbols. Data has become a critical aspect of every business industry like agriculture, real estate, education, banking, food industry and others. Collecting data about your business results in better understanding of your customers and business. In fact, with the use of advanced data analytics and user-friendly tools it has become quite easy to take full advantage of data and analytics to transform any business. **Digital data** is the electronic representation of information in a format or language that machines can read and understand. In more technical terms, digital data is a binary format of information that's converted into a machine-readable digital format. The power of digital data is that any analog inputs, from very simple text documents to genome sequencing results, can be represented with the binary system.

An **Information Asset** is information that is worth something to someone and where the holder of that asset might use the information to their benefit or might sell the information to others for a profit. Most information assets occur in the business and commercial world. Information assets are represented as digital assets in today's digital era. A **Digital Asset** is generally anything that is created and stored digitally, is identifiable and discoverable, and has or provides value. Digital assets have become more popular and valuable as technological advances become integrated into our personal and professional lives. Data, images, video, written content, and more are considered digital assets with ownership rights.

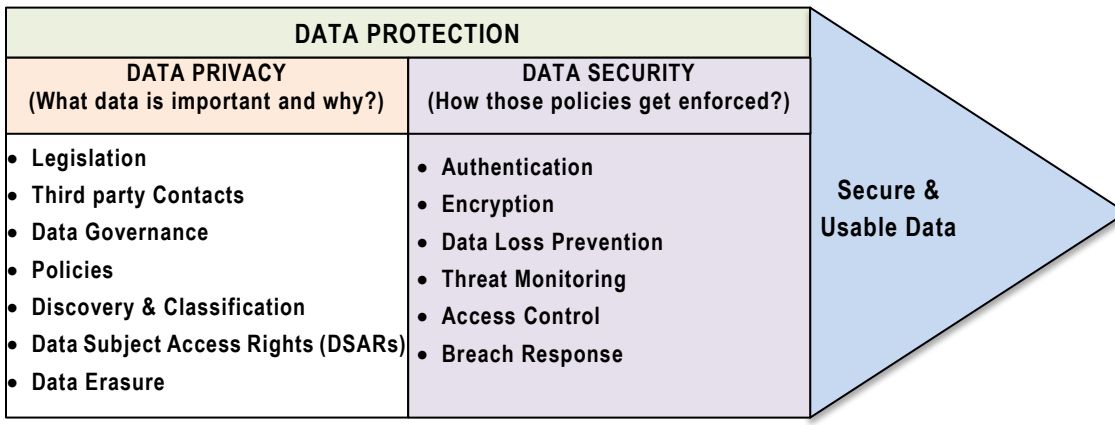


Fig. 10.1: Data Protection Components

- In technical terms, **Data Protection** (Fig. 10.1) is a set of strategies and processes one can use to secure the privacy, availability, and integrity of your data. A data protection strategy is vital for any organization that collects, handles, or stores sensitive data. A successful strategy can help prevent data loss, theft, or corruption and can help minimize damage caused in the event of a breach or disaster. Data loss can occur in many ways:
  - Physical loss of the data itself, either temporarily or permanently.
  - Loss of confidentiality of sensitive data.
  - Loss of the ability to be able to use the data because of a loss of access to the data for any reason or a loss of responsiveness in which the data cannot be retrieved for use (even if it is technically available) within a reasonable period.
- Data protection, as a ***have-to*** function, means that it is a cost of doing business, and not a ***want-to*** function, which directly carries out the mission of any organization. This means that managing the costs of data protection is important, since spending more money on data protection generates fewer profits for non-profit businesses. Data protection solutions rely on technologies such as Data Loss Prevention (DLP), storage with built-in data protection, firewalls, encryption, and endpoint protection. Protection touches a wide spectrum of business issues, including but by no means limited to backup and restore, disaster recovery, business continuity, high availability, compliance, governance, data privacy, data security and e-discovery.
- **Data Privacy** is a guideline for how data should be collected or handled, based on its sensitivity and importance. Data privacy helps ensure that sensitive data is only accessible to approved parties so as to prevent criminals from being able to maliciously use data and help ensure that organizations meet regulatory requirements. Data privacy is also important because for individuals to be willing to engage online, they have to trust that their personal data will be handled with care. Organizations use data protection practices to demonstrate to their customers and users that they can be trusted with their personal data. Personal data can be misused in several ways if it is not kept private or if people don't have the ability to control how their information is used - Entities may sell personal data to advertisers or other outside parties without user consent, which can result in users receiving unwanted marketing or advertising, which may prove to be harmful for the individuals. For a business, these outcomes can irreparably harm their reputation, as well as resulting in fines, sanctions, and other legal consequences.

In addition to the real-world implications of privacy infringements, many people and countries hold that privacy has intrinsic value: that privacy is a human right fundamental to a free society, like the right to free speech. Overall, the primary data protection objectives have a role in data privacy:

- **Data availability/data responsiveness:** Individuals are more and more likely to have the right to access personal information and to access it in a specified period.
- **Data preservation:** The right to make sure that the data is accurate and the ability to rectify mistakes will become more and more critical, and issues of data retention are likely to become more prominent.
- **Data confidentiality:** Data privacy is a subset of data confidentiality - is at the heart of the loss of data privacy.

♦ **Data Security** is focused on protecting personal data from any unauthorized third-party access or malicious attacks and exploitation of data. It is set up to protect personal data using different methods and techniques to ensure data privacy. Data security ensures the integrity of the data, meaning data is accurate, reliable, and available to authorized parties.

Most online businesses and websites collect personal data, from email addresses to phone numbers, credit cards, and log-in details. Ideally, these entities shouldn't keep more information than is necessary, nor should they keep it longer than necessary.

Table 10.1: Differentiation between Data Privacy, Data Security and Data Protection

Data Privacy	Data Security	Data Protection
Data privacy is about proper usage, collection, retention, deletion, and storage of data, i.e. it is more about guarding the data against unauthorized access.	Data security is policies, methods, and means to secure personal data, i.e. it is more about guarding against malicious threats.	Data protection provides tools and policies to restrict access to the data and makes sure that an organization has a way of restoring its data following a data loss event.
Emphasizes on "Are you who, you say, you are?"	Emphasizes on "Prove you are, who you say, you are."	Emphasizes on "How can we ensure that the data is protected?"
For example - If we are using a Google Gmail account, then the way Google uses our data to administer our account, would be data privacy.	For example - If we are using a Gmail account, the password would be a method of data security.	For example – In an Insurance Policy, the aim of data protection is not to maximize profits or revenues, or to minimize costs, but to minimize worst-case losses.

Data privacy is post requisite to data security.	Data security is a prerequisite to data privacy.	It is a combination of Data privacy and Data security. mcq tha

10.3 WHAT ARE FAIR INFORMATION PRACTICES?

The Fair Information Practices are as follows:

- **Collection limitation:** There should be limits to how much personal data can be collected. Further data collection procedures should be standardized across all business processes covering the concerns of all the related stakeholders.
- **Data quality:** When collecting personal data, it should be accurate and directly relevant to its intended purpose. Data plays a crucial role in any business process, and if not maintained correctly, it can result in misunderstandings and incorrect decision-making. Therefore, adequate controls are essential to ensure data quality at every stage, including collection, processing, and storage, thereby maintaining the integrity of the data.
- **Purpose specification:** The use of personal data should be specified, and data should only be used for the same. Further it should be ensured that data should be encrypted during and after usage. This may include three states of data - rest, processing, transmission. Encryption will ensure confidentiality of data and only intended participants will be able to access the data.
- **Use limitation:** Data should not be used for purposes other than what was specified and that can be ensured by using multi-factor authentication and authorization mechanisms. This will ensure need to know and need to do access control.
- **Security safeguards:** Data should be secured through encryption at all three stages: processing, transmission, and storage.
- **Individual participation:** Individuals have several rights, including the right to know who has their personal data, to have their data communicated to them, to know why a request for their data is denied, and to have their personal data corrected or erased.
- **Accountability:** Anyone who collects data should be held accountable for implementing these principles.

Table 10.2: Challenges user/businesses face when protecting their online privacy.

Challenges users face when protecting their online privacy	Challenges businesses face when protecting users' privacy
• **Online tracking:** User behavior is regularly tracked online. Cookies often record a	• **Communication:** Organizations sometimes struggle to

user's activities, and while most countries require websites to alert users of cookie usage, users may not be aware of to what degree cookies are recording their activities.	communicate clearly to their users what personal data they are collecting and how they use it.
• **Losing control of data:** With so many online services in common use, individuals may not be aware of how their data is being shared beyond the websites with which they interact online, and they may not have a say over what happens to their data. • **Lack of transparency:** To use web applications, users often have to provide personal data like their name, email, phone number, or location; meanwhile, the privacy policies associated with those applications may be dense and difficult to understand. • **Social media:** It is easier than ever to find someone online using social media platforms, and social media posts may reveal more personal information than users realize. In addition, social media platforms often collect more data than users are aware of. • **Cybercrime:** Many attackers try to steal user data to commit fraud, compromise secure systems, or sell it on underground markets to parties who will use the data for malicious purposes. Some attackers use phishing attacks to try to trick users into revealing personal information; others attempt to compromise companies' internal systems that contain personal data.	• **Cyber-crime:** Attackers target both individual users and organizations that collect and store data about those users. In addition, as more aspects of a business become Internet-connected, the attack surface increases. • **Data breaches:** A data breach can lead to a massive violation of user privacy if personal details are leaked, and attackers continue to refine the techniques they use to cause these breaches. • **Insider threats:** Internal employees or contractors might inappropriately access data if it is not adequately protected.

10.4 DATA SECURITY TOOLS

♦ **Encryption:** Encryption is a way to conceal information by scrambling it so that it appears to be random data. Only parties with the encryption key can unscramble the information, thereby offering advanced protection to prevent misuse of business data, even if it gets accidentally or intentionally leaked. Data encryption tools encrypt business information in a coded format

which can be decoded only by authorized persons after entering the preset security key. This proves beneficial in events where corporate devices have been compromised due to theft or hacking. Refer Fig. 10.2. Let's consider if a system wants to send some data secretly to another system, then the sender system will encrypt(codify) the data using a secret key and coded data would be generated that would be sent to the receiver computer in encrypted(coded) form. Now the receiver system will take the same key and decrypt the coded data to get the original data sent by the sender.

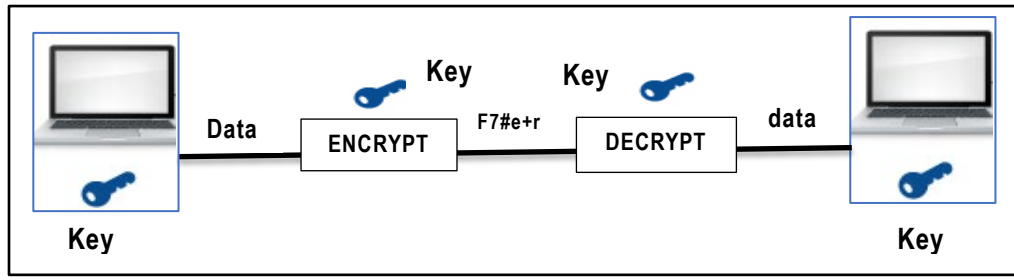
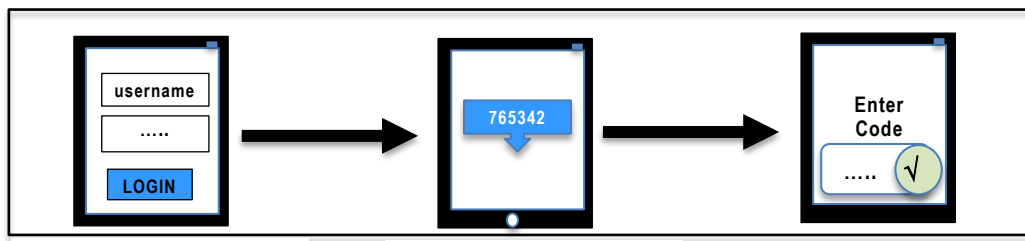


Fig. 10.2: Encryption Technique

- **Firewalls:** Business networks experience a constant inflow of incoming and outgoing traffic as employees try to access these networks several times a day from multiple locations. Firewalls act as a great first line of defense as they monitor the traffic. They are easy to implement and offer good resistance against external cyber threats trying to break into your networks. Businesses must implement a third-generation firewall that not only monitors their network traffic but also detects and blocks sophisticated cyber-attacks using in-line deep packet inspection.

- **Two-factor Authentication (2FA):** 2FA is one of the most important technologies for regular users, as it makes it far harder for attackers to gain unauthorized access to personal accounts. Verification of users will be a two-step process to make it more effective. This generally includes a combination of biometric information based on something the user knows (Username, password, pin), something the user has (ATM card, mobile phone) and something the user is (Biometric properties). Use of username and password control along with mobile based OTP is a widely used example of two factor authentication as shown in the following Fig. 10.3.



The user enters in their username and password

An authentication code is sent to the user's mobile device

The user enters in their authentication code to log into the application.

Fig. 10.3: Two Factor Authentication

- **Access Control:** The best way to curb insider security threats, as well as external unwanted entry to corporate devices and networks, is by restricting access to them. Access control ensures that only authorized parties access systems and data. Access control systems allow company IT admins to define who within the organization can access which files and networks. Access controls perform the steps of authentication and authorization to verify and validate whether a user is allowed to access data or not. Users are either allowed or blocked access to selective corporate resources. Most systems use user authentications to enable access to corporate data. Access control can be combined with Data Loss Prevention (DLP) to stop sensitive data from leaving the network.

- **Data Loss Prevention (DLP):** Data loss prevention systems help businesses secure their data against unwanted copying or deletion. It helps monitor the use of data, as well as detect any suspicious activities to prevent the leakage of confidential business information. Modern-day DLP systems help businesses tackle threats on multiple levels, including network data, device data, as well as cloud data.

mcq tha

10.5 DATA ANALYSIS

When most people think of "Business data," they automatically think about the numbers and statistics. But there are several types of business data:

- **Internal Data:** This type of data comes from business transactions such as point-of-sales and customer records. It provides insight into how your enterprise operates and the financial condition of the organization. Internal data includes any other information relevant to management, such as managerial performance metrics and productivity statistics.

- **External Data:** External data focuses on analyzing trends relating to consumers, competitors, markets, and suppliers. This category encompasses sources such as trade associations, government agencies, and trade publications.

- **Marketing:** Marketing data pertains to information about customers and their behaviors and preferences, which is used to target specific individuals with tailored messages. This type of data may include the various ways customers interact with your company, such as social media activity, web cookies, and advertising retargeting.

- **Structural:** Structural data is used to design or redesign physical infrastructure, such as building plans or blueprints that show how structural elements should be configured in each area. Data scientists often use mapping software for this purpose too.

Table 10.3 shows majorly the two categories of data.

Table 10.3: Categories of Data

Qualitative Data	Quantitative Data
Qualitative data asks "why," and consists of characteristics, attributes, labels, and other identifiers.	Quantitative data asks, "how much" or "how many," and consists of numbers and values.
Some examples of how qualitative data is generated include texts and documents, audio and video recordings, images and symbols, interview transcripts and focus groups and observations and notes.	Some examples of how quantitative data is generated include tests, experiments, surveys, market research and metrics.
Qualitative data is descriptive and non-statistical, as opposed to quantitative data.	Quantitative data is statistical, conclusive, and measurable, making it a more optimal candidate for data analysis.
It can be used to gain insights into a particular practice.	It helps in measuring the magnitude from a particular practice.
It does not have any predefined output categories.	It involves predefined output categories.
It can create patterns from insights and concepts.	It follows the test hypothesis statistical technique to gain insights and patterns from the data. It can numerically aggregate the data and the output categories can be clustered.
It can also perform an in-depth analysis of the data coming from a small sample.	It requires independent data from a large statistical sample.
The sampling involved is theoretical.	The sampling involved is statistical.

Refer Fig. 10.4.A well-organized data analysis practice helps in addressing business challenges and facilitate business decision making for complicated business questions by answering the questions like –

How can we improve our product and predict sales trends with effective marketing efforts?

How can we make it easier and faster for our customers to get what they need from us?

How do we beat out the competition and grow as a business and keep track of social media interaction?

How can we solve business problems like discovering new customers and ensuring customer retention with effective customer service?

Fig. 10.4: Commonly addressed business Challenges

The role of business data in business is changing rapidly as we move from companies using analytics to measure past performance to using them proactively to manage risk and increase profitability. There are four key insights that are commonly practiced in organizations. Refer Fig. 10.5 that depicts that Data provides an opportunity for -

Operational efficiency. Business data collected from the operations can be analyzed to improve business operations by reducing costs and improving efficiencies, businesses will become leaner and more competitive.

Abetter understanding of customers. Customer being the most critical component for any business carries valuable data. Collecting and analyzing behavioral and customer sentiment data helps understand customers better. These insights help staff in serving customers in a better way, they can sell more, provide a personalized customer experience, and increase customer retention.

New business models. Data is such a critical element nowadays that the data available in the public domain referred as Big Data can help in understanding market trends and other external factors that may impact business. In the age of "big data," companies need to learn how to harvest, use and monetize their own data.

Risk management. The future is uncertain; with technological transformations change will happen fast, and businesses will be unable to plan without good data on which to make decisions.

Fig. 10.5: Opportunities that Digital data provides

Data Analysis is a process of delving into raw data and drawing insights and conclusions from it. Data Analysis encompasses all aspects of analyzing digital data with the purpose of getting answers. It includes collecting, measuring, mining, filtering, visualizing, and optimizing data. You may already

be doing this using Google Analytics. Many data analysis software is available to make data analysis easier and faster. One of the most popular data analysis software, **Microsoft Excel** offers a range of data analysis features and Microsoft Power BI is an interactive data visualization software product developed by Microsoft with a primary focus on business intelligence.

By analyzing historical data, we can make better business decisions as we're more able to anticipate fluctuations in consumer demand, and to understand why these occur. However, it all depends on data quality and efficient data management, hence structured data is indispensable for effective data analysis. If the data is substandard or somehow unreliable, the business decisions cannot be optimized.

How can businesses use Data Analysis?

The stages involved in Data Analysis are as follows are depicted in Fig. 10.6.

quesns tha

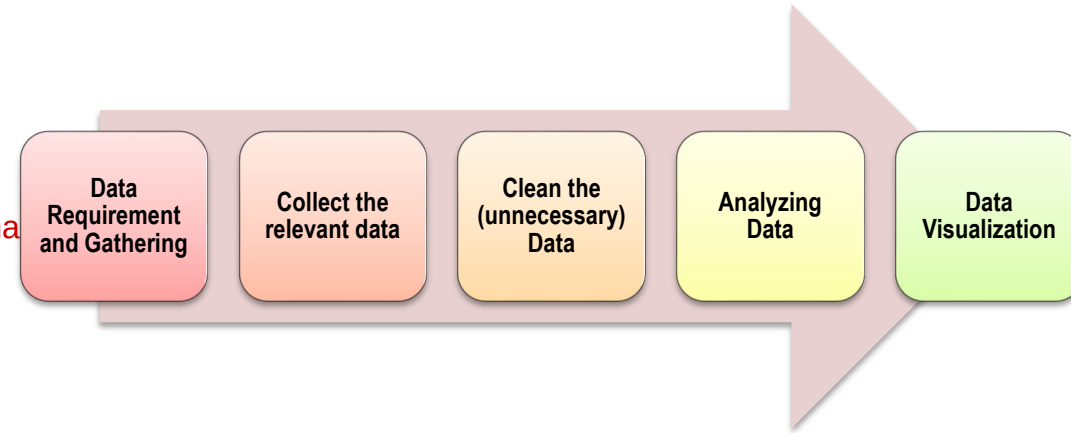


Fig. 10.6: Stages of Data Analysis Process

The explanation of these stages is provided in Table 10.4.

Table 10.4: Stages of Data Analysis

Data Requirement and Gathering	As a first step, Businesses must ensure that they have a long-term plan and clear objectives in mind. They must ask themselves questions about their data requirements like why they want to collect certain types of data and what they hope to achieve. It is therefore important that we define the question well, as a well-defined question will provide the relevant data that is required to be analyzed to achieve the desired output.
Collect the relevant data	Once businesses are clear in their own mind about the purpose of data analytics, they then need to determine which data sources are to be used, which data points need to be concentrated and how to collect that data.

	Some may simply use transaction and social media data, while others use high-tech sources including GPS and RFID chips.
Clean the (unnecessary) Data	Businesses must ensure that the quantitative data they collect is relevant and that they know how to make sense of it. Simply hoovering up huge quantities of data may prove to be actively counter-productive. Once data is collected from all the necessary sources, it needs to be tasked with cleaning and sorting, simply because not all data is *good* data. Data scientists must identify and purge duplicate data, anomalous data, and other inconsistencies that could skew the analysis to generate accurate results.
Analyzing Data	One of the last steps in the data analysis process is analyzing and manipulating the data which can majorly be done through different techniques. • Data Mining which is defined as "knowledge discovery within databases" that includes techniques like clustering analysis, anomaly detection, association rule mining, and others could unveil hidden patterns in data that weren't previously visible. • There's also business intelligence and data visualization software, both of which are optimized for decision-makers and business users. These options generate easy-to-understand reports, dashboards, scorecards, and charts. • Data scientists may also apply predictive analytics, which makes up one of the four data analytics used today (descriptive, diagnostic, predictive, prescriptive). Predictive analysis looks ahead to the future, attempting to forecast what will likely happen next with a business problem or question.
Data Visualization	Whatever the analysis method is used, we would get a set of data as results and a set of data visualized in the form of a chart. Data visualization with the help of tools like Tableau generate results in the form of charts and graphs that helps in interpreting and understanding the results.

10.6 DATA ANALYSIS TOOLS

As mentioned before, the data analysis can be performed in five stages - Data Requirement and Gathering, Data Collection, Data Cleaning, Analyzing Data, Data Interpretation, and Data Visualization. To achieve the above, many tools are available in the market. Let us discuss some of the most popular ones used through Table 10.5.

Table 10.5: Data Analysis Tools

Tools	Type	Availability	Mostly used for	Pros	Cons
Microsoft BI	Business analytics suite.	Commercial software (with a free version available).	Everything from data visualization to predictive analytics.	Great data connectivity, regular updates, good visualizations.	Clunky user interface, rigid formulas, data limits (in the free version).
Statistical Analysis System (SAS)	Statistical software suite.	Commercial.	Business intelligence, Multivariate and Predictive Analysis.	Easily accessible, business-focused, good user support.	High cost, poor graphical representation.
Tableau	Data Visualization tool.	Commercial.	Creating data dashboards, and worksheets.	Great visualizations, speed, interactivity, mobile support.	Poor versions control, no data pre-processing.
KNIME	Data integration platform.	Open source.	Data mining and machine learning.	Open-source platform that is great for visually – driven programming.	Lacks scalability, and technical expertise is needed for some functions.
MS Excel	Spreadsheet software.	Commercial.	Data wrangling and reporting.	Widely-use with lots of useful functions and plug-ins.	Cost, calculation errors, poor at handling big data.
Python	Programming Language.	Open source, with thousands of free libraries.	Everything from data scraping to analysis and reporting.	Easy to learn, highly versatile and widely used.	Memory-intensive – doesn't execute as fast as some other languages.
R	Programming Language.	Open source.	Statistical Analysis and data mining.	Platform independent, highly compatible, lots of packages.	Slower, less secure, and more complex to learn than Python.

10.7 DATA ANALYTICS

Data Analytics is taking the analyzed data and working on it in a significant and useful way to make well-versed business decisions and meaningful insights. These insights are then used to determine the best course of action like –

- When is the best time to roll out that marketing campaign?
- Is the current team structure as effective as it could be?
- Which customer segments are most likely to purchase your new product?

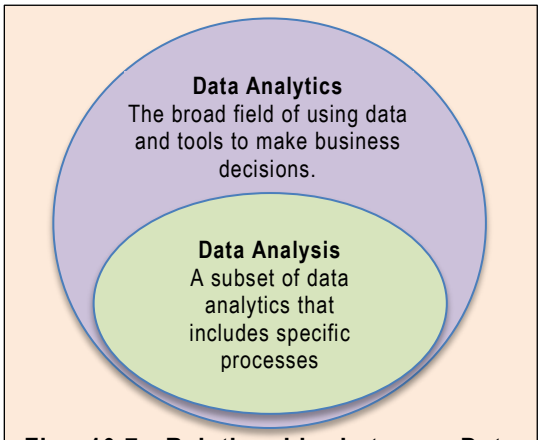


Fig. 10.7: Relationship between Data Analysis and Data Analytics

Refer Fig. 10.7 to understand Data Analysis and Data Analytics.

Data Analytics is a crucial driver of any successful business strategy. Nowadays, data is collected by businesses constantly: through surveys, online tracking, online marketing analytics, collected subscription and registration data, social media monitoring, among other methods. Various types of Digital analytics strategies can be used to track business performances, understand customers' behavior, evaluate the effectiveness of marketing channels etc.

Some of the key benefits of Data Analytics include the following:

- **Better decision making:** Data analytics allows businesses to sharpen their decision-making skills. Equipped with a more thorough understanding of their customer base and their own performance, they can use the insights obtained via data analytics to make improved decisions as well as making project management more effective.
- **Enhanced efficiency:** It is possible for businesses to streamline many of their processes, thus rendering them more efficient while also enabling them to cut costs. Thus, it also helps them with financial analysis, enabling them to deploy their resources more efficiently. For instance, with regard to targeted marketing campaigns.
- **Improved customer service:** Data analytics can also help businesses to improve their overall standard of customer service. Firstly, it provides in-depth insights into what customers want and their preferences. Secondly, storing data in a single central location and allowing your whole customer service team to access it can help to ensure better consistency of service quality.

Why should any business invest in digital analytics on a priority basis?

- In the current digital era, making informed decisions requires more than personal experience, intuition, or knowledge alone. Rapid changes demand real-time, data-based decision-making for business owners, researchers, and marketers alike.
- Businesses need to collect and process a huge amount of data for analysis to yield meaningful results. Handling huge data is not manually possible, hence Digital tools help to get the job done.

A digital analytics tool can provide historical knowledge and an understanding of customer's behavior so as to allow businesses to optimize customer experience based on data. Another possibility for businesses is to allow them to analyze their position in the market and benchmark against competition.

Types of Data Analytics

With a large amount of data getting generated on daily transactions across several industries around the globe, there comes a requirement to analyze the same for getting better business insights. Data Analytics techniques provide a viable solution in which the data can be extracted from multiple sources and is pre-processed which involves steps like validation, cleaning of data, etc. to segment it into various defined patterns. This comes under a stage called EDA (Exploratory Data Analysis) which helps in better understanding of the data and market trends. It helps in increasing the productivity and business acumen of an organization. The demand for data analytics has increased over the years. There are four major types of Data Analytics given below in Fig. 10.8.

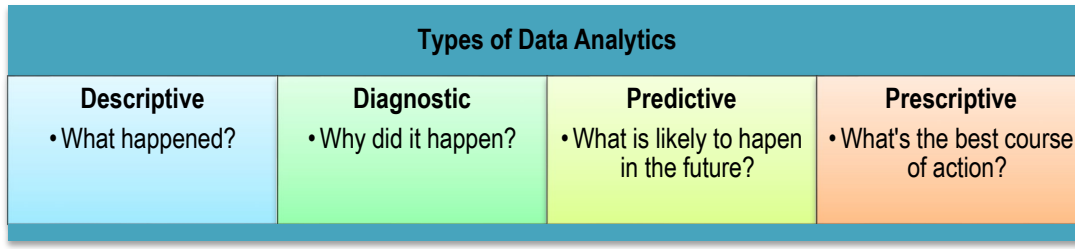


Fig.10.8: Types of Data Analytics

- **Descriptive Analytics:** This provides an objective, fact-based description of ***'what has happened'*** in the past, i.e. ***'A' occurred***. In other words, it describes what has occurred over a certain period of time. For example, processing and reviewing millions of customer sales transactions for last quarter doesn't give you the average amount spent by customers or total sales compared to previous quarters. Descriptive analytics is the first step in making sense of that raw data. It often uses basic mathematical operations to produce summary statistics

like average revenue per customer, that leads to a better understanding of the current state of your business. Once companies identify trends, they may plan other types of analysis and analyze causes and consequences of variations identified to improve business processes. Descriptive Analytics can be implemented by identifying the metrics that reflect key business goals of each group or of the company overall. If data is collected from multiple sources, it needs to be modeled into uniform structure so that it is ready for Descriptive analysis. Companies can use a variety of tools like spreadsheet applications or Business Intelligence (BI) software to generate visual representations for better understanding.

- **Diagnostic Analytics:** Diagnostic analytics not only focuses on what happened in the past, but also aims to describe the techniques used to answer questions like: ***'Why did this happen?'*** i.e. ***'A' occurred because 'B'***. It's like doing a deep dive into your data to search for valuable insights. To understand the "why" behind what happened, the first step is to set up the data investigation to identify the issues so that analysis can be initiated. There could be a single root cause, or there could be multiple data sets to isolate a pattern and find a correlation. Statistical techniques like Linear Regression can help find relationships by fitting a set of variables into a linear equation. For instance, the HR department might use this method to analyze employee performance, considering factors like quarterly performance levels, absenteeism, and weekly overtime hours.

- **Predictive Analytics:** Predictive analytics predict what is likely to take place in the relatively near term based on previous data for better decision making in business. In other words, it uses past data to forecast trends i.e. ***because 'A' occurred, we predict that 'C' will occur in the future***. The operation of predictive analytics is based on mathematical models, historical and current data. On par with traditional data analysis, predictive analytics utilizes artificial intelligence, machine learning and deep learning models and can look at all potential scenarios without human interference. In addition, cloud technologies enable real-time data processing and speed up decision-making.

  Predictive analytics software solutions help marketers and retail specialists in predictive marketing to optimize marketing campaigns, create personalized recommendations and forecast sales based on insightful data. This approach contributes to increased revenue and improved customer retention. Notably, predictive analytics finds applications across various industries such as healthcare, sports, weather, insurance, and financial modeling.

- **Prescriptive Analytics:** Prescriptive analytics is the process of using data to find out the best possible solution by including all significant factors. In other words, this aims to provide actionable steps towards a chosen goal i.e. ***To achieve goal 'X', we must take action 'Y'***. This analysis provides options that facilitate data-driven decision-making. This involves

extensive use of machine-learning algorithms. These algorithms process large amounts of data and using conditional statements make recommendations based on combination of specific requirements. For example - Investment decisions can be strengthened by Prescriptive analytics that considers risks and recommends whether to invest or not. Like nowadays investment decision in startups involves high risk and Prescriptive analytics can make this decision making effective. Prescriptive analytics can be used for detection and flagging of bank fraud, as huge volumes of transactions need to be reviewed that is not feasible manually. An algorithm—trained using customers' historical transaction data—analyzes and scans new transactional data for anomalies. The algorithm analyzes patterns in any transactional data, alerts the bank, and provides a recommended course of action like blocking the transaction.

Other types of data analysis techniques are used by developers like Descriptive Analysis, Inferential Analysis, Text Analysis, Statistical Analysis, Diagnostic Analysis, Predictive Analytics, and Prescriptive Analytics. But all of these can be categorized under either Quantitative or Qualitative Analysis techniques which are more generic. The methodology discussed above is contingent upon the specific requirements of the organization, including considerations such as setup cost, technological stack, business ideology, and customer needs.

10.8 DATA ASSURANCE

Data Assurance focuses on data quality and is important because we need:

- accurate and timely information to manage services and accountability.
- good information to manage service effectiveness.
- to prioritize and ensure the best use of resources.

Data Assurance can be achieved by an effective data quality management process by implementing a balanced set of practices to prevent future data quality issues and to cleanse data that does not meet the data quality Key Performance Indicators (KPIs) needed to achieve the established business objectives. The data quality KPIs will typically be measured on the core business data assets within the data quality dimensions as data uniqueness, completeness, consistency, conformity, precision, relevance, timeliness, accuracy, validity, and integrity. The data quality KPIs must relate to the KPIs used to measure business performance in general. The practices used to prevent data quality issues and eventual data cleansing includes these disciplines:

- **Data Governance:** Data governance (DG) is the process of managing the availability, usability, integrity, and security of the data in enterprise systems, based on internal data

standards and policies that also control data usage. Effective data governance ensures that data is consistent and trustworthy and doesn't get misused. It's increasingly critical as organizations face new data privacy regulations and rely more and more on data analytics to help optimize operations and drive business decision-making. A well-designed data governance program typically includes a governance team, a steering committee that acts as the governing body, and a group of data stewards. They work together to create the standards and policies for governing data, as well as implementation and enforcement procedures that are primarily carried out by the data stewards. Ideally, executives and other representatives from an organization's business operations take part, in addition to the IT and data management teams.

- **Data Profiling:** Data profiling is the process of examining, analyzing, and creating useful summaries of data. The process yields a high-level overview which aids in the discovery of data quality issues, risks, and overall trends. Data profiling produces critical insights into data that companies can then leverage to their advantage.
- **Data Matching:** Data matching refers to the process of comparing two different sets of data and matching them against each other. The purpose of the process is to find the data that refer to the same entity. Many a times, the data comes from two or more different sets of data and have no common identifiers. But data matching is also useful to detect duplicate data within a database.
- **Data Quality Reporting:** Data quality reporting is the process of removing and recording all compromising data. This should be designed to follow a natural process of data rule enforcement. Once exceptions have been identified and captured, they should be aggregated so that quality patterns can be identified.
- **Master Data Management (MDM):** Master data represents "data about the business entities that provide context for business transactions". The most found categories of master data are parties, products, financial structures, and locational concepts. Master data management (MDM) is a technology-enabled discipline in which business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency, and accountability of the enterprise's official shared master data assets.
- **Customer Data Integration (CDI):** Customer data integration (CDI) is the process of combining and organizing customer data from different databases into a single more usable and accessible form to enhance analytical capabilities. For example, a company might use data integration to run an ad campaign that targets their most engaged customers.
- **Product Information Management (PIM):** Product information management is the process of managing all the information required to market and sell products through distribution

channels. This product data is created by an internal organization to support a multichannel marketing strategy.

- **Digital Asset Management (DAM):** A digital asset management solution is a software and systems solution that provides a systematic approach to efficiently storing, organizing, managing, retrieving, and distributing an organization's digital assets. Digital Asset Management (DAM) can be used to refer to both a business process and a form of information management technology, or a digital asset management system. DAM functionality helps many organizations create a centralized place where they can access their media assets. The digital asset is a key component of the DAM process. It is any file type of value that is owned by an enterprise or individual, comes in a digital format, is searchable via metadata, and includes access and usage rights. There are many types of digital assets, including but not limited to Documents, Images, Audio content, Video, Animations, Media files, Graphics, Presentations, any digital media that includes the right to use etc.

10.9 INFORMATION TECHNOLOGY ACT, 2000 BASED REGULATORY COMPLIANCES

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament notified on 17th October 2000. India became the 12th nation in the world to adopt cyber laws by passing the Act. It is the primary law in India dealing with cybercrime and electronic commerce. 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 IT Act was amended in 2008. It introduced Section 66A which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism.

The provisions of the Information Technology Act 2000 and the amendments of 2008 are simple to understand and most of these are self-explanatory. In modern enterprises, most of the critical information is input, processed and stored in computers even in the 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.

The objectives of the Act are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper-based methods of communication.
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law.
- To facilitate electronic filing of documents with Government departments.
- To facilitate electronic storage of data.
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.
- To give legal recognition for keeping books of accounts by bankers in electronic form.
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

Some of the key issues of electronic information impacting enterprises and auditors are as follows:

- **Authenticity:** How do we implement a system that ensures that transactions are genuine and authorized?
- **Reliability:** How do we rely on information which does not have physical documents?
- **Accessibility:** How do we gain access and authenticate this information, which is digital form?

What are the privacy requirements under the Information Technology Act?

Under the Act, the Ministry of Electronics & Information Technology of India, develops and promulgates specific rules and regulations. In 2011, the newly enacted privacy rules established a comprehensive set of privacy and personal data protection requirements. The Indian privacy regime is quite strict, for example - a written consent is required for collection and processing of personal data (a letter, fax or email shall normally suffice).

The Rules offer special protection for Sensitive Personal Information (SPI) that includes passwords, financial information, credit card and debit card details, physical, physiological, and mental health conditions, sexual orientation, medical records and history, and biometric information of individuals.

Under the Rules, all organizations, collecting personal data, must develop and make readily accessible a privacy notice that would clearly elaborate what personal data is being collected from the individuals, for what purposes and duration, and with whom it will or may be shared. Likewise, the privacy notice must explain how personal data is being protected from cyber-attacks and unlawful access.

What are the cybersecurity requirements under the Information Technology Act?

The above-mentioned "Information Technology Rules" also address cybersecurity and data protection questions by mandating all entities that collect or process personal data, to comply with reasonable security practices and procedures.

Furthermore, the requisite compliance must be thoroughly documented to explain implementation of adequate managerial, technical, operational, and physical security controls. The ISO 27001 standard is expressly mentioned as an example of the reasonable security standard that evidences proper adherence to the data security requirements imposed by the Rules under the Act. An independent external entity shall certify compliance with such a standard by the virtue of annual security audits.

In a nutshell, under the Rules, virtually all Indian companies, as well as foreign businesses that do business in India, are required to abide by the norms of ISO 27001 or another similar standard. Among the specific security measures required to comply are holistic IT asset inventory, information classification, regular risk assessments, continuous security monitoring, incident detection and response plan, security training and awareness program, annual penetration testing and ongoing vulnerability scanning for external systems that process or store personal data.

Additionally, individuals whose personal data is stolen due to poor or insufficient cybersecurity practices in violation of the above-mentioned Rules, may also file a civil lawsuit claiming damages under Section 43A of IT Act 2000.

Keys Provisions of IT Act

The IT Act provides the legal framework for electronic governance by giving recognition to the electronic records and digital signature. It also deals governing of various nature of cybercrimes and facilitate electronic commerce. It also prescribes penalties provisions in case of violations of the requirements of the IT Act.

I. Relevant terminologies under the Information technology Act, 2000:

The IT Act, 2000 defines the terms **Access** in Section 2(a), **computer** in Section 2(i), **computer network** in Section (2j), **data** in Section 2(o) and **information** in Section 2(v). These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime.

2(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;

2(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;

2(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;

2(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;

2(v) **"Information"** includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated microfiche;

In a cyber-crime, computer or the data are the target or the object of offence or a tool in committing some other offence. The definition of term computer elaborates that computer is not only the computer or laptop on our tables, as per the definition computer means any electronic, magnetic, optical or other high speed data processing devise of system which performs logical, arithmetic and memory function 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. Thus, the definition is much wider to include mobile phones, automatic washing machines, micro-wave ovens etc.

II. Some of key provisions of IT related offences:

In case of violation of any compliances related to the cyber security and of privacy requirements, punishments and penalties are prescribed under the said Act. Following are the relevant penalties:

- **Section 43:** Penalty and compensation for damage to computer, computer system, etc.
- **Section 43A:** Compensation for failure to protect data.
- **Section 65:** Tampering with Computer Source Documents.
- **Section 66:** Computer Related Offences.
- **Section 66B**: Punishment for dishonestly receiving stolen computer resource or communication device.
- **Section 66C**: Punishment for identity theft.
- **Section 66D:** Punishment for cheating by personation by using computer resource.
- **Section 66E:** Punishment for violation of privacy.
- **Section 66F:** Punishment for cyber terrorism.
- **Section 67:** Punishment for publishing or transmitting obscene material in electronic form.
- **Section 67A:** Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.
- **Section 67B:** Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

[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 incharge 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 database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database 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 thereunder;

(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) steal, 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, know-ledge, 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 rearrange 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 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 program, 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. The explanation clarifies that '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 5 lakh rupees or with both.

[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 for 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 that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

[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

(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.

10.10 DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Personal data is information that relates to an identified or identifiable individual. Businesses as well as government entities process personal data for delivery of goods and services. Processing personal data allows understanding preferences of individuals, which may be useful for customization, targeted advertising, and developing recommendations and may also aid law enforcement. Unchecked processing may have adverse implications for the privacy of individuals, which has been recognized as a fundamental right, that may further subject individuals to harm such as financial loss, loss of reputation, and profiling.

The Digital Personal Data Protection Act, 2023 (DPDP Act or DPDPA-2023) is an Act of the Parliament of India to provide for the processing of digital personal data within the territory of India in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. The DPDP Act is India's first data protection act, and it establishes a framework for the processing of personal data in India.

Highlights of The Act

- **Applicability:** The Act applies to the processing of digital personal data within India where such data is either collected online or collected offline and is digitized. It will also apply to the processing of personal data outside India if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing is defined as either wholly or partially automated operations, or a set of operations, performed on digital personal data. This includes collection, storage, use, and sharing of such data.
- **Consent:** Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. Notice that should contain details about the personal data to be collected and the purpose of processing, must be given before seeking consent. Consent may be withdrawn at any point in time and will not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by an individual voluntarily, (ii) provision of benefit or service by the government, (iii) medical emergency, and (iv) employment. For individuals below 18 years of age, consent will be provided by the parent or the legal guardian.
- **Rights and duties of the data principal:** An individual/citizen whose data is being processed (data principal), will have the right to (Fig. 10.9):

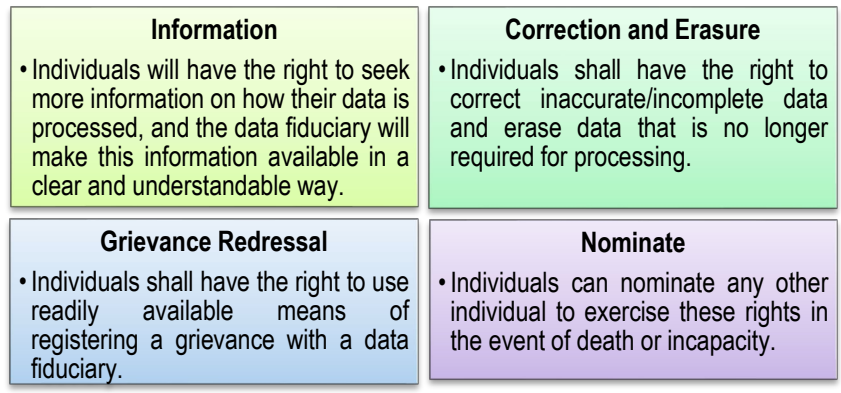


Fig.10.9: Rights of Data Principal

Data principals will have certain duties, the violation of which will be punishable with a penalty of up to ₹ 10,000. They must not: (i) register a false or frivolous complaint, and (ii) furnish any false particulars or impersonate another person in specified cases.

- **Obligations of data fiduciaries:** The entity determining the purpose and means of processing, (data fiduciary), must: (i) make reasonable efforts to ensure the accuracy and completeness of data, (ii) build reasonable security safeguards to prevent a data breach, (iii) inform the Data Protection Board of India and affected persons in the event of a breach, and (iv) erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). In the case of government entities, storage limitation and the right of the data principal to erasure will not apply.
- **Transfer of personal data outside India:** The Act allows transfer of personal data outside India, except to countries restricted by the central government through notification.
- **Exemptions:** Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases. These include: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of the Act. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.
- **Data Protection Board of India:** The central government will establish the Data Protection Board of India. Key functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons. Board members will be appointed for two years and will be eligible for re-appointment. The central government will prescribe details such as the number of members of the Board and the selection process. Appeals against the decisions of the Board will lie with Telecom Disputes Settlement & Appellate Tribunal (TDSAT).
- **Penalties:** The schedule to the Act specifies penalties for various offences such as up to: (i) ₹ 200 crore for non-fulfilment of obligations for children, and (ii) ₹ 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry.

The General Data Protection Regulation (GDPR)

The DPDPA is similar to **The General Data Protection Regulation (GDPR) of the European Union.** The GDPR is unified data privacy laws across the European Union (EU) and European Economic Area (EEA). The objective of the GDPR is to protect individuals and data that describes them and also ensure that the organization must collect that data in a responsible manner. The GDPR strengthens the individual's fundamental rights in this digital age by protecting their personal data from unauthorized access, use, disclosure or destruction and also facilitates the organizations by clarifying rules for companies and public bodies in the digital market. Indian government designates data fiduciary (data Controller) or a class of data fiduciary on the basis of volume and sensitivity of personal data it needs to process; risk to the data protection rights of the data principals; potential impact on the sovereignty and integrity of country; risk to electoral democracy; security of the state and public order to carry out risk mitigation measures. European countries have national bodies that are responsible for protecting personal data. The GDPR established the European Data Protection Board which is an independent European body that ensures the consistent application of data protection rules throughout the EU.

Principles of The General Data Protection Regulation

The GDPR follows seven principles which are based on its regulations and rules of compliance related to personal data of individuals. These are as follows:

- **Lawfulness, fairness and transparency:** It states that the individuals should be clearly informed about the purpose for which their data will be used. The processing of data should be lawful, fair and transparent.
- **Purpose Limitation:** It states that data should be collected only for specific purpose. The organizations should explicitly outline the end goal for which the data is collected, and the time required to carry out that goal.
- **Data minimization:** The data collected should be collected in the smallest amount that is absolutely necessary for specific purpose. Organizations cannot collect personal data for the possibility that it could be useful later on.
- **Accuracy:** The data collected by the organization should be accurate and up-to-date. The data should be changed whenever a request is made.
- **Storage limitation:** The data should be stored as long as it is necessary for specific purpose. After an organization no longer requires personal data, for the reason for which it was gathered, it should be deleted.

- **Integrity and confidentiality:** The processing of data should use appropriate protection measures to ensure security, integrity and confidentiality of data.
- **Accountability:** The data controller should be responsible for ensuring the data is in compliance with the GDPR. This indicates that organizations should be able to provide evidence of the measure they have taken to ensure compliance.

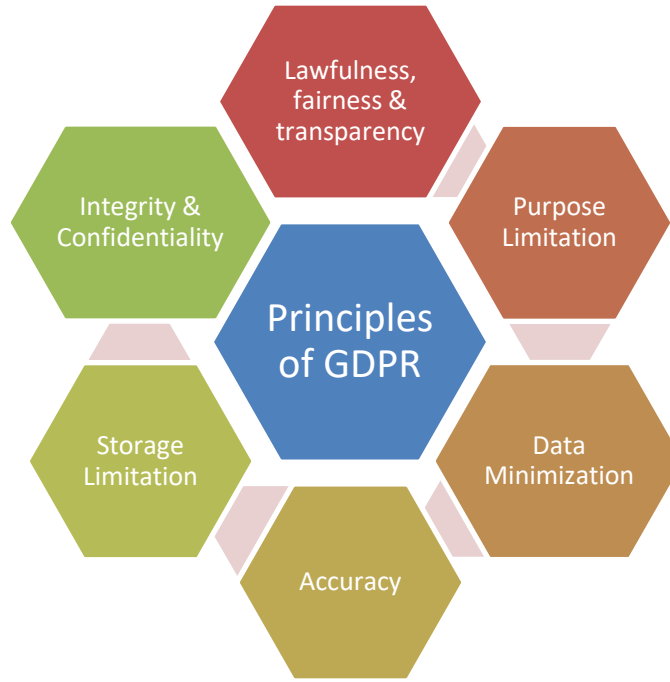


Fig.10.9: Principles of the GDPR

Similarities between GDPR and DPDPA: The DPDPA follows many similar principles with those set out in the GDPR and specifies the rules for data processor and right for data principals. Both the DPDPA and the GDPR work on data protection, and contain similar provision for the security measures to be adopted while processing personal data, hence have many similarities which are as follows:

- Both of them impose obligations to organizations that process personal data such as report data breaches to relevant authority.
- Both contain the provisions for enforcement and penalties in case of non-compliance of regulation.
- Both the DPDPA and the GDPR permit an individual, number of rights over personal data such as the right to erase, object and access to the processing of personal data.

Difference between the DPDPA and the GDPR

- The DPDPA is applicable to all organizations that process personal data of individuals irrespective whether the organization is located in India or not whereas the GDPR is applicable to all organizations that process personal data of individual located in European Union, irrespective whether the organization is located in EU or not.
- The DPDPA is applicable to all personal data excluding data available publically. There is no special category of data whereas the GDPR is applicable to data available publically in scope. It recognizes the special categories of data such as racial origin, philosophical or political views.
- On the grounds of processing, the DPDPA is consent centric and has lesser legitimate interest for processing. The GDPR has broader legitimate interests for processing.
- The GDPR is applicable to all personal data whether data is digitized or not whereas the DPDPA is applicable to only personal digitized data.
- In GDPR, the age of consent ranges between 13-16 years depending on the individual member state while in the DPDPA the age of consent is 18 years. The processing of the data of an individual below 18 years needs "verifiable parents consent".

SUMMARY

The chapter has provided deep insight into the security mechanisms related to data. The discussion is on Data protection that safeguards information from loss through backup and recovery, whereas data security that refers specifically to measures taken to protect the integrity of the data itself against manipulation and malware. It provides defense from internal and external threats. Data privacy refers to controlling access to the data. Furthermore, the discussion is on Digital Personal Data Protection Act, 2023 that provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Mr. Neeraj is working on a project on healthcare system where he has to perform data analysis on the database of patients of last five years in ABC Hospital. The hospital provided him inconsistent data with lots of errors, duplicate and missing values. He has to apply various techniques to get rid of these anomalies. Identify from the following process which he can use to get rid of these anomalies.

   (a) Cleaning of data

   (b) Selection of data

   (c) Integration of data

   (d) Data Visualization

2. The key provisions of IT related offences are for the smooth working of bank. In purview of same, what is the primary objective of SPI?

   (a) Protecting Computer Software

   (b) Securing critical Information

   (c) Sensitive Personal Information

   (d) Identifying sensitive Information

3. Which of the following is not a type of Data Analytics technique?

   (a) Descriptive

   (b) Deductive

   (c) Predictive

   (d) Prescriptive

4. What does the term “data security” encompass?

   (a) It is the protection of physical assets of an organization.

   (b) It provides tools and policies to restrict access to the data.

   (c) It is to ensure the integrity of data.

(d) It is a guideline for how data should be collected or handled, based on its sensitivity and importance.

5. ABC Corporative bank strictly follows the policy of Sensitive Personal Information. Choose the attribute that is not defined as Sensitive Personal Information.

(a) Home address

(b) Password

(c) Financial information

(d) Biometric information

ANSWERS/SOLUTIONS

1.	(a)	2.	(c)	3.	(b)	4.	(c)	5.	(a)

CHAPTER 11

BUSINESS INTELLIGENCE

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- establish an understanding about the concept of Business Intelligence (BI) and its functionalities.
- appreciate the usage of BI tools in organizations.

CHAPTER OVERVIEW

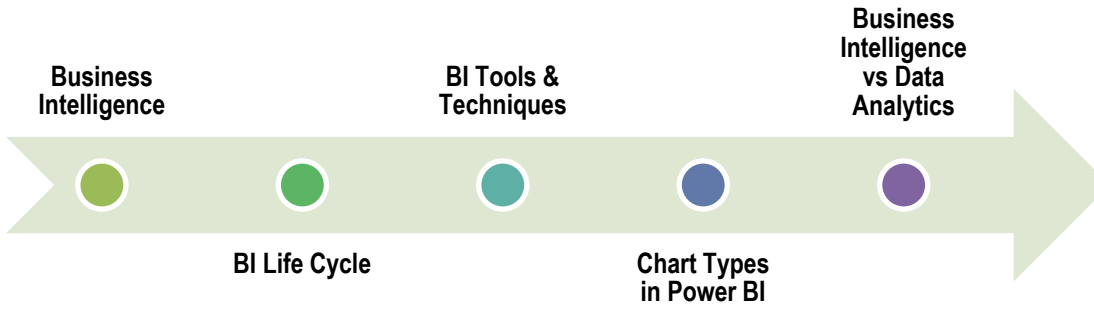


Illustration : Heathrow Airport

The challenge: Heathrow airport is an international airport in London. It is the second busiest international airport in the world after Dubai international airport and the seventh largest in terms of total passenger traffic managing 2,00,000 passengers every day.

Every department needs to be in absolute coordination and sync to be able to manage the passenger traffic and give them a smooth experience at the airport. At such busy airports, every day brings new challenges and uncertainties with it. Unexpected disruptions in the smooth workflow of operations at the airport disturb the entire functioning. Issues can arise due to stormy weather, delayed flights, canceled flights, shifts in jet streams, etc. disturbing the airport's smooth functioning. Such problems send the passengers as well as airport employees into turmoil.

The airport needed a **Central Digitized Management System** as a solution to this problem. Such a system would use the large amounts of data being produced by operational systems at the airport and transform it into useful visual insights. The interpretations produced by the BI tool can be used by airport staff for better functioning and passenger management.

The Change: Heathrow group went with Microsoft Power BI as their BI software and Microsoft Azure for cloud services. The airport deployed Microsoft Azure technology to collect data from back-end operational systems at the airport. These systems are check-in counters, baggage tracking systems, flight schedules, weather tracking systems, cargo tracking and many more. The operational data from these systems are forwarded to business intelligence platforms like Power

BI. In Power BI, users shape this data into useful information that the airport staff can use. Power BI transforms crude information into informative visuals showing different statuses and statistics of the airport systems. Then, the ground staff like baggage handlers, gate agents, air traffic controllers, etc. uses this information to properly operate and manage passengers.

Services such as Azure Stream Analytics, Azure Data Lake Analytics, and Azure SQL Database are used to extract, clean and prepare operational data in real-time. This data is about flight movements, security queues, passenger transfers, and immigration queues. Ultimately, Power BI uses data from these Azure services for analysis and interpretation. Operational data from different data sources come into Power BI that transforms data into meaningful insights with the help of visual reports, graphics, and dashboards. About 75,000 airport employees have information on their fingertips by virtue of Power BI.

With the presence of smart BI solutions like Power BI, airport staff is notified in advance about the probable delays and the sudden rush of passengers at the airport. This helps management groups and other employees to take suitable actions in advance like increasing the food stock, adding extra passenger buses, increasing the ground staff, directing the passengers to the waiting area, etc. to avoid any last-minute hustle. Thus, with the help of a powerful BI tool like Power BI, Heathrow has benefited in more than one way. They are extremely happy and satisfied with the capabilities of Power BI helping them give a hassle-free airport experience to their passengers. Heathrow also is extending Power BI applications by trying to anticipate passenger flow at the airport to avoid any unexpected disruptions for the passengers.

11.1 INTRODUCTION

Business Intelligence (BI) is all about turning an organization's data into insights that can be used to inform business decisions. In other words, Business Intelligence is the process of analyzing unprocessed data and turning it into knowledge that the company can use to make decisions. BI analysts will use BI tools, software, or services to access and analyze datasets and translate their findings into reports, summaries, dashboards, graphs, charts, or maps. In recent years, the advent of modern data visualization and reporting tools has transformed the discipline, empowering businesses to use big data insights to identify, develop and create new business opportunities. Business intelligence enables organizations to gain a deeper understanding of their marketing strategies, financial performance, effective development, and management, as well as market trends and consumer behavior.

Functionalities of Business Intelligence

- **Analytics:** This refers to a BI technique that explores data to extract trends and insights from historical and current findings, facilitating valuable data-driven decisions. The BI solution analyzes raw data through techniques such as seasonal and trend analysis, 'what if' scenarios, and modeling using various data modeling techniques and similar functionalities.
- **Dashboards:** The solution provides dashboards which help the business to monitor, measure and manage business performance in a very quick manageable way. Interactive collections of role-relevant data are typically stocked with intuitive data visualizations, KPIs, analytics metrics and other data points that play a role in decision-making.
- **Data mining:** This practice uses statistics, database systems and machine learning to uncover patterns in large datasets. Data mining also requires pre-processing of data. End-users use data mining to create models that reveal patterns.
- **Extract Transfer Load (ETL):** This tool extracts data from data-sources, transforms it, cleans it in preparation for reports and analysis, and loads it into a data warehouse.
- **Model Visualization:** Some of the BI solutions provide advanced analytics and visualization capabilities enabling real time visualization in different forms and methods and to augment additional functionalities. The model visualization technique transforms facts into charts, histograms, and other visuals to support correct insight interpretation.
- **Online Analytical Processing (OLAP):** OLAP is a technique for solving analytical problems with multiple dimensions from various perspectives. OLAP is useful for completing tasks such as performing CRM data analysis, financial forecasting, and budgets.
- **Predictive modeling:** It is a BI technique that utilizes statistical methods to generate probabilities and trend models. With this technique, predicting a value for specific data sets and attributes using many statistical models is possible.
- **Reporting:** The solution provides very comprehensive functionalities for creating reports for better understanding of the business data. Business users can create, view, modify reports and visualizations online and offline and with other office products. Reporting involves gathering data using various tools and software to mine insights and provides observations and suggestions about trends to simplify decision-making.
- **Scorecards:** Business Intelligence solutions provide industry standard scorecards to enable the business to measure the Key Performance Indicators (KPIs). Visual tools such as BI dashboards and scorecards provide a quick and concise way to measure KPIs and indicate how a company is progressing to meet its goals.

- **Real time monitoring:** The BI solution offers tools to analyze operational data in real-time, up to the the limit to seconds, thereby enabling businesses to make quick and informed decisions.
- **Collaborative Business Intelligence:** BI solution provides capabilities to collaboratively share information with different stakeholders within the organization and outside.
- **Mobile Business Intelligence:** The BI solution offers functionalities to make information, such as reports, dashboards, and monitoring, accessible on mobile devices.

11.2 BUSINESS INTELLIGENCE LIFE CYCLE

Business Intelligence provides the proper approach for the data analysis and decision-making process. It helps the business to achieve goals and gain profits. The overall phases of business intelligence make the further development and maintenance process easy.

To gather, integrate, analyze, and present data in a way that helps corporate decision-making, BI entails the use of technology, tools, and methodologies. Data warehouses or data marts are frequently used to store and manage the data in BI, which includes a variety of activities like data mining, reporting, dashboards, and visualizations. By offering insights into operations, clients, and markets, BI ultimately aims to assist organizations in making more educated and data-driven decisions. Businesses can use BI to find growth possibilities, streamline processes, and enhance overall performance.

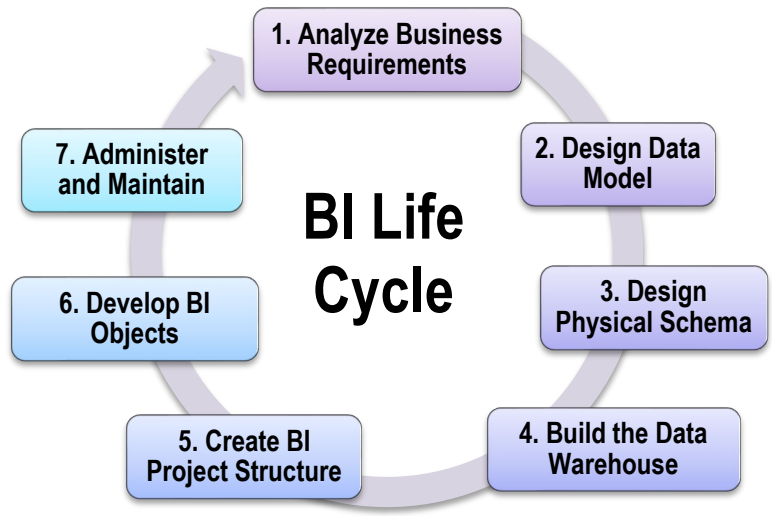


Fig. 11.1: Business Intelligence Life Cycle

Phase 1: Analyze Business Requirements

The first step in the Business Intelligence life cycle is to analyze the business requirements. The user identifies the business requirements to determine the type of analysis that the user then needs to perform. Identifying the requirements let the users decide the further action to be performed. For example - any retail company can analyze the sales data to figure out the products that are top-selling and the products that least sell.

Phase 2: Design Data Model

Once the requirements are identified, the user needs to design the logical model according to the requirements. This logical model helps the user to analyze the relationships that exist within the data entities. For example - for any retail company, the data model consists of products, their customers, and the sales data.

Phase 3: Design the Physical Schema

Once the logical model is prepared, the next step is to design the physical schema using the data model that describes the structure and the content of the data warehouse. For example - in any retail company, physical schema consists of sales-related facts, product-customer relationships, and the sales transactions.

Phase 4: Build the Data Warehouse

Once the logical and physical schema is designed, the next step is to build the data warehouse. The design of a data warehouse depends on the physical and logical schema. After the design of the data warehouse, the data and the content from the source system are loaded into the data warehouse for further steps. For example - for the retail system, designing the data warehouse consists of developing a database that would store the details of customers, products, and other requirements for the business.

Phase 5: Create BI Project Structure (Metadata)

The next step after designing the data warehouse is to create a project structure also known as metadata. With the help of this created project structure, the mapping of the tables and data in the data warehouse is easier. Creating the project structure describes the further steps and types that need to be implemented. For example - the project structure of the retail company consists of the attributes of the data, the design, and the working flow of the system. This project structure or metadata gives a brief idea about the working of the system.

Phase 6: Develop the BI Objects

The next step is to develop the BI objects such as metrics, attributes, dashboards, reports, and facts. This step consists of developing the reports and dashboards that can be used to analyze the data in the data warehouse. For example - the retail company can develop reports and statistics charts that can describe the profit and loss margins.

Phase 7: Administer and Maintain the Project

The last step is to administer and maintain the project continuously as it undergoes changes. The project needs to be monitored to maintain the changes, security, and performance of the system. For example - the retail company needs to monitor the reports and statistics accordingly to increase the profit from the sales.

11.3 BUSINESS INTELLIGENCE TOOLS

BI tool is an application software that collects, processes, and analyzes large amounts of structured and unstructured data from both internal and external systems. These tools pool this data together which is collected from numerous databases, portals, Customer Relationship Management (CRM) systems, Enterprise Resource Planning (ERP) systems, and more. Data sources might include documents, images, email, videos, journals, books, social media posts, files and more. BI tools find this information through queries which can present the data in user-friendly formats such as reports, dashboards, charts, and graphs. This leads to an outcome that offers all the employees of an organization the power to make improved decisions, pinpoint upcoming potentials for revenue, identify the latest opportunities for growth, increase business efficiency, interpret market trends, and more.

Why do we use BI Tools?

- **Centralized data:** BI tools can perform functions such as data mining, data visualization, performance management, analytics, reporting, text mining, predictive analytics, and much more. BI tool brings the entire data in one place and delivers certain types of views (issues, trends, analytics) based on users' queries or what s/he wants to know. As a result, employees can harness this information to make better decisions based on predictions, market trends, and Key Performance Indicators (KPIs).
- **Agile decision making:** BI tools can help organizations in understanding and analyzing their operations efficiently and effectively, thereby leading to smart, agile decision making to achieve toward accomplishing organizations objectives. These tools enable seamless scalability of users across various business enterprises - from single users to hundreds of users without significant shift in costs.

- **Automatic reports:** Instead of inputting data manually into Excel spreadsheets or toggling between different tools, many BI tools are automated. BI tools allow the integration of powerful reporting software like crystal reports which can be customized for usage by customers, board directors, managers, and personnel. Availability of the BI tools on cloud enables fast and real-time access to crucial data despite location. Data can be integrated and formatted from different sources, and this enables managers to run various ad-hoc reports. Improved business processes lead to enhanced efficiency and productivity.
- **Easy to be exported:** Insights are provided for both historical and real-time data. Resulting reports can be exported in various user-defined formats like Excel, PDF, or PowerPoint presentations. Users monitor various analytical metrics from a user-friendly dashboard that can be customized to suit user-preferences. This real-time access to crucial data enables decision-makers to act as it arises. In the end, BI tools are great for mitigating risk and enhancing efficiency.
- **Compatible and Integrated:** Centralization of the company's database promotes collaboration between different departments while eliminating the duplication of resources. Some BI tools are open source that allows for customization and integration with other applications. Data is arranged in columns with users having access to various analytical filters. Analysis reports produced can be shared to colleagues through email at scheduled intervals. BI generated charts, graphs and visualization can be integrated with existing customized applications.
- **Reduces business costs:** BI tools can do so much from analyzing consumer behavior and sales forecasting to real-time process monitoring, that analyzing, planning, and reporting processes are way more efficient and accurate than ever before.
- **Make predictions:** With access to so much data from the past and present, employees can make evidence-based decisions. Predictive analytics and forecasting enable users to generate insights based on a product or service's performance history. If a business condition changes, the intelligent tools can automatically figure out the anomalies and users will be able to react to disruptions as they arise.

Table 11.1: Popular BI Tools

Microsoft Power BI: Power BI is one of the most popular and widely used BI tools, developed by the leading software giant Microsoft. This interactive tool provides an environment for the analysis, integration, and visualization of data and can easily sync with sources such as Facebook, Oracle, and more, generate reports and dashboards in minutes. It comes with built-in AI capabilities, Excel integration, and data connectors, and

offers end-to-end data encryption and real-time access monitoring and is efficient and effective in assisting organizations to make informed business decisions.

For example - ABB Italy needed an innovative system that would provide greater market analyses and visual reporting for its manufacturing branch. Initially, it built its own solution, but their system meant reports were generated through a third-party IT supplier. Reports took up to four weeks to come through, which was frustrating and inefficient. As a result, ABB Italy adopted a Power BI system that can generate customized reports in just a few hours. This reduces reliance on external suppliers and allows stakeholders to develop more insightful reporting.

Tableau: Tableau is an excellent data visualization and BI tool, widely used for reporting and analyzing vast volumes of data. It helps users create different charts, graphs, maps, dashboards, and stories for visualizing and analyzing data, to help in making business decisions. Tableau is known for its user-friendly data visualization capabilities, but it can do more than make pretty charts. Their offering includes live visual analytics, an interface that allows users to drag and drop buttons to spot trends in data quickly. The tool supports data sources such as Microsoft Excel, Box, PDF files, Google Analytics, and more. Its versatility extends to being able to connect with most databases.

QlikSense: QlikSense is a BI tool that emphasizes a self-service approach, meaning that it supports a wide range of analytics use cases, from guided apps and dashboards to custom and embedded analytics. It offers a user-friendly interface optimized for touchscreens, sophisticated AI, and high-performance cloud platforms. Its associative exploration capability, Search and conversational Analytics allows users to ask questions and uncover actionable insights, which helps increase data literacy for those new to using BI tools.

Dundas BI: Dundas BI is a browser-based BI tool that features a drag-and-drop function allowing users to analyze data on their own, without involving their IT team. The tool is known for its simplicity and flexibility through interactive dashboards, reports, and visual analytics. Since its inception as a data visualization tool, it has evolved into an end-to-end analytics platform that is able to compete with the new BI tools available today.

Sisense: Sisense is a user-friendly BI tool that focuses on being simplified and streamlined. With this tool, users can export data from sources like Google Analytics, Salesforce, and more. Its in-chip technology allows for faster data processing compared to other tools. Key features include the ability to embed white-label analytics, meaning a

company can fully customize the services to its needs. Like others, it also has a drag-and-drop features and allows users to share reports and dashboards with their team members as well as externally.

Other popular BI tools include Zoho Analytics, Oracle BI, SAS Visual Analytics, Domo, Datapine, Yellowfin BI, Looker, SAP Business Objects, Clear Analytics, Board, MicroStrategy, IBM Cognos Analytics, Tibco Spotfire, BIRT, Intercom, Google Data Studio, and HubSpot.

11.4 CHART TYPES IN POWER BI

Following are popular chart types available in Power BI:

1. **Line Charts:** Line charts are mostly used charts to represent the data and are characterized by a series of data points connected by a straight line. Each point in the line corresponds to a data value in the given category. It shows the exact value of the plotted data. Line charts should only be used to measure the trends over a period, e.g. dates, months, and years.

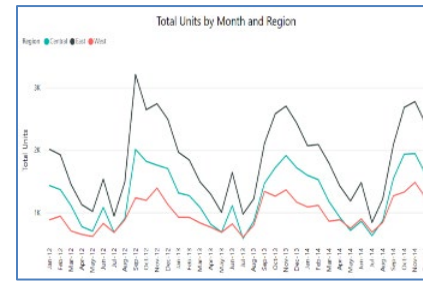


Fig. 11.2: Line Chart

Refer Fig. 11.2 which displays an example of a line chart representing total units sold month and region wise.

2. **Bar Charts:** Bar charts mostly use graphs because they are simple to create and easy to understand. Bar charts are also called horizontal charts that represent the absolute data. They are useful to display data that include negative values because it is possible to position the bars above and below the x-axis. Fig. 11.3 is an example of a Bar chart representing outstanding control tests moth wise.

Fig. 11.3: Bar Chart

3. **Pie Charts:** A pie chart is a circular statistical chart, and it shows the whole data in parts. Each portion of a pie chart represents the percentages, and the sum of all parts should be equal to 100%. The whole data can be divided into slices to show the numerical propositions of each part of the data. Pie charts are mostly used to represent the same category of data. It helps users to understand the data quickly. They are widely used in education, the business world, and communication media. Fig. 11.4 is an example of a pie chart representing product-wise data highlighting percentage distribution.

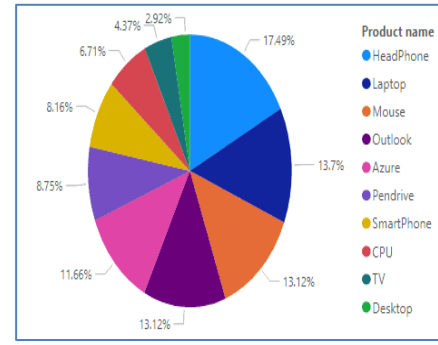


Fig. 11.4: Pie Chart

4. **Doughnut Charts:** Doughnuts are like pie charts, and it is named doughnut chart because it looks like a doughnut. You can easily understand the data because doughnut charts show the whole data into the proposition. It is the most useful chart when you need to display various propositions that make up the final value. Fig. 11.5 is an example of a doughnut chart representing cost price, profit, margin, and tax distribution for a product.

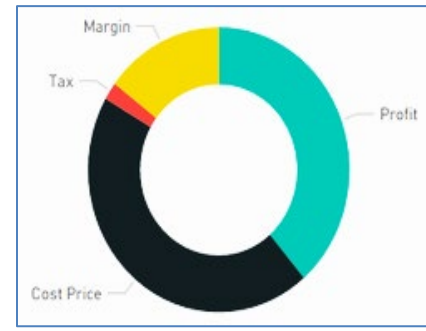


Fig. 11.5: Doughnut Chart

5. **Funnel Charts:** The funnel chart is a type of chart which is used to visualize the data that flows from one phase to another phase. In the funnel chart, the whole data is considered as 100%, and in each phase, it is represented as numerical propositions of the data. Fig. 11.6 is an example of a funnel chart presenting various stages of the recruitment process in respect to the total number of applications.

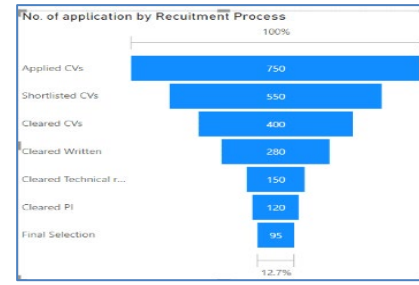


Fig. 11.6: Funnel Chart

11.5 BUSINESS INTELLIGENCE VS DATA ANALYTICS

Refer Table 11.2 for Business Intelligence vs Data Analytics.

Table 11.2: Business Intelligence vs Data Analytics

Business Intelligence	Data Analytics
Refers to the ***information required to enhance business decision-making activities.***	Refers to ***modifying the raw data into a meaningful format.***
The prime purpose is to provide support in decision-making ***using actionable insights*** obtained through data analytics and help organizations grow their business.	The prime purpose is to model, cleanse, predict, and transform the raw data ***into actionable insights*** as per the business needs.
Primarily concerned with ***looking back*** to see what has already occurred, using this information to inform future strategy.	While data analytics also identifies past patterns, it often uses these data to ***forecast*** what might occur in the future.
Utilizes ***structured data***, i.e. data stored in warehouses, tabulated databases, or other systems. These data are used to produce dashboards and reports.	Also uses structured data, but usually begins with ***unstructured, real-time data***. One task of data analysts is to clean and order these data, before storing them for future analysis.
Is primarily used by ***leadership teams and non-technical personnel, such as chief executives, financial directors, or chief information officers***.	Is usually the ***preserve of analysts, data scientists, and computer programmers*** who have a more technical focus?
Usually thinks in 'blue sky' terms, asking ***high-level strategic questions*** about an organization's overall direction.	Tends to ***focus on a single issue*** or question, e.g. 'Why are sales on product A dropping, despite positive reviews?'
Relies on clear dashboards, reporting, and other monitoring techniques to ***relay insights*** in a clear, easily consumable way.	To obtain insights, data analytics gets ***'under the hood'*** with data, carrying out tasks like data mining, algorithm development, modeling, & simulations.
Can be implemented using various ***BI tools*** available in the market.	Can be implemented using various ***data storage tools*** available in the market.
Is implemented ***only on historical data*** stored in data warehouses or data marts.	***Can also be implemented using BI tools***, but it depends on the approach or strategy designed by an organization.

Can be debugged only through ***historical data*** provided and the end user requirements.	Can be debugged via the ***proposed model*** to convert the data into a meaningful format.

Illustration : SkullCandy – a leading supplier

For SkullCandy, a leading supplier of headphones, earbuds, and other audio devices, tracking all of this meant their data covered more than 100-million rows in multiple source locations – a logistical nightmare, as one can imagine. To get all this information in one unified place, they turned to a BI solution.

With the system they had in place before, they often found they were missing certain bits of data, and the results regularly were not accurate – not a good thing for a retail company trying to stay on top of things.

BI is a benefit Behind-the-Scenes.

- SkullCandy implemented Sisense across the board – from their IT department to their HR department and everything in between. It became the go-to data software for the entire company.
- Each department can now easily add new data, access automated reports, and send results from one sector to another without having to wade through hundreds of different documents.
- Data is refreshed immediately, meaning there are less inaccuracies, and the whole team can get their hands on fast data as and when they need it.

BI as a benefit to Retailers in General.

- As the retail industry is huge, keeping up with the crowds and constantly implementing systems and strategies to increase sales and stay ahead of the game is no easy task. But with a BI solution, a user can start collecting and tracking the data that matters.
- Gathering data from all departments – not just sales – is a logistical nightmare, especially if that data is being delivered in multiple different formats from multiple different sources.
- With a simple BI solution, we can put all that data in one place and easily track trends, sales, and important information on the fly.

Key Advantages of BI for Retail

- **Improved customer experience:** Customer expectations are higher than ever now that there's more competition in the retail world, and brands to ensure that customers are retained and kept happy at every stage of the shopping process.
- **Predictive modeling:** With a retail predictive analytics tool, companies can combine current data with other relevant stats to seek out new sales opportunities, identify upcoming trends, and create models for the items customers are most likely to buy.
- **Optimize price:** Having access to relevant big data means brands can update their prices in real-time to coincide with current supply, demand, and upcoming trends.

SUMMARY

Businesses are moving at neck-breaking speeds and so is their competition. For these businesses to have an edge in the market, every decision they make must be informed. Irrespective of the industry, every business has access to a lot of data that they can leverage to their advantage. But unfortunately, very few do. This chapter deals with the concepts related to Business intelligence (BI) that uncovers insights for making strategic decisions. BI helps these businesses to use their data to their advantage by presenting the otherwise unusable pile of data into an understandable and interpretable form. Business Intelligence (BI) empowers us to synergize the power of technology with business expertise, facilitating fully informed decisions and ensuring a competitive advantage. BI tools analyze both historical and current data, presenting their findings in intuitive visual formats. These tools play a crucial role in organizing unstructured data, visually representing it through graphs, charts, maps, and more, thereby enhancing productivity and ensuring effective decision-making.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Which of the following chart shows the whole data into the propositions and is used to display various propositions that make up the final value?

   (a) Pie chart

   (b) Doughnut chart

   (c) Bar Chart

   (d) Line Chart

2. _____ refers to the information required to enhance business decision-making activities.

   (a) Data Analysis

   (b) Charts

   (c) Business Intelligence

   (d) Machine Learning

3. Which of the following is not the usage of Business Intelligence tools?

   (a) Reduce business costs

   (b) Generation of automatic reports

   (c) Compatibility

   (d) Distributed data

4. Following are the various phases involved in Business Intelligence Life Cycle.

   (a) Create BI Project Structure

   (b) Analyze Business Requirements

   (c) Design Data Model

   (d) Design the Physical Schema

   (e) Build the Data warehouse

   Pick the correct sequence.

(a) (i), (ii), (iii), (iv), (v)

(b) (iv), (iii), (ii), (i), (v)

(c) (ii), (iii), (iv), (v), (i)

(d) (v), (iii), (ii), (i), (iv)

5. In which phase of Business Intelligence Life Cycle, metadata is created?

(a) Design Data Model

(b) Building of data warehouse

(c) Creation of BI Project structure

(d) Development of BI Objects

ANSWERS/SOLUTIONS

1.	(b)	2.	(c)	3.	(d)	4.	(c)	5.	(c)

UNIT – V

DIGITAL ECONOMY

CHAPTER 12

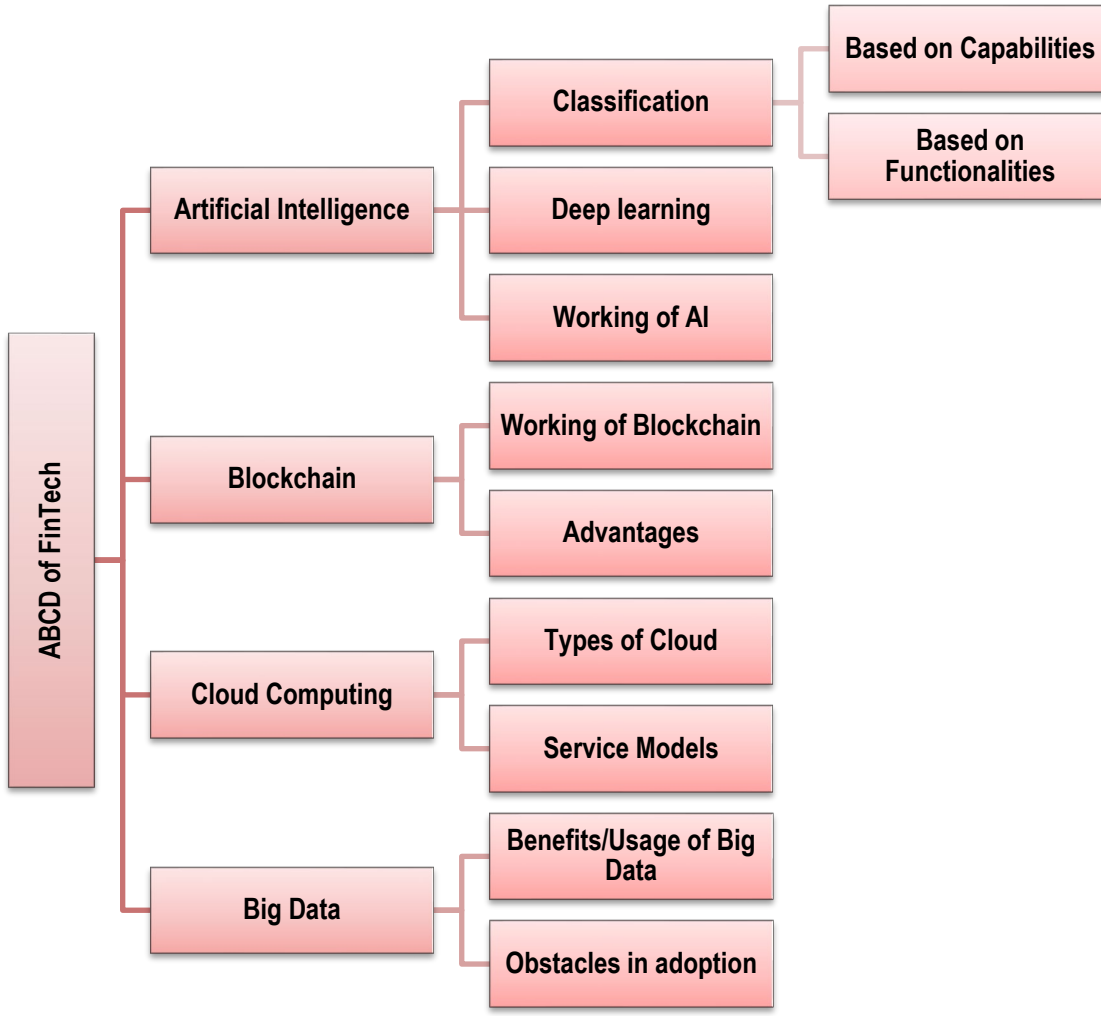
ABCD OF FINTECH

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- comprehend the ABCD technologies used in FinTech.
- acknowledge the usage of Artificial Intelligence in real time situations.
- grasp the understanding of Blockchain in Financial institutions.
- understand the concepts of Cloud Computing in detail.
- acquire the role of Big Data in Financial Institutions.

CHAPTER OVERVIEW



12.1 INTRODUCTION

FinTech, the abbreviation for Financial Technology, is a broad category that refers to the innovative use of technology in the design and delivery of financial services and products. The application of FinTech cuts across multiple business segments, including lending, borrowing advice,derivates, assets managements, insurance, investment management and payments. Many FinTech companies harness mobile technologies, big data and superior analytics to tailor products for various customer segments.

FinTech companies offer a wide range of products and services. These can broadly be split into two categories, depending on who their 'customer' is **Business-to-Consumer (B2C)** and **Business-to-Business (B2B)**. Some may define FinTech as technology that increases efficiency and creates new financial business models that utilize some or all - **Artificial Intelligence (AI), Blockchain, Cloud Computing and Big Data.**

Some of the major FinTech products and services currently used in the marketplace are Peer to Peer (P2P) lending platforms, Crowd funding, Distributed Ledgers Technology (DLT), Robo advisors, etc. These FinTech products are currently used in international finance, which bring together the lenders and borrowers, seekers, and providers of information, with or without a nodal intermediation agency.

- **Peer-to-Peer (P2P) lending:** Peer-to-peer (P2P) lenders connect lenders and borrowers, using advanced technologies to speed up loan acceptance. These technologies are designed to increase efficiency and reduce the time involved in access to credit. While P2P lending originally involved direct matching of individual lenders and borrowers on a one-to-one basis, it has evolved into a form of marketplace lending where institutional and high net worth individual investors lend into a pool that borrowers can access.
- **Crowd funding:** Crowd funding is a way of raising debt or equity from multiple investors via an internet-based platform. Securities and Exchange Board of India (SEBI) has released a paper and defined crowd funding as "solicitation of funds (small amount) from multiple investors through a web-based platform or social networking site for a specific project, business venture or social cause." The platform providers offer a range of information about the potential borrowers/issuers, ranging from credit ratings (for most peer-to-peer loan arrangements) to business model to verification of information and AML (Anti Money Laundering) checks of firms that want to raise equity capital.
- **Distributed Ledgers Technology (DLT):** Distributed ledger technologies, like blockchain, are peer-to-peer networks that enable multiple members to maintain their own identical copy of a shared ledger. Rather than requiring a central authority to update and communicate records to all participants, DLTs allow their members to securely verify, execute, and record their own transactions without relying on a middleman.
- **Robo Advisor:** A robo-advisor is a digital platform that provides automated, algorithm-driven financial planning and investment services with little to no human supervision. A typical robo-advisor asks questions about user's financial situation and future goals through an online survey and then uses the data to offer advice and automatically invest for the user.

I. **What objectives does FinTech have? :** The primary objective of FinTech is to assist various businesses and consumers in the efficient administration of financial transactions. Since FinTech makes it possible for people to obtain desired financial services from their smartphones, financial transactions are no longer limited to laptops and desktops.

II. **Why Consumers choose FinTech institutions instead of trusted banks FinTech?**

- FinTech companies are versatile and include lower fees and better rates, lower thresholds for investments, lower thresholds for loans, ease of use and convenience. This is manifested in lower margins, asset-light nature, and high scalability.
- Second is their intense use of technology including onboarding, social networks, crowd knowledge/wisdom, big data with the requisite analytics for market analysis and credit scoring.
- The use of AI with the requisite cybersecurity as in the use of a private key and touch recognition are equally important to ensure customer trust.

III. **How Does FinTech Work?:** While FinTech is a multifaceted concept, it simplifies financial transactions for consumers or businesses, making them more accessible and generally more affordable. It can also apply to companies and services utilizing AI, Big Data, and encrypted blockchain technology to facilitate highly secure transactions amongst an internal network. Broadly speaking, FinTech strives to streamline the transaction process, eliminating potentially unnecessary steps for all involved parties. For example, a mobile service like Unified Payment Interface (UPI) allows users to pay other people at any time of day, sending funds directly to their desired bank account.

IV. **The Technologies that Power FinTech:** Modern FinTech is primarily driven by Artificial Intelligence (AI), big data, and blockchain technology — all of which have completely redefined how companies transfer, store, and protect digital currency. Specifically, AI can provide valuable insights on consumer behavior and spending habits for businesses, allowing them to better understand their customers. Big data analytics can help companies predict changes in the market and create new, data-driven business strategies. Blockchain, a newer technology within finance, allows for decentralized transactions without inputs from a third party; tapping a network of blockchain participants to oversee potential changes or additions to encrypted data.

V. **FinTech Trends:** Over the years, FinTech has grown and changed in response to developments within the wider technology sector with several prevailing trends:

- **Digital banking continues to grow:** Digital banking is easier to access than ever before. Many consumers already manage their money, request, and pay loans, and

purchase insurance through digital-first banks. This simplicity and convenience will likely drive additional growth in this sector.

- **Blockchain:** Blockchain technology allows for decentralized transactions without a government entity or other third-party organization being involved. Blockchain technology and applications have been growing quickly for years, and this trend is likely to continue as more industries turn to advanced data encryption.
- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML technologies have changed how FinTech companies scale, redefining the services they offer to clients. AI and ML can reduce operational costs, increase the value provided to clients, and detect fraud. As these technologies become more affordable and accessible, expect them to play an increasingly large role in FinTech's continued evolution — especially as more brick-and-mortar banks go digital.

VI. Benefits of FinTech: The proponents of FinTech highlight a range of ways that it may be able to benefit society and individual consumers:

- **Economic opportunities:** The FinTech industrygenerates employment opportunies and attracts investments. While the Government estimates that around 76,500 people currently work in FinTech, the Department of International Trade predicts that this will grow to 105,500 by 2030.
- **Improved speed and efficiency:** Digitizing and automating finance enable the swift completion of services that previously took days to process, now accomplished within seconds. Slow and costly settlement processes, such as those for reconciling payments, can be sped up by distributed ledger technology. This is because the technology allows each participant in the settlement to have access to the "same, distributed but synchronized data", thus providing "a single source of truth" for all parties to work from.
- **More resilient systems:** Distributed ledgers may be able to help make systems that are harder to break. This is because copies of the data are recorded by multiple participants at the same time, minimizing the impact of data loss should there be an issue with one participant.
- **More competition and choice:** It has been anticipated that the older and larger banks, which still account for most of the retail banking market, do not have to work hard enough to win and retain customers and it is difficult for new and smaller providers to attract customers. The new technologies and Government measures may allow

smaller firms to enter the market, using their 'agile' nature to innovate quickly and so give consumers more choice.

- **Better insights equal better products:** Big data and advanced data analytics can allow firms to provide products or services that are more tailored to individual consumers. An additional benefit of modern data-driven approaches is that they are more objective and therefore less prone to bias than a human would be (although algorithmic discrimination is still a risk).
- **Improved financial inclusion:** While there is a risk that new technologies may open up new forms of exclusion, FinTech is considered to have the power to include more people in the financial system. This may be particularly true in developing economies, where mobile financial services products, such as M-Pesa in India, have helped boost the rate of access to formal financial services.
- **Solutions to specific problems:** FinTech is already being used to tackle particular challenges that consumers or businesses face like addresses for homeless individual, efficiency in debt advice, gambling addiction, paying rent deposits and verifying identity digitally etc.

VII. Challenges for consumers

- **Some may be left behind:** Some consumers may be digitally or financially excluded and therefore at risk of being unable to participate fully in society as the use of FinTech becomes the norm as it has been observed that people may struggle to cope in a cashless society. Therefore, it would be required to improve digital skills, connectivity, and financial inclusion of the society at large.
- **Others may be excluded by automated decision-making:** Some consumers could find themselves increasingly marginalized by automated decision-making systems. There are substantial concerns about how 'algorithmic discrimination' could lead to biases in decision-making against certain groups.
- **Lack of regulatory protection:** When using FinTech products or services, consumers may not enjoy the same regulatory protections from all financial service providers. For example – the right to resolve complaints through X Financial Service Provider may not be the same as provided through Y Financial service provider.
- **Limited consumer understanding:** As financial products become more technologically complex, consumers may find it harder to fully understand what they are signing up to.

- **Risk of scams:** New technologies and new financial products, along with possible regulatory, could lead to more consumers falling victim to scams and fraud.
- **Other financial crimes:** New technologies also open up new possibilities for crime. For instance - some of the main characteristics of cryptocurrencies that can assist fraudsters are market volatility, complex concepts, decentralized control, anonymity, and ease of cross-border payments.
- **Loss of consumer control over data:** Without adequate protections, consumers may also find it difficult to understand which organizations have access to their data and what this consists of. For example, In the U.K. in the year 2020, the Information Commissioner's Office (ICO) published its findings on the use of data by major credit reference agencies (Equifax, and Experian, not Cibil as Cibil is an Indian credit information company). It reported that "significant 'invisible' processing took place, likely affecting millions of adults. It is 'invisible' because the individual is not aware that the organization is collecting and using their personal data. This is against data protection law.
- **Manipulating consumer behavior:** Technology could be used to exert unnecessary or excessive control over consumers' behaviors and so coerce people into complying with financial services' preferences. People might, for example, edit or filter what they put on social media if they know that a financial business will analyze it. But the impact can go far beyond this.
- **Issues when technology fails:** Consumers can have problems when the technology behind FinTech malfunctions. More than 5 million payments, including 2.4 million in the UK, failed in 2018 when the VISA network experienced issues at its data centre. Passengers have also faced extra charges on the Transport for London network when their phone battery has died before they tap out at the end of their journey.

VIII. FinTech Top Use Cases: The impact of FinTech has been evident in the way it has caused improvement in conventional banking and financial services. The multiple FinTech use cases have emerged as prominent trends in the traditional, brick-and-mortar institutions for financial services. As of now, millions of users rely on FinTech in some form or the other, generally through smartphones and mobile devices.

Most important of all, FinTech has developed as a productive solution to the problems of access to banking and financial services, thereby have opened the doors to financial services for unbanked people in the world. The FinTech examples would help you understand how it can improve the accessibility of financial services without relying on traditional banks and

other financial institutions. Here are some of the notable uses of FinTech, along with the relevant examples for each use case.

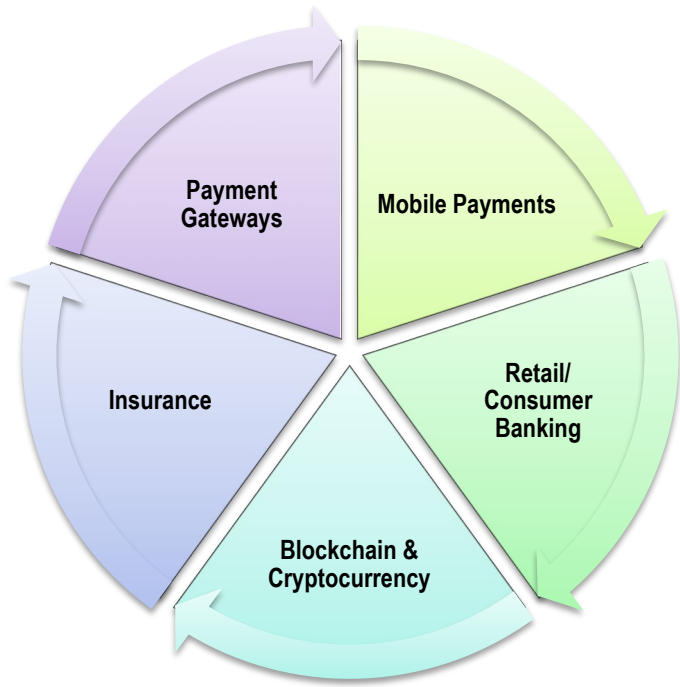


Fig. 12.1: FinTech Top Use Cases

(A) **Mobile Payments:** FinTech companies are always developing innovative approaches to granting access to their services, regardless of location. Digital authentication, Near Field Communication technology (NFC), and mobile wallet technologies are a few of the noteworthy FinTech advancements that have fueled the expansion of mobile payments. The combination of financial services with mobile computers has also been remarkable. Mobile payments might contribute to laying the groundwork for a world without cash. Apple Pay, Google Pay, and Samsung Pay are examples of mobile payment apps that allow users to store their credit and debit card information on their smartphones and make payments by tapping their phones on payment terminals. Additionally, these apps provide additional security features, such as biometric authentication and tokenization, making mobile payments more secure than traditional card payments.

(B) **Retail/Consumer Banking:** Consumer banking platforms or FinTech solutions contribute to increased financial service affordability and accessibility. Traditional banks have always operated with methods that isolate specific sections of society from

banking and financial services. For example, the transaction fees in banks and identity verification requirements could create troubles for any individual in accessing banking services. With the help of FinTech, users could find alternative consumer banking products and solutions geared toward resolving accessibility difficulties and affordability of financial services.

(C) **Blockchain & Cryptocurrency:** Blockchain technology makes use of cryptography technology to create cryptocurrencies which act as a reliable and effective replacement for cash. Blockchain technology and cryptocurrencies have been widely employed by businesses to gain major advantages such as increased traceability, security, and transparency, as well as quicker transactions and reduced prices. Additionally, blockchain-based smart contracts may set new standards for how people can access financial services. Blockchain and cryptocurrency examples in FinTech would refer to a variety of platforms and programs, including Bitcoin, Ethereum and many others.

(D) **Insurance:** The flow of other financial services like banking has also been changed by FinTech. The use of FinTech in insurance has also produced new benefits, while the list of many FinTech instances in banking has opened new pathways for efficiency. InsurTech combines "Insurance" and "Technology", wherein the businesses concentrate on creating, distributing, and aggregating digital insurance products.

Numerous **InsurTech** platforms have created cutting-edge insurance applications that could make it simpler to get insurance. The businesses and service providers in the insurance sector work together with traditional insurers to automate insurance processes and manage coverage. The elimination of labor-intensive and complicated processes would be one of FinTech's most notable benefits in the transformation of insurance. As a result, it can make insurance services more accessible while also making it easier to handle coverage and claims. For example - PolicyBazaar is India's largest online insurance aggregator and a prominent player in the Insurtech space. They offer a wide range of insurance products, including health, life, motor, and travel insurance.

(E) **Payment Gateways:** Payment gateways are the next common example of FinTech use cases. Before the advent of e-commerce, electronic payment systems were operational. The advent of online payment gateways contributed to the transformation of payment on e-commerce platforms by enhancing the practicality, usability, and accessibility of financial services. Payment gateways solved the issue of sending money without the involvement of banks, thereby benefiting consumers by reducing

costly bank transaction costs. The most well-known FinTech instances among payment gateways in India are PayU India which is one of the biggest payment gateway aggregators in India.

IX. **Compliance with Government Regulations for the financial industry:** Compliance with government regulations is an essential aspect of the financial sector. Regulations are put in place to protect consumers, prevent financial crimes, and ensure the stability of the financial system. In recent years, data protection has become an increasingly important aspect of regulatory compliance, with the rise of data breaches and concerns over privacy. The Application of Data Protection by Design and by Default principles is one way that FinTech can meet these regulatory requirements.

- **Application of Data Protection by Design and by Default Principles**

  Financial institutions must comply with a range of regulations, including Anti-Money Laundering (AML) and Know-Your-Customer (KYC) requirements, as well as regulations related to consumer protection, privacy, and data security. These regulations are designed to protect consumers and prevent financial crimes such as fraud, money laundering, and terrorist financing. **Data Protection by Design and by Default (DPbDD)** is a set of principles that encourage the integration of data protection measures into the design and development of systems, products, and services. This approach aims to ensure that privacy and data protection are built into the core of a product or service rather than added as an afterthought. Therefore, DPbDD principles can help to ensure that FinTech are in compliance with regulations. Because of the sensitive financial data processing, we can expect sharpening the regulatory challenges and severe consequences of not following them. Therefore, incorporating DPbDD principles will be an indispensable part of building compliant solutions.

- **Regulators In India**

  RBI has been instrumental in enabling the development of FinTech sector and espousing a cautious approach in addressing concerns around consumer protection and law enforcement. The key objective of the regulator has been around creating an environment for unhindered innovations by FinTech, expanding the reach of banking services for unbanked population, regulating an efficient electronic payment and providing alternative options to the consumers. FinTech enablement in India has been seen primarily across payments, lending, security/biometrics and wealth management. These have been the prime focus areas for RBI, and we have seen significant approaches published for encouraging FinTech participations.

For example - Introduction of "Unified Payment Interface" with National Payments Corporation of India (NPCI), which holds the potential to revolutionize digital payments and take India closer to objective of "LessCash" society.

- **Cyber security and FinTech:** Since the early 1990s (accelerated in 2000s) with entry of New Pvt. Sector banks, the PSU banks have also embraced technology by leaps and bounds in the last decade or so. But the key shift has been brought in by consumer demand for real-time and always ON (anytime/anywhere) banking aided by growing demand coming from explosive growth in use of personal computing devices and internet connectivity, innovative products (plastic cards, now contactless cards, future - internet of things) by consumers. The banks have also been trying to make their processes more efficient and continuously looking for ways to leverage enhanced level of engagement with customers with a view to offering innovative products and services keeping in view cost, convenience, and profitability factors. Being a largely service based industry, there is a high degree of dependency on technology for delivering services (be it from sourcing to servicing) by banks and competitive pressures to continually innovate to retain customers in the wake of entry of niche players/new players/entrants (banks, small finance banks, payment banks).

  The advancements in technology and shift in consumer preferences driven by (SMAC – Social media, Mobility (Mobile Computing), Analytics (Big data), Cloud computing, etc.) have further brought on opportunities and challenges in terms of their utility/efficiency, complexity of products, deployment architecture, accompanied by persistent concerns over consumer protection in this era of instant communication and real time transactions, sometimes through opaque channels. Along with the benefits that the technology advancements have brought in, with increased reach of connectivity (internet) and geopolitical/macro-economic factors, cyber-attacks are on the rise and may well continue in the future with connected devices set to exceed the human population at some point in the future. Cyber Security is an issue that has been growing in importance with the advancements in technology. From a securities market point of view, some developed jurisdictions have observed cases of hacking of trading accounts for market manipulation.

- **Customer Data Protection (CDP):** The FinTech entities are heavily dependent on technology for each and every product they offer to their consumers. These entities may collect various personal and sensitive information about the customer and become the owners/custodians of such data. Therefore, the onus of CDP lies with these entities ranging from data Preservation, Confidentiality, Integrity, and Availability of the same, irrespective of whether the data is stored/in transit within themselves or

with customers or with the third-party vendors. The confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by FinTech.

Section 43A of the Information Technology Act, 2000, provides for payment of compensation by a body corporate in case of negligence in implementing reasonable security practices and procedures in handling sensitive personal data or information resulting in wrongful loss to any person.

In terms of **Section 72A** of IT Act; disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine. Hence, that data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms personal data, personal sensitive data, its dissemination, etc. As such, it may be necessary to emphasize the need for an exhaustive stand-alone legislation on data protection in India keeping in mind the innovations in FinTech and risk to personal data which comes to the possession of these entrepreneurs.

- **Classification of Customer Organization Data (CCOD):** The FinTech entities should classify data/information based on information classification / sensitivity criteria of the organization. It becomes important to appropriately manage and provide protection within and outside organization borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed, and put to use within/outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

- **Adherence to Safe Transaction Principles (STP):** A transaction in the IT parlance is termed as successful, if the transaction does not suffer from loss of Confidentiality, loss of Integrity, and loss of Availability. These three together are referred to as the Security Triad/the CIA Triad. The three consequences of lack of CIA leads to **"Data Leakage to Unauthorized Parties", "Data Tampering/Destruction by an Unauthorized Party", "Non-Availability of the Data/System at times it is really needed".** The FinTech entities need to satisfy these principles in order to build faith in the new ecosystem.

- **Configuration/Patch Management Systems:** The FinTech entities should install systems and processes to identify, track, manage and monitor the status of patches

to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.

- **Audit Log Management System (ALMS):** The FinTech entities should implement ALMS to periodically validate settings for capturing of appropriate logs /audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.
- **Incident Response & Management Framework (IRMF):** The FinTech entities need to have clear procedures for responding to cyber incidents and a mechanism for dynamically recovering from cyber threats. Technical progress fosters innovation, but it also entails new risks. At the same time, the primary mandate of the regulator is to protect the users of financial services and the stability of the financial system. The two issues the regulator needs to focus on are firstly the threat of cyber-attacks and secondly the risks related to the outsourcing of certain traditional bank activities.

X. Evolution of Digital Currency as Alternative Currency: Various innovative money payment systems in the market have arrived with smart phones, Internet, and digital storage cards. The emergence of this class of digital payment systems has revolutionized the way values are being transferred. The latest and most interesting form of value transfer was created by Satoshi Nakamoto (2008). Satoshi's Bitcoin is now a well-known system of cross border value transfer for untrusted parties without a centralized authority.

Bitcoin, commonly abbreviated as "BTC" is a medium of exchange, a store of value and a unit of account. **Conventionally, the uppercase "Bitcoin" refers to the network and technology, while the lowercase "bitcoin(s)" refers to units of the currency.**

Some technical terms

Few technical terms that will be used in the chapter often are explained below:

- **Open Source:** The term "open source" means that something people can modify and share because its design is publicly accessible. This will allow trusted core developers to verify and suggest changes for the code to be adopted by the network.
- **Centralized Network:** This is a network where all users are connected to a single or central server that acts as an agent for all communications. The centralized server stores both the communications and user account information. It is important to note that while the computing power can be distributed Digital Currency network like in

case of Cryptocurrency, a single entity does not control the entire network. Unlike centralized systems like Google and Facebook, these decentralized networks operate without a single controlling authority.

- **Decentralized Networks:** A server based decentralized network has no single entity that controls the network. The computing power is distributed. There must be a consensus algorithm and it has to handle crashes and faults. Any permitted entity can be read and write data while clients can maintain anonymity, **validators (or nodes confirming transactions)** often operate without anonymity. Examples of decentralized networks include Corda and Multichain.
- **Fully Server-free or Public Decentralized Network:** In this type of network, no single entity controls the system, and computing is distributed. The consensus algorithm must be robust enough to handle crashes, Byzantine Faults, and sybil Attacks. Both clients and validators maintain anonymity. Participants can freely read and write data. Notable examples of such networks include Bitcoin and Ethereum.
- **Distributed Network:** This refers to a system where computer programming and data are distributed across multiple computers without reliance on a centralized server or control.
- **Peer-to-Peer (P2P):** In its simplest form, two or more personal computers are connected and share resources without going through a server computer. A P2P network is created when two or more computers are connected in that way.

Bitcoin features

- Bitcoin is a decentralized peer-to-peer (P2P) digital currency network designed for the verification and processing of transactions.
- Unlike traditional systems relying on trusted third parties, Bitcoin employs cryptographic proof in its computer software.
- This cryptographic proof-of-work mechanism verifies the legitimacy of bitcoin transactions and records them in a decentralized ledger.
- Crucially, Bitcoin is not a fiat currency issued by a central government or its authorized agents
- It lacks backing as legal tender by any physical commodity. Nevertheless, similar to fiat currencies, the value of bitcoin is determined by the principles of supply and demand rather than the intrinsic value of its material. Bitcoin exists as a virtual currency, residing in a computer database or ledger.

- The Bitcoin software protocol is open source, allowing developers to contribute and enhance its functionalities. This collaborative effort has led to a flourishing Bitcoin community.
- The power to modify the Bitcoin protocol lies with miners and developers. However, neither miners nor developers can unilaterally enforce changes to the protocol without a fork, which involves breaking compatibility with the rest of the network.

12.2 ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence. While AI is an inter-disciplinary science with multiple approaches, advancements in machine learning and deep learning in particular are creating a paradigm shift in virtually every sector of the tech industry. AI is redefining the way business processes are carried out in various fields, such as marketing, healthcare, financial services, and more. Companies are continuously exploring the ways they can reap benefits from this technology. As the quest for improvement of current processes continues to grow, it makes sense for professionals to gain expertise in AI. When you enter a dark room, the sensors in the room detect your presence and turn on the lights. This is an example of non-memory machines. Some AI programs are able to identify your voice and perform an action accordingly. If you say, "turn on the TV", the sound sensors on the TV detect your voice and turn it on.

Benefits of AI and ML in Business Organization: For Finance function

- The development of Robotic Process Automation (RPA) in many companies are run unattended to automate large volumes of specific accounting processes that are structured and repetitive, such as data entry and reconciliation activities. When deployed at scale, RPA has the potential to act like a virtual workforce and position the accounting profession to provide higher value functions and activities.
- Beyond automation, AI technologies can further be used to analyze large quantities of data at speed and at scale. It has the ability to detect anomalies in the system and optimize workflow. Finance professionals can use AI to assist with business decision-making, based on actionable insights derived from customer demographics, past transactional data, and external factors, all in real-time.
- By implementing automated anti-fraud and finance management systems, practices can also significantly improve compliance procedures and protect both their own and clients' finances. In this way, AI technology and accountants can work together to provide a more predictive, strategic function.

- AI will provide businesses with the ability to capture business activity in real time, perform continuous reconciliation and make adjustments such as accruals throughout the month. This will also help reduce the burden at the end of the period.
- AI can also facilitate effective continuous audit, significantly reducing risks of financial fraud and minimize accounting errors, often caused by human interaction.

Benefits of AI and ML in Business Organization: Beyond the Finance function

- **Customer and stakeholder satisfaction:** As businesses use robots and automated data analysis through social networks, websites, email exchanges and other data sources, it is in the integration of the data from various sources that will create the actionable insights for the business.
- **Security:** AI deployment in finance can also allow businesses to find breaches in security systems to be detected as well as to explore solutions. It will be able to analyze documentation for account registration and detect issues within accounts for instance.
- **Risk management:** It is difficult to overestimate the potential impact and benefits of AI when it comes to risk management. Enormous processing power allows vast amounts of data to be handled in a short time, and cognitive computing can help to manage both structured and unstructured data, a task that would take far too much time for humans to do effectively.
- **Fraud prevention:** AI has been very successful in battling financial fraud and is getting enhanced as AI is becoming more widely adopted. Fraud detection systems can analyze clients' behavior, location, and buying habits and trigger a security mechanism when something seems out of the ordinary and contradicts established spending patterns for instance.
- **Process automation:** Forward-thinking industry leaders are looking to RPA when they want to cut operational costs and boost productivity. AI-enabled software can also be used to verify data and generate reports automatically according to the given parameters, as well as review documents, and extract meaningful insights from the data being processed.

TYPES OF ARTIFICIAL INTELLIGENCE

Artificial Intelligence can be divided into various types as shown in Fig. 12.1. There are mainly two types of main categories which are based on **'Capabilities'** and based on **'Functionalities'** of AI and discussed in detail in Table(s) 12.1 and 12.2 respectively.

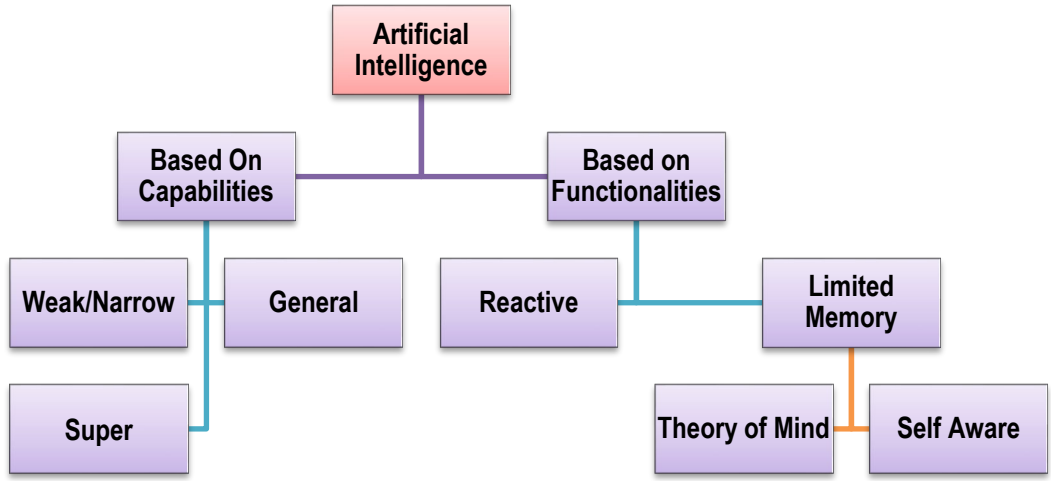


Fig. 12.1: Classification of AI

Table 12.1: AI Classification - Based on Capabilities

Weak/Narrow AI	General AI	Super AI
Narrow AI is a type of AI which can perform a dedicated task with intelligence. The most common and currently available AI is Narrow AI in the world of Artificial Intelligence. Narrow AI cannot perform beyond its field or limitations, as it is only trained for one specific task. Hence it is also termed as weak AI. Narrow AI can fail in unpredictable ways if it goes beyond its limits.	General AI is a type of intelligence which could perform any intellectual task with efficiency like a human. The idea behind the general AI is to make such a system which could be smarter and think like a human on its own. Currently, there is no such system which could come under general AI and can perform any task as perfect as a human. The worldwide researchers are now focused on developing machines with General AI.	Super AI is a level of Intelligence of Systems at which machines can surpass human intelligence and can perform any task better than humans with cognitive properties. It is an outcome of general AI. Some key characteristics of strong AI include capability include the ability to think, to reason, solve the puzzle, make judgments, plan, learn, and communicate on its own.
Apple Siri is a good example of Narrow AI, but it operates with a limited pre-defined range of functions. Some other examples are playing chess, purchasing suggestions on e-commerce site, self-driving cars, speech, and image recognition.	Systems with general AI are still under research and it will take lots of effort and time to develop such systems.	Super AI is still a hypothetical concept of Artificial Intelligence. Development of such systems in real is still world changing task.

Table 12.2: AI Classification - Based on Functionalities

Reactive AI	Limited Memory AI	Theory-of-mind AI	Self-aware AI
Reactive AI uses algorithms to optimize outputs based on a set of inputs. This kind of AI is purely reactive and does not have the ability to form 'memories or use 'past experiences' to make decisions. These machines are designed to perform specific tasks.	Limited memory AI can adapt to past experience or update itself based on new observations or data. Often, the amount of updating is limited, and the length of memory is relatively short. This kind of AI uses past experiences and the present data to make a decision. Limited memory means that the machines are not coming up with new ideas. They have a built-in program running the memory. Reprogramming is done to make changes in such machines.	Theory-of-mind AI is fully adaptive and has an extensive ability to learn and retain past experiences. These AI machines can socialize and understand human emotions and will have the ability to cognitively understand somebody based on the environment, their facial features, etc.	Self-aware AI, as the name suggests, become sentient and aware of their own existence. This is the future of AI. These machines will be super-intelligent, sentient and conscious.
For example - Chess-playing AIs, for example, are reactive systems that optimize the best strategy to win the game. Reactive AI tends to be fairly static, unable to learn or adapt to novel situations. Thus, it will produce the same output given identical inputs.	Self-driving cars are examples of limited memory AI. Autonomous vehicles, for example, can "read the road" and adapt to novel situations, even "learning" from past experience.	Machines with such abilities have not been developed yet. *There* is a lot of research happening with this type of AI.	They are able to react very much like a human being, although they *are* likely to have their own features. Still in the realm of science fiction, some experts believe that an AI will never become conscious or "alive".

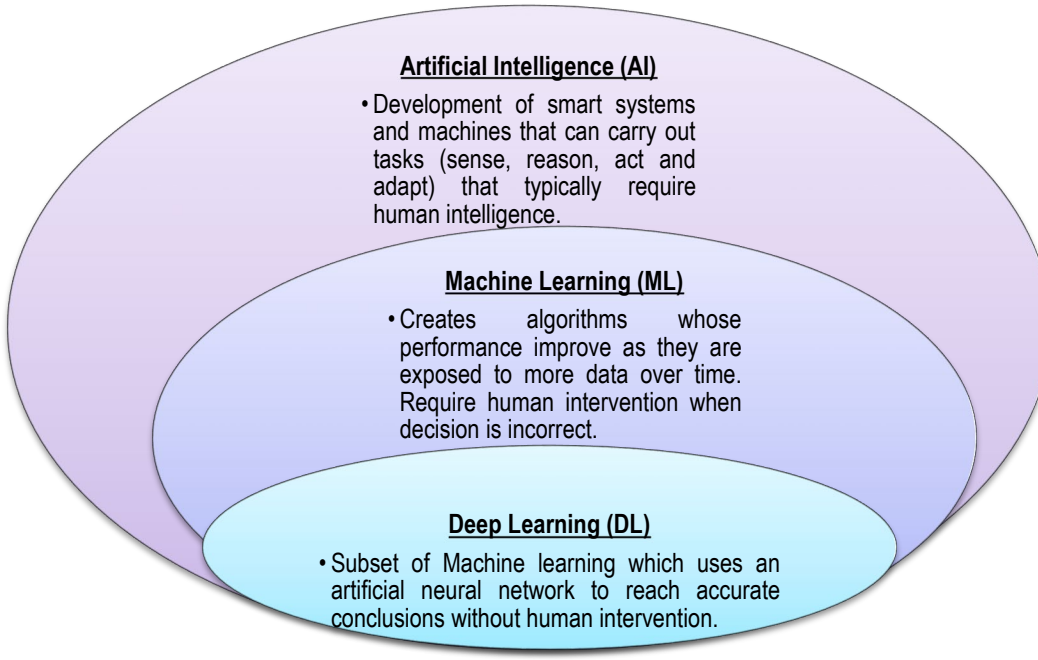


Fig. 12.2: Distinction between AI, ML and DL

Refer Fig. 12.2 to know broadly the distinction between AI, ML and DL.

Machine Learning (ML) is the science and art of programming computers so that they can learn from data. It is a subset and application of AI that provides the system with the ability to automatically learn without being explicitly programmed. For example, spam filter is a type of machine learning that learns to recognize spam e-mails by figuring out the words and patterns commoly found in spam.

Deep Learning (DL) is a relatively new set of methods that is changing machine learning in fundamental ways. DL isn't an algorithm per se, but rather a family of algorithms that implements deep networks (many layers). These networks are so deep that new methods of computation, such as Graphics Processing Units (GPUs), are required to train them, in addition to clusters of compute nodes. DL works very well with large amounts data, and whenever a problem is too complex to understand and engineer features (due to unstructured data, for instance). DL almost always outperforms the other types of algorithms when it comes to image classification, natural language processing and speech recognition. For example - Virtual Assistants like Amazon Alexa, Siri, and Google Assistant need internet-connected devices to work with their full capabilities. Each time a command is fed to them, they tend to provide a better user experience based on past experiences using Deep Learning algorithms. Currently, the larger the neural network and the more data that can be added to it, the better the performance a neural network can provide.

DL is very powerful, but it has a couple of drawbacks. It's almost impossible to determine why the system came to a certain conclusion. This is called the "black box" problem, though there are now many available techniques that can increase insights in the inner workings of the DL model. Also, deep learning often requires extensive training times, a lot of data and specific hardware requirements, and it's not easy to acquire the specific skills needed to develop a new DL solution to a problem. In conclusion, there is no one algorithm that can fit or solve all problems. Success really depends on the problem user needs to solve and the data available to him/her.

Illustration on Artificial Intelligence – Nike & Starbucks

The world's biggest shoe brand **Nike** has launched an AI system that enables customers to design their own sneakers in their online store. Not only it is a secret to improve sales, but also collects useful data about customers that ML algorithms can use to design future sneakers and provide personalized recommendations.

Starbucks uses its mobile app and loyalty card to collect and analyze customers' information including, the place and time of product made and time, and sales. The firm uses Predictive Analytics to process this useful data to offer personalized messages to customers, including recommendations when they reach their local retail stores and with the goal of improving their average cost. The virtual barista service in the AI-based application allows people to place orders directly through voice command in their mobile device.

12.3 BLOCKCHAIN

A **Blockchain** is a data structure that makes it possible to create a digital ledger of data and share it among a network of independent parties. A blockchain is like a giant spreadsheet for registering all assets, and an accounting system for transacting them on global scale that can include all form of assets held by all parties worldwide. It is a shared, decentralized, and open ledger of transactions. This ledger database is an append-only database which cannot be altered but can be replicated across many nodes. It means that every entry is a permanent entry. Any new entry on it gets reflected on all copies of the databases hosted on different nodes and thus there is no need for trusted third parties to serve as intermediaries to verify, secure, and settle the transactions. It is another layer on top of the Internet and can coexist with other Internet technologies.

I. **Types of Blockchain (Refer Fig. 12.3)**: All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. The removal of central authority from database structure is one of the most important and powerful aspects of blockchains. In the blockchain ecosystem, any asset that is digitally transferable between two people is called a token ie.. tokens are assets that allow information and value to be transferred, stored, and verified in an efficient and secure manner. These crypto tokens can take many forms and can be programmed with unique characteristics based on which they have different classification. Basically blockchain is categorized in two types- **permissioned** and **permissionless** blockchain.

Permissioned blockchain restricts the number of nodes which may access the network and its potential access rights. The users in permissioned blockchain are aware of the identity of the other users of that blockchain. Permissioned blockchain is further divide into two categories- Private and consortium

In **Permissionless blockchain,** there is no central authority to give the permission for accessing the network. Therefore, due to large number of nodes and extent of transaction, this type of blockchains has slow transaction processing rates. The Public Blockchain falls under this category.

There is more type of Blockchain i.e. **Hybrid Blockchain** which has the features of both **Permissioned and Permissionless Blockchain.**

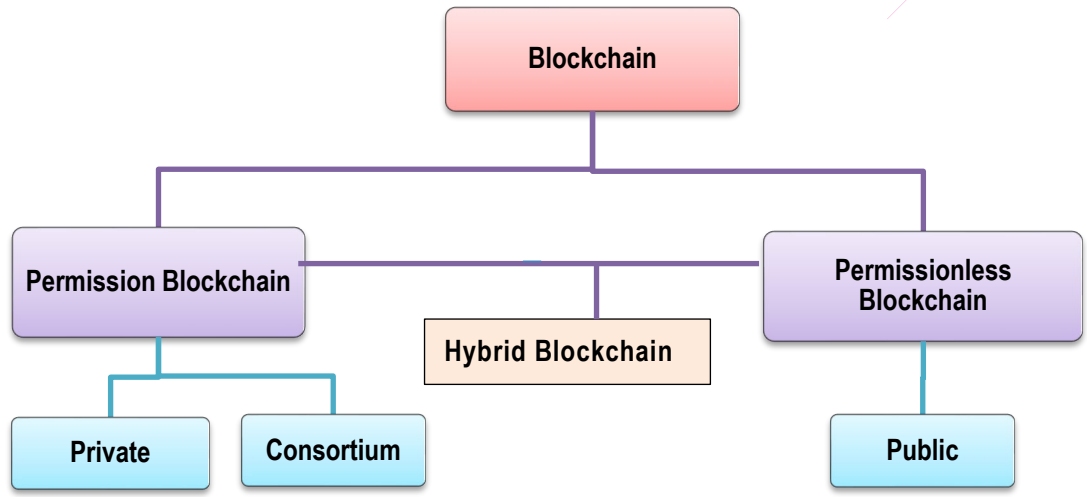


Fig.12.3 Types of Blockchain

Public Blockchains	Consortium Blockchain	Private Blockchains	Hybrid Blockchain
• Public blockchains, such as Bitcoin, are large, distributed networks that are run through a native token. • They are open for anyone to participate at any level and have open-source code that their community maintains.	• Consortium blockchains are a hybrid between public and private blockchains. They are controlled by a group of organizations, and participation is limited to the members of the consortium. • there is a validator node which inititate, receive and validate the transaction.	• Private blockchains tend to be smaller and do not utilize a token. Their membership is closely controlled. • These types of blockchains are favored by consortiums that have trusted members and trade confidential information.	• Hybrid blockchain enables the features of both private and public blockchain. It allows the organization to choose who can access the certain data of block chain and which data can be made public. It works in closed environment, hence prevent outside hacker to enter in network.

Fig. 12.4: Detail of various types of Blockchain

II. **The Structure of Blockchain (Refer Fig. 12.5):** Blockchains are composed of three core parts:

- **Block:** A list of transactions recorded into a ledger over a given period. The size, period, and triggering event for blocks is different for every blockchain. Not all blockchains are recording and securing a record of the movement of their cryptocurrency as their primary objective. But all blockchain do record the movement of their cryptocurrency or token. Think of the transaction as simply being the recording of data. Assigning a value to it (such as happens in a financial transaction) is used to interpret what that data means.
- **Chain:** A hash that links one block to another, mathematically "chaining" them together. This is one of the most difficult concepts in blockchain to comprehend. It's also the magic that glues blockchains together and allows them to create mathematical trust. The hash in blockchain is created from the data that was in the previous block. The hash is a fingerprint of this data and locks blocks in order and time. Although blockchains are a relatively new innovation, hashing is not. For practical purposes, think of a hash as a digital fingerprint of data that is used to lock it in place within the blockchain.
- **Network:** The network is composed of "full nodes." Think of them as the computer running an algorithm that is securing the network. Each node contains a complete record of all the transactions that were ever recorded in that blockchain. The nodes

are located all over the world and can be operated by anyone. It's difficult, expensive, and time-consuming to operate a full node. They're incentivized to operate a node because they want to earn cryptocurrency. The underlying blockchain algorithm rewards them for their service. The reward is usually a token or cryptocurrency, like Bitcoin.

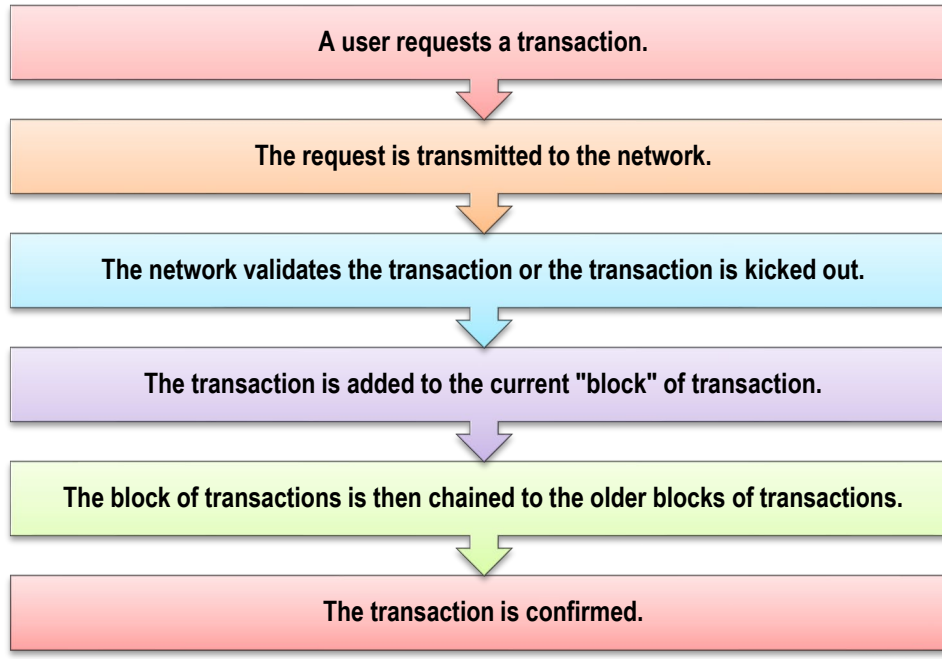


Fig. 12.5: Working of Blockchain

Blockchains create permanent records and histories of transactions, but nothing is permanent. The permanence of the record is based on the permanence of the network. In context of blockchain, this means that a large portion of a blockchain community would all have to agree to change the information and are motivated not to change the data. When data is recorded in a blockchain, it's extremely difficult to change or remove it. When someone wants to add a record to a blockchain, also called a transaction or an entry, users in the network who have validation control verify the proposed transaction. This is where things get tricky because every blockchain has a slightly different spin on how this should work and who can validate a transaction.

III. Why Blockchains matter?

Blockchain technology is a decentralized, distributed, and public ledger that is used to record transactions across many computers within a network. Because of its design and properties, blockchain is secure, transparent, and nearly impossible to alter.

When information has been written into a blockchain database, it's nearly impossible to remove or change it. This capability has never existed before and thus blockchains can create trust in digital data. When data is permanent and reliable in a digital format, user can transact business online in ways that, in the past, were only possible offline. Everything that has stayed analog, including property rights and identity, can now be created, and maintained online. Slow business and banking processes, such as fund settlements, can now be done nearly instantaneously. The implications for secure digital records are enormous for the global economy.

IV. Features of Blockchain

- **Decentralized:** Blockchain is based on a peer-to-peer network design—where each participant, or node, in the network is equal to all others. This means there is no controlling central authority that can unduly influence the system. The rules and behaviors of the network are embedded within the software protocol. The larger the network grows, the more standardized rules and behaviors are propagated, making it increasingly unlikely that any one actor, or multiple actors, could maliciously change the system's behavior.
- **Distributed:** Each node on the network contains a complete copy of the entire ledger, from the first block created—the genesis block—to the most recent one. This distributed approach increases the overall resiliency and security of the system. If any node or collection of nodes goes offline, the system will continue to function. In the Bitcoin example, its ledger holds every transaction ever done on every participating node for past years.
- **Distributed consensus:** This mechanism enables the entire network to reach agreement about which blocks of transactions are valid and which ones are not, enabling peer-to-peer value exchange without involving a trusted third party or intermediary for that consensus.
- **Tamper proof (immutability):** Each transaction must be digitally signed using a participant's private encryption key, which is kept only by the signer. The digital signature on a transaction can be validated by a signer's corresponding public key. Public keys, as the name implies, are designed to be shared with anyone. This ensures a transaction can only be created by the holder of a specific private key. Once a transaction signature is validated, a transaction is cryptographically bound, through a mathematical algorithm called "hash." The hash function creates a unique digital fingerprint for the transaction. Transactions are then hashed with other transactions

into a block. When a block of transactions has been accepted by the network, it is cryptographically bound to the ledger and distributed to all the nodes on the network.

- **Transparency:** The distributed ledger contains a full history of every transaction, enabling traceability of each asset—digital coin or other asset tracked by the ledger—back to its origin. With the distributed ledger published openly to every node on the network, it is easy for a network participant to unambiguously determine the current and past states of assets within the ledger. This creates a highly available, auditable trail of activities for each asset that has contributed to the current system state.
- **Distributed system:** Whether a system is centralized or decentralized, it can still be distributed. A centralized distributed system is one in which there is, say, a master node responsible for breaking down the tasks or data and distribute the load across nodes. On the other hand, a decentralized distributed system is one where there is no "master" node as such and yet the computation may be distributed. Blockchain is one such example.

V. Benefits of Blockchain

The benefits of blockchain-based transfers for merchants include the following (Refer Fig. 12.6):

Reduced fees: When customers pay with a credit card, merchants pay processing fees that cut into profit. Blockchain payments reduce or eliminate fees by streamlining the transfer process.

Preventing Insufficient Funds: Traditional payments, especially via cheques, can result in losses and additional fees for merchants due to insufficient funds. Blockchain-based payments offer merchants the assurance of a valid transaction within seconds or minutes, reducing the risk and inconvenience associated with insufficient funds

Improved Payment Security: The most secure payment methods traditionally include cash, wire transfers, and cashier's cheques. However, cash transactions lack traceability, wire transfers can be time-consuming, and cashier's cheques are susceptible to forgery. Blockchain-based payments address these concerns, providing a solution that removes these issues and instills greater confidence in transactions.

Fig. 12.6: Benefits of Blockchain

VI. **Applications of Blockchain:** Blockchain applications are built around the idea that the network is the arbitrator. Computers don't have the same social biases and behaviors as humans do and their code becomes law and rules are executed as they were written and interpreted by the network. Insurance contracts arbitrated on a blockchain have been heavily investigated as a use case built around this idea. Another interesting thing that blockchains enable is impeccable record keeping. They can be used to create a clear timeline of who did what and when. Many industries and regulatory bodies spend countless hours trying to assess this problem. Blockchain-enabled record keeping will relieve some of the burdens that are created when we try to interpret the past.

1. **Cryptocurrencies:**The first and most well-known application of blockchain, Bitcoin uses a blockchain to enable secure and decentralized digital currency transactions.
2. **Supply Chain Management:** Blockchain helps enhance transparency and traceability in supply chains by recording every transaction and movement of goods. This reduces fraud, errors, and inefficiencies.
3, **Cross-Border Payments:** Blockchain simplifies and accelerates cross-border payments by providing a decentralized and transparent ledger. This reduces the need for intermediaries and minimizes delays and costs.
4. **Healthcare Data Management:** Blockchain secures the storage and sharing of healthcare records. Patients can grant access to their data securely, ensuring interoperability and data integrity.
5. **Real Estate:** Blockchain simplifies and secures real estate transactions by providing transparent and unalterable records of property ownership, reducing fraud and disputes.
6. **Food Safety:** In the food industry, blockchain can be used to trace the origin and journey of food products from farm to table, ensuring safety and authenticity.
7. I**nsurance:** Blockchain enhances the transparency and efficiency of insurance processes, including claims processing, policy issuance, and fraud prevention.

Illustration on Blockchain – Voting System

Using blockchain technology, personal identity information can be held on blocks and then it can be ensured that nobody votes twice, only eligible voters are able to vote, and votes cannot be tampered with. What's more, it can increase access to voting by making it as simple as pressing a few buttons on your smartphone, thereby reducing the cost of running an election substantially.

12.4 CLOUD COMPUTING

To understand Cloud Computing, we first must understand what the cloud is. **"The Cloud"** refers to applications, services, and data storage on the Internet. These service providers rely on giant server farms and massive storage devices that are connected via Internet protocols. Cloud Computing is the use of these services by individuals and organizations. We probably already use cloud computing in some forms. For example, if we access our e-mail via our web browser, we are using a form of cloud computing. If we use Google Drive's applications, we are using cloud computing. While these are free versions of cloud computing, there is big business in providing applications and data storage over the web. Salesforce is a good example of cloud computing as their entire suite of CRM applications are offered via the cloud. Cloud Computing is not limited to web applications; it can also be used for services such as phone or video streaming. 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 computers through the Internet.

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.

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 thus 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. 12.7). 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.

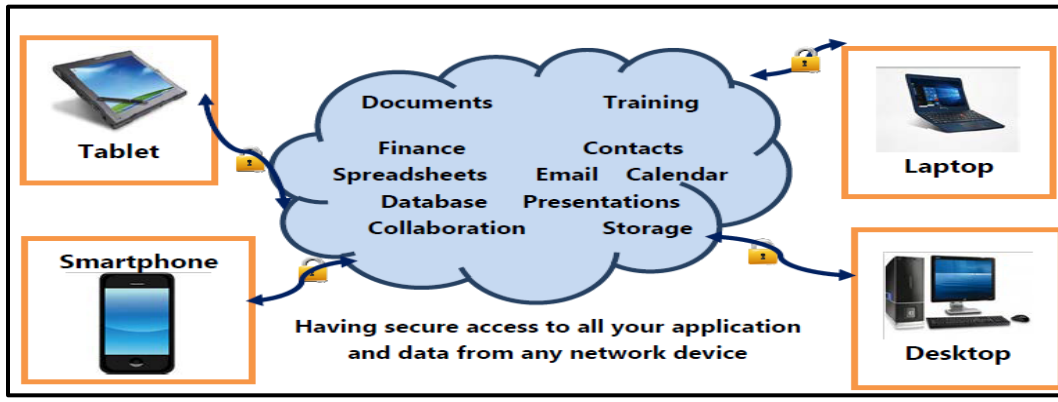


Fig. 12.7: Cloud Computing Scenario

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 benefit to small and medium-sized business systems, who wish to completely outsource their data-center infrastructure; or large companies, who wish to get peak load capacity without incurring the higher cost of building larger data centers internally. In both the instances, service consumers use **'what they need on the Internet'** and **'pay only for what they use'**.

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 is 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 up-fronts, 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'.

I. **Characteristics of Cloud Computing:** The following is a list of characteristics of a cloud-computing environment. Not all characteristics may be present in a specific cloud solution. However, some of the key characteristics as defined by National Institute of Standards and Technology (NIST), the American Standards Body are as follows:

- **On demand Self-service:** For the provision, monitoring, and management of computing resources, there is no client interaction with human administrators. The client can unilaterally provision computing resources, such as server processing time, storage, and so on, automatically and as needed, without requiring human interaction with the service vendor.
- **Broad network access:** Vendors deliver cloud computing resources over standard networks and heterogeneous devices, possibly the Internet. ICT (Information and Communication Technology) capabilities are available over the network and are

accessed through standard mechanisms, including many devices such as thin or thick client platforms (for example mobile phones, laptops, and smartphones).

- **Wide elasticity:** ICT resources can be provisioned to scale up quickly or be released rapidly to scale down fast. To the client, the capabilities available for provisioning might appear to be infinite, as they can potentially be purchased in any quantity and at any time.
- **Resource pooling:** The ICT resource vendors serve all clients using a multitenant model. Different physical and virtual resources are dynamically assigned and re-assigned according to the client demand. Examples of resources include storage, processing, memory, network bandwidth, and Virtual Machines (VM).
- **Measured service:** ICT resource utilization is measured for each application and for each tenant for public cloud billing or private cloud chargeback. Cloud systems automatically control and optimize resource usage by leveraging a metering capability. This should be appropriate to the type of service (for example storage, processing, bandwidth, and active client accounts). Resource consumption can be monitored and reported, providing visibility for both the vendor and the client of the services used.

II. Advantages of Cloud Computing

- **Achieve economies of scale:** In cloud computing; computational resources, storage, and services are shared between multiple customers. This results in achieving efficient utilization of resources and that too at reduced cost. Volume output or productivity can be increased even with fewer systems and thereby reduce the cost per unit of a project or product.
- **Reduce spending on technology infrastructure:** Data and information can be accessed with minimal upfront spending in a pay-as-you-go approach, which is based on demand. With the increased dependency of business organizations on IT, huge investment is required for acquiring IT resources. By using cloud computing, the organization can avoid purchasing hardware, software, and licensing fees. Moreover, cloud service providers are paid based on actual usage of resources, which is based on demand.
- **Globalize the workforce:** Cloud computing allows users to globalize their workforce and improve accessibility while shortening training time and new employee learning curves.
- **Streamline business processes:** Cloud Service Providers (CSPs) manage underlying infrastructure to enable organizations to focus on application development in less time with less resources.

- **Reduce capital costs:** Cloud computing users worldwide can access the cloud with Internet connection that subsequently does not require them to spend on technology infrastructure, hardware, software, or licensing fees.
- **Easy access to information/applications:** One can access information and applications as utilities anytime and anywhere, over the internet using any smart computing device.
- **Pervasive accessibility:** Data and applications can be accessed anytime, anywhere, using any smart computing device, making our life so much easier.
- **Backup and Recovery:** It is relatively much easier to backup and restore data stored in cloud. Even if one hard disk fails, data will be safe and will continue to be available automatically on another one.
- **Monitor projects more effectively:** It is feasible to confine within budgetary allocations and can be ahead of completion cycle times.
- **Less personnel training is needed:** It takes fewer people to do more work on a cloud with a minimal learning curve on hardware and software issues.
- **Minimize maintenance and licensing software:** As there is not much of non-premise computing resources, maintenance becomes simple and updates and renewals of software systems rely on the cloud vendor or provider.
- **Load balancing:** Load balancing is defined as the process of distributing workloads across multiple servers to prevent any single server from getting overloaded and possibly breaking down. It plays an important role in maintaining the availability of cloud-based applications to customers, business partners, and end users, thus making it more reliable.
- **Improved flexibility:** Cloud users can make fast changes in their work environment without serious issues at stake in order to scale services to fit their needs.

III. Drawbacks of Cloud Computing

- If Internet connection is lost, the link to the cloud and thereby to the data and applications is lost.
- Security is a major concern as entire working with data and applications depend on other cloud vendors or providers.
- Although Cloud computing supports scalability (i.e. quickly scaling up and down computing resources depending on the need), it does not permit the control on these resources as these are not owned by the user or customer.

- Depending on the cloud vendor or service provider, customers may have to face restrictions on the availability of applications, operating systems, and infrastructure options.
- Interoperability (ability of two or more applications that are required to support a business need to work together by sharing data and other business-related resources) is an issue wherein all the applications may not reside with a single cloud vendor and two vendors may have applications that do not cooperate with each other.

IV. Cloud Computing Deployment Models

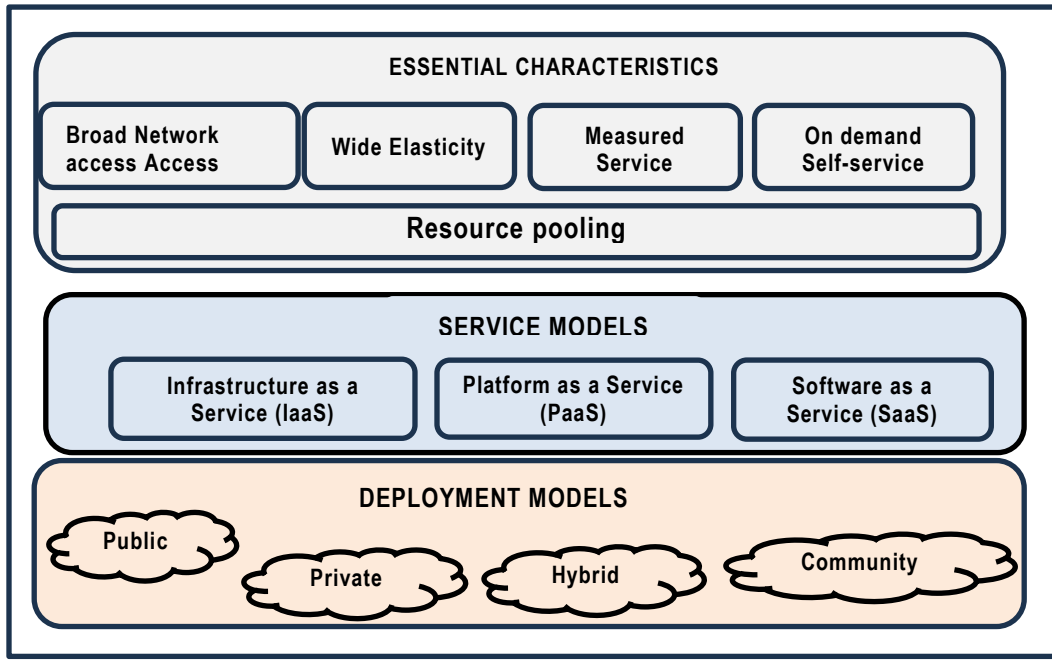


Fig. 12.8: The Cloud's Three Dimensions

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. 12.8 & Fig. 12.9).

(A) **Private Cloud:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for an organization's benefits. Also called **Internal Clouds** or **Corporate Clouds,** Private Clouds can either be private to an organization and managed by the single organization **(On-Premises Private Cloud)** or can be managed by third party **(Outsourced Private Cloud)**. 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.

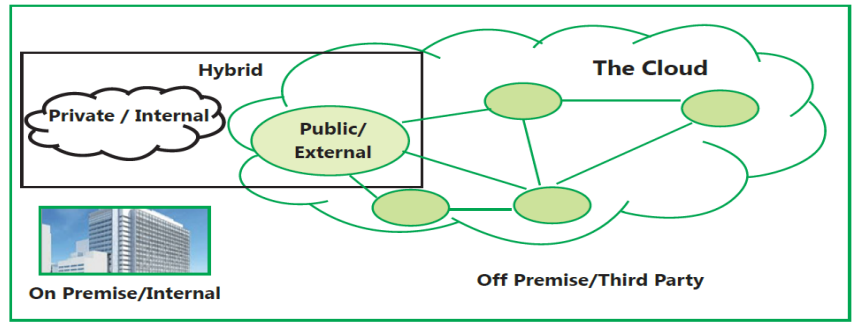


Fig. 12.9: Cloud Deployment Models

Characteristics of Private Cloud

- **Secure:** The private cloud is secure as it is deployed and managed by an organization itself, and hence there is least chance of data being leaked out of the cloud.
- **Central Control:** As usually the private cloud is managed by the organization itself, there is no need for an organization to rely on anybody and it is controlled by the organization itself.
- **Weak Service Level Agreements (SLAs):** SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider. In private cloud, either formal SLAs do not exist or are weak as it is between the organization and user of the same organization. Thus, high availability and good service may or may not be available.

Advantages of Private Cloud

- It improves average server utilization; allows usage of low-cost servers and hardware while providing higher efficiencies; thus, reducing the costs that a greater number of servers would otherwise entail.
- It provides a high level of security and privacy to the user as private cloud operations are not available to public.
- It is small and controlled and maintained by the organization.

Moreover, one major **limitation of Private Cloud** is that IT teams in an organization may have to invest in buying, building, and managing the clouds independently. Private cloud resources are not as cost-effective as public clouds and they have weak SLAs. The organizations require more skilled and expert employees to manage private clouds.

(B) Public/Provider Cloud: The public cloud is the cloud infrastructure that is provisioned for open use by the public. It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. Public cloud consists of users from all over the world wherein a user can simply purchase resources on an hourly basis and work with the resources which are available in the cloud provider's premises. Examples of public clouds are Google, Amazon, etc.

Characteristics of Public Cloud

- **Highly Scalable:** The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are scalable.
- **Affordable:** The cloud is offered to the public on a pay-as-you-go basis; hence the user has to pay only for what s/he is using (using on a per-hour basis) and this does not involve any cost related to the deployment.
- **Less Secure:** Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.
- **Highly Available:** It is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.
- **Stringent SLAs:** As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.

Advantages of Public Cloud

- It is widely used in the development, deployment, and management of enterprise applications, at affordable costs. Since public clouds share same resources with large number of customers, it has low cost.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- There is no need for establishing infrastructure for setting up and maintaining the cloud.
- Public clouds can easily be integrated with private clouds.

- ❖ Strict SLAs are followed.
- ❖ There is no limit to the number of users.

Moreover, one of the **limitations of Public Cloud** is security assurance and thereby building trust among the clients is far from desired because resources are shared publicly. Further, privacy and organizational autonomy are not possible.

(C) **Hybrid Cloud:** 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. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used. The hybrid cloud can be regarded as a private cloud extended to the public cloud and aims at utilizing the power of the public cloud by retaining the properties of the private cloud. The organization may perform non-critical activities using public clouds while the critical activities may be performed using private clouds. 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. Fig. 12.10 depicts hybrid cloud.

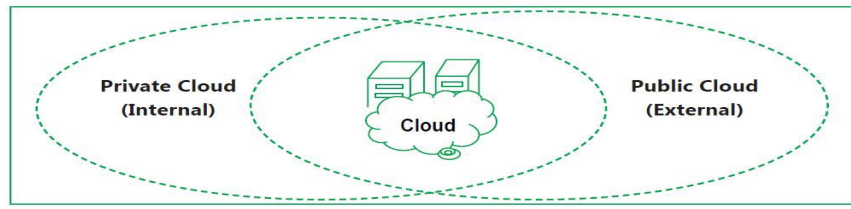


Fig. 12.10: Hybrid Cloud

Characteristics of Hybrid Cloud

- ❖ **Scalable:** The hybrid cloud has the property of public cloud with a private cloud environment and as the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable.
- ❖ **Partially Secure:** The private cloud is considered as secured and public cloud has high risk of security breach. The hybrid cloud thus cannot be fully termed as secure but as partially secure.
- ❖ **Stringent SLAs:** In the Hybrid Cloud, the SLAs are overall more stringent than the private cloud and might be as per the public cloud service providers.
- ❖ **Complex Cloud Management:** Cloud management is complex as it involves more than one type of deployment model, and the number of users is high.

The **Advantages of Hybrid Cloud** include the following:

- ❖ It is highly scalable and gives the power of both private and public clouds.
- ❖ It provides better security than the public cloud.

The **limitation of Hybrid Cloud** is that the security features are not as good as the private cloud and complex to manage.

(D) **Community Cloud:** The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. Fig. 12.11 depicts Community Cloud. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Characteristics of Community Cloud

- ❖ **Collaborative and Distributive Maintenance:** In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
- ❖ **Partially Secure:** This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.
- ❖ **Cost Effective:** As the complete cloud is being shared by several organizations or community, not only does the responsibility gets shared; the community cloud becomes cost effective too.

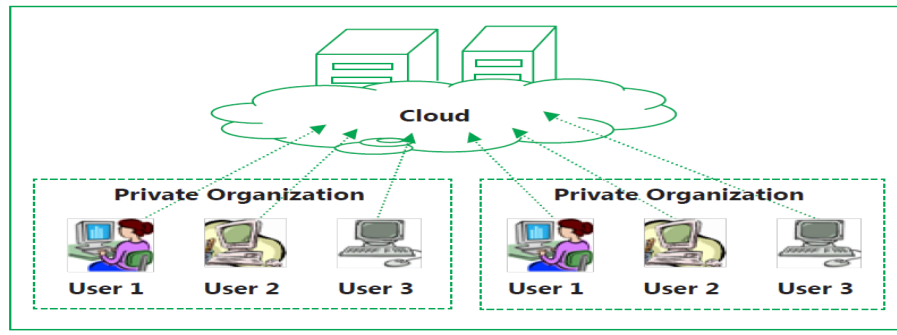


Fig. 12.11: Community Cloud

Advantages of Community Cloud

- ❖ It allows establishing a low-cost private cloud.
- ❖ It allows collaborative work on the cloud.
- ❖ It allows sharing of responsibilities among the organizations.
- ❖ It has better security than the public cloud.

The **limitation of Community Cloud** is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the case where there is no collaboration.

VI. Cloud Computing Service Models: Cloud computing is a model that enables the end users to access the shared pool of resources such as compute, network, storage, database, and application as an on-demand service without the need to buy or own it. The services are provided and managed by the service provider, reducing the management effort from the end user side. The essential characteristics of the cloud include on-demand, self-service, broad network access, resource pooling, rapid elasticity, and measured service. The National Institute of Standards and Technology (NIST) defines three basic service models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), presented pictorially in Fig. 12.12.

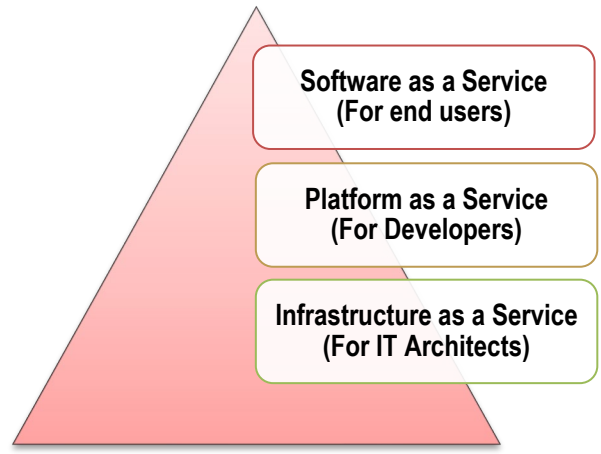


Fig. 12.12: Cloud Computing Service Models

(A) Infrastructure as a Service (IaaS): IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand. This allows users to maximize the utilization of computing capacities without having to own and manage their own

resources. The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs) and design virtual infrastructure, network load balancers etc., based on their needs.

Different Services provided by IaaS are shown in the Fig. 12.13.

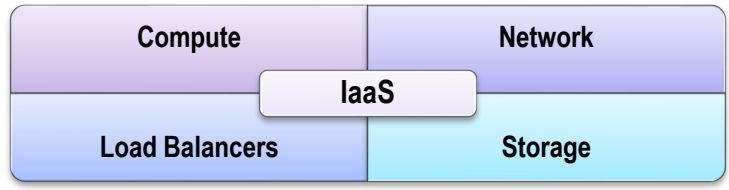


Fig. 12.13: Services Provided by IaaS

An IT architect need not maintain the physical servers as it is maintained by the service providers. Examples of IaaS providers include Amazon Web Services (AWS), Google Compute Engine, OpenStack and Eucalyptus.

Characteristics of IaaS

- **Web access to the resources:** The IaaS model enables the IT users to access infrastructure resources over the Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.
- **Centralized Management:** The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.
- **Elasticity and Dynamic Scaling:** Depending on the load, IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.
- **Shared infrastructure:** IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensures high resource utilization.
- **Metered Services:** IaaS allows the IT users to rent the computing resources instead of buying them. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

(B) **Platform as a Service (PaaS): PaaS** provides the users the ability to develop and deploy an application on the development platform provided by the service provider. In traditional application development, the application will be developed locally and will

be hosted in the central location. In stand-alone application development, the application developed by traditional development platforms results in licensing - based software whereas PaaS changes the application development from local machine to online. PaaS providers provide a pre-built computing platform consisting of operating system, programming languages, database, testing tools apart from some build tools, deployment tools, and software load balancers. The software developers can develop and run their software solutions on cloud platform without incurring cost and complexity of acquiring and managing the underlying software and hardware. For example- Google App Engine, Windows Azure Compute etc. Different Services provided by PaaS are shown in the Fig. 12.14.

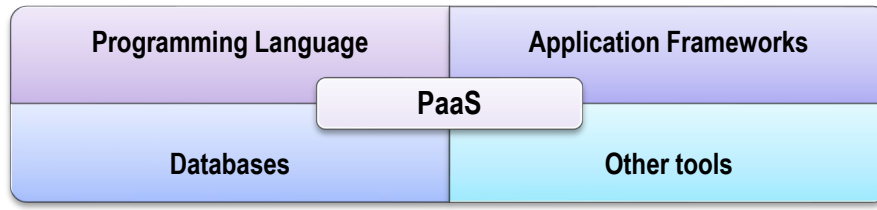


Fig. 12.14: Services Provided by PaaS

Typical PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases.

(a) **Programming Languages:** PaaS providers provide a wide variety of programming languages like Java, PHP, Python, Ruby etc. for the developers to develop applications.

(b) **Application Frameworks:** PaaS vendors provide application development framework like Joomla, WordPress, Sinatra etc. for application development.

(c) **Database:** Along with PaaS platforms, PaaS providers provide some of the popular databases like ClearDB, Cloudant, Redis etc. so that applications can communicate with the databases.

(d) **Other Tools:** PaaS providers provide all the tools that are required to develop, test, and deploy an application.

Characteristics of PaaS are as follows:

- **All in One:** Most of the PaaS providers offer services like programming languages to develop, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).

- **Web access to the development platform:** PaaS provides web access to the development platform that helps the developers to create, modify, test, and deploy different applications on the same platform.
- **Offline Access:** To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.
- **Built-in Scalability:** PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.
- **Collaborative Platform:** To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.
- **Diverse Client Tools:** PaaS providers offer a wide variety of client tools like Web User Interface (UI), Application Programming Interface (API) etc. to help the developers to choose the tool of their choice.

(C) **Software as a Service (SaaS): SaaS** provides the ability to the end users to access an application over the Internet that is hosted and managed by the service provider. Thus, the end users are exempted from managing or controlling an application, the development platform, and the underlying infrastructure. SaaS has changed the way the software is delivered to the customers. SaaS provides users to access a large variety of applications over internet that is hosted on service provider's infrastructure. The main difference between SaaS and PaaS is that PaaS normally represents a platform for application development, while SaaS provides online applications that are already developed. 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. Different Services provided by SaaS are shown in the Fig. 12.15.

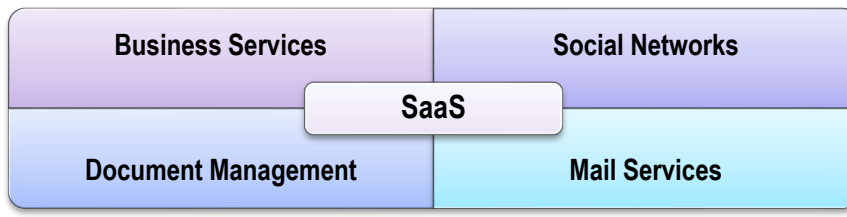


Fig. 12.15: Services Provided by SaaS

The services provided by SaaS as depicted in Fig. 12.15 are as follows:

(a) **Business Services:** SaaS providers provide a variety of business services to startup companies that include ERP, CRM, billing, sales, and human resources.

(b) **Social Networks:** Since the number of users of the social networking sites is increasing exponentially, cloud computing is the perfect match for handling the variable load.

(c) **Document Management:** Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.

(d) **Mail Services:** To handle the unpredictable number of users and the load on e-mail services, most of the email providers offer their services as SaaS services.

Characteristics of SaaS are as follows:

- **One to Many:** SaaS services are delivered as one-to-many models where a single instance of the application can be shared by multiple customers.
- **Web Access:** SaaS services allow the end users to access the application from any location of the device is connected to the Internet.
- **Centralized Management**: Since SaaS services are hosted and managed from the central location, the SaaS providers perform the automatic updates to ensure that each customer is accessing the most recent version of the application without any user-side updates.
- **Multi-device Support:** SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones, and thin clients.
- **Better Scalability:** Most of the SaaS services leverage PaaS and IaaS for its development and deployment and ensure a better scalability than traditional; software.
- **High Availability:** SaaS services ensure 99.99% availability of user data as proper backup and **recovery** mechanisms are implemented.
- **API Integration:** SaaS services have the capability of integrating with other software or services through standard APIs.

(D) Other Cloud Service Models (Refer Table 12.3)

Table 12.3: Other Cloud Service Models

Instance	Description
Communication as a Service (CaaS)	• It 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.
Data as a Service (DaaS)	• This provides data on demand to diverse set of users, systems or application. The data may include text, images, sounds, and videos. • Data encryption and operating system authentication are commonly provided for security. DaaS users have access to high-quality data in a centralized place and pay by volume or data type, as needed. • However, as the data is owned by the providers, users can only perform read operations on the data. DaaS is highly used in geography data services and financial data services.
Security as a Service (SECaaS)	• It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. • It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats.
Identity as a Service (IDaaS)	• It is an ability given to the end users; typically, an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed, and provided by the third-party service provider. • Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

Network as a Service (NaaS)	• It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis. • Provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. • Allows network architects to create virtual networks; virtual Network Interface Cards (NICs), virtual routers, virtual switches, and other networking components. • Allows the network architect to deploy custom routing protocols and enables the design of efficient in-network services, such as data aggregation, stream processing, and caching. NaaS providers operate using three common service models: Virtual Private Network (VPN), Bandwidth on Demand (BoD) and Mobile Virtual Network (MVN).
Storage as a Service (STaaS)	• It is an ability given to the end users to store the data on the storage services provided by the service provider. • This provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. • STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center.
Database as a Service (DBaaS)	• It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis. • This provides users with seamless mechanisms to create, store, and access databases at a host site on demand. • The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.
Backend as a Service (BaaS)	• This provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using

	custom software development kits and application programming interfaces.
Desktop as a Service (DTaaS)	• It is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. • It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. • The end-users are responsible for securing for managing their own desktop images, applications, and security. These services are simple to deploy, are highly secure, and produce better experience on almost all devices.
Testing as a Service (TaaS)	• This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.
API as a Service (APIaaS)	• This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
Email as a Service (EaaS)	• This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

VI. Pertinent Issues related to Cloud Computing: As an emerging technology, cloud computing involves several issues, out of which some of them are as follows:

- **Threshold Policy:** The main objective of implementing threshold policy is to inform cloud computing service consumers and providers what they should do. Quite often, this policy does not exist. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do. However, there is no standard format for the SLA, and as such, there may be services not documented in the SLA that the customer may be requiring in future.
- **Interoperability:** If a company enters a contract with one cloud computing vendor, it may find it difficult to change to another computing vendor that has proprietary APIs (Application Programming Interfaces) and different formats for importing and exporting

data. Industry cloud computing standards do not exist for APIs or formats for importing/exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. Once a company is locked in with one cloud provider, it is not easy to move an entire infrastructure to other clouds. Moreover, each cloud provider offers a unique set of services and tools for operating and controlling its cloud. Learning a new cloud environment is like learning a new technology.

- **Hidden Costs:** Such costs may include higher network charges for storage and database applications, or latency issues for users who may be located far from cloud service providers.
- **Unexpected Behavior:** An application may perform well at the company's internal data center. It does not necessarily imply that the application will perform the same way in the cloud. Therefore, it is essential to test its performance in the cloud for unexpected behavior. Testing may include checking how the application allocates resources on sudden increase in demand for resources and how it allocates unused resources. This problem must be solved before obtaining services from the cloud.
- **Security Issues:** Cloud computing infrastructures use new technologies and services, most of which have not been fully evaluated with respect to security. The important security issues with cloud computing are the management of the data might not be fully trustworthy; the risk of malicious insider attacks in the cloud; and failing of cloud services. Maintaining confidentiality is one of the major issues faced in cloud systems because information is stored at a remote location which can be accessed by the service provider. Data confidentiality can be preserved by encrypting data. Cloud systems share computational resources, storage, and services between multiple customer applications to achieve efficient utilization of resources while decreasing cost. However, this sharing of resources may violate the confidentiality of users' IT Assets. It must be ensured that there is a degree of isolation between these users. In most cases, the provider must ensure that their infrastructure is secure and that their consumers' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.
- **Legal Issues:** Cloud systems need to adhere to several regulatory requirements, privacy laws and data security laws. These laws vary from country to country and cloud users have no control over where their data is physically located.
- **Software Development in Cloud:** From the perspective of the application development, developers face the complexity of building secure applications that may

be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security. The project manager must keep in mind the applications should be upgraded frequently. For this, the project manager must ensure that their application development processes are flexible enough to keep up with the changes.

- **Bugs in Large-Scale Distributed Systems:** One of the difficult challenges in Cloud Computing is removing errors in these very large-scale distributed systems.

Illustration on Cloud Computing - Netflix

- From its beginnings as a DVD rental business, the Netflix streaming service has come a long way. It commands the attention of millions of people who are eager to watch one of its hundreds of critically acclaimed programs, films, or documentaries.
- Soon Netflix realized that their typical in-house data center was rapidly becoming too inefficient, and they need to explore a method that could store all its data due to its large user base. They required scalability in their infrastructure.
- Netflix claims that its 117.58 million global customers view 140 million hours of video each day. In other words, a usual Netflix customer spends 1 hour and 11 minutes each day on the site or 71 minutes per day.
- The Netflix is a worthy example of visualizing how they were able to move their entire data on the cloud using the technology.

12.5 BIG DATA

Big Data is a term for a collection of data which is so large that it becomes difficult to store and process using traditional databases and data processing applications. Some examples of data that inputs into big data systems can include social network traffic, web server logs, streamed audio content, banking transactions, web page histories and content, government documentation and financial market data etc.

According to **Gartner, Big Data** can be described using the **'3Vs'** i.e. **Big data** is high-**volume**, high-**velocity** and/or high-**variety** information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.

- **Volume:** Refers to the significant amount of data that an organization needs to store and process.
- **Variety:** Wide variety of data that can come from various sources.

- **Velocity:** Data is likely to change on a regular basis and needs to be continually updated.

Another 'V' which is added by some organizations to the above list is -

- **Veracity (truthfulness):** Organization gathers the data that is accurate, the failure to do will make analysis meaningless.

I. What is Big Data in FinTech?

Big Data in finance refers to the petabytes of structured and unstructured data that may be utilized by banks and financial organizations to predict consumer behavior and develop strategies. The financial sector creates a large amount of data.

Structured data is information that is maintained within a company to give crucial decision-making insights. **Unstructured data** is accumulating from a variety of sources in ever-increasing numbers, providing considerable analytical potential.

Emerging FinTech is using big data to forecast client behavior and generate sophisticated risk evaluations, setting them apart from traditional financial institutions. Disruptive FinTech and challenger banks can react to a changing market thanks to the speed of real-time data. They may flip to aggressive methods at any time, leaving the major banks struggling to stay up.

FinTech can make better judgments and provide more personalized consumer experiences thanks to their capacity to handle big data volumes. FinTech may utilize big data to understand their consumers on a one-to-one basis, rather than guessing or covering their backs with cautious risk assessments.

II. Big Data in FinTech Industry

Emerging FinTech can benefit from big data analysis in four ways:

(i) **Customer Orientation:** FinTech may utilize big data to develop thorough user profiles and precise client segmentation strategies, allowing them to customize their services to their specific demands. Individualized services may be provided using sophisticated modeling approaches that consider an individual's risk perception, age, gender, money, location, and even relationship status.

(ii) **Enhanced Security:** While fraud is a prevalent problem in the digital banking sector, big data may assist FinTech in developing accurate fraud detection systems by detecting any odd transactions. FinTech may also use digital applications to keep consumers informed about security concerns and secure their money.

(iii) **Improved Risk Assessments:** FinTech businesses that specialize in big data analytics may integrate data from a variety of sources to guarantee that no stone is left unturned. FinTech can operate with more financial certainty, manage cash flow, and give consumers competitive rates thanks to improved risk assessments.

(iv) **Unmatched Customer Service:** FinTech may use big data to establish a digital trail of a customer's financial behavior, spot possible problems, and give consistent assistance. FinTech may also use data and forecasts to propose the correct services/products depending on their clients' specific spending habits.

III. Chatbots and Robotic Process Automation (RPA)

Chatbots use artificial intelligence to enable interaction on 24x7 basis. These intelligent Chatbots may assist consumers in several ways, including handling transactions, providing vital information, and handling transactions. RPA improves the user experience by allowing bots to undertake repetitive (and labor-intensive) tasks without the need for human interaction. It not only reduces mistakes but also frees up team members to deal with more complicated issues and deliver better customer support.

IV. Big Data in developing strategies in companies.

Big data is in high demand in finance for a variety of reasons:

(i) Lack of personal connection with the customers: Users expect to be able to address their problems without having to go to a bank office, but this makes gathering information on clients more difficult. Mobile gadgets can be of assistance. They let companies gather many sorts of information, such as geolocation, the most common user interactions, user behavior, and browsing history. This information may then be utilized to make up for a lack of face-to-face connection with clients.

(ii) Growth in FinTech's social media footprint: Users make purchases and engage with companies using social media, which is no longer only a platform for connecting with friends and family. Examining user behavior on social media is critical for FinTech firms to gain insights and apply them when selling products or services. Insurers, for example, may create unique plans based on social media data, and banks can use social media data to create credit scores.

(iii) Shift in customers' expectations: Customers want businesses to not just meet their requirements, but also to anticipate and surpass them. This is impossible without consumer information. To provide tailored offers for clients, a FinTech company should collect data from numerous channels such as their mobile app, website, wearables, social media, and smart devices. The client no longer needs to visit physical sites or

wait days for transactions to be completed. FinTech has developed cross-border financial services that enable real-time data sharing and allows buyers/sellers to conduct business without friction.

IV. FinTech is becoming increasingly competitive

The FinTech sector is quickly expanding, attracting an increasing number of entrepreneurs, startups, and established businesses every day. The ability of a FinTech product to deliver a service is critical to its success in this competitive industry.

Big data enables businesses to optimize their operations in real-time and provide their customers with the finest services possible based on hard facts.

Reduced operating expenses allow firms to dedicate resources to marketing and decrease pricing for customers, allowing them to stay ahead of the competition. As a result, FinTech companies must automate their operations to save money and big data insights can assist.

V. Obstacles in adopting analytics by Financial Institutions

Though big data has many benefits to financial organizations, there are many institutions still hesitant about adopting digitization. There are several reasons for that – a few of them are listed below:

- **Outdated software:** Outdated software is among the top reasons why financial organizations are unwilling to adopt innovative technologies, including analytics. In order to do so, a financial organization would have to redesign its existing system to make it compatible with the needed software solution. And this might take too much time and resources.
- **Lack of needed resources:** Proper information processing requires many resources, including specific specialists (like data scientists), implementation (and sometimes development) of an ML model for information processing and analysis, and implementation of the selected analytics solution. Thus, an organization needs to have a scalable and robust infrastructure and most financial organizations find these processes too cumbersome.
- **Lack of short-term results:** Financial Institutions are very slow with the adoption of technological innovations is that they do not see short-term results. It might take more than 5 years to start receiving sufficient ROI from implementing a single software solution, and for some organizations, the wait is not worth it.

Illustration on Big data: IBM

IBM is a technology and consulting corporation that manufactures computer hardware and software and offers infrastructure for products ranging from mainframe computers to nanotechnology.

IBM made itself committed to Big Data and Analytics through sustained investments and strategic acquisitions. Also, IBM tried to bring as many Big Data technologies as possible under its umbrella. The strategy of the company was to combine a wide array of Big Data analytic solutions and conquer the Big Data market. The aim of the company was to offer the broadest portfolio of products and solutions with a depth and breadth that no other company could match.

The company observed that over the years, consumer attention had shifted from radio, print, and television to the digital media as it facilitated real-time engagement of consumers. Brands competed for consumer attention through such media and relied on them for data and analytics for customer acquisition and retention and to offer tailor-made products and services to them. The company found that the real challenge with such data was that it was mostly unstructured, and the difficulty lay in structuring it and filtering the genuine data.

The company developed new systems, software, and services to complement its Big Data platform as they found that the Big Data solution is meant to protect data and identify and restrict suspicious activity and block access to company data.

It enabled companies to run live simulations of trading strategies, geological and astronomical data, and stockbrokers could analyze public sentiment about a company from social media. Emerging technologies such as Hadoop and NoSQL made such analytics possible.

SUMMARY

This chapter provides the detail of FinTech. It is the abbreviation for financial technology, is a broad category that refers to the innovative use of technology in the design and delivery of financial services and products. FinTech companies offer a wide range of products and services. FinTech companies are versatile and include lower fees and better rates, lower thresholds for investments, lower thresholds for loans, ease of use and convenience. This is manifested in lower margins, asset-light nature, and high scalability.

Bitcoin technology that uses cryptographic proof in its computer software, instead of trusted third parties, to process and record transactions. Cryptography proof of work is used to verify the legitimacy of bitcoins. Bitcoin is not a fiat currency issued by a central government or an authorized agent of the government.

Artificial Intelligence in FinTech stands for Development of smart systems and machines that can carry out tasks (sense, reason, act and adapt) that typically require human intelligence.

Blockchain of FinTech is like a giant spreadsheet for registering all assets, and an accounting system for transacting them on global scale that can include all form of assets held by all parties worldwide.

Cloud computing in FinTech is also discussed that simply means the use of computing resources as a service through networks, typically the Internet. Cloud Computing is both a combination of software and hardware-based computing resources delivered as a networked service.

Big data of FinTech technology is a term for a collection of data which is so large that it becomes difficult to store and process using traditional databases and data processing applications.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Ms. Komal a technical product developer at FEGO Ltd. suggested the company to manufacture a model of self-driving car based on image and text recognition. This is a good example of _____.

   (a) Artificial Intelligence

   (b) Expert System

   (c) Cloud Computing

   (d) Mobile Computing

2. Which of the following is not the service provided by Infrastructure as a Service (IaaS) model of Cloud Computing?

   (a) Load balancer

   (b) Storage

   (c) Network

   (d) Application framework

3. Which of the following instance of Cloud Computing is being used by Amazon Web Service (AWS)?

   (a) Infrastructure as a Service

(b) Storage as a Service

(c) Network as a Service

(d) Software as a Service

4. Which of the following is not an advantage of Cloud Computing?

(a) Improved flexibility

(b) Streamline business processes

(c) Interoperability

(d) Reduce Capital Costs

5. In Cloud Computing, which instance of Software as a Service (SaaS) allows users to explore functionality of Web services such as Google Maps, Payroll processing and Credit Card processing services, etc.?

(a) Testing as a Service (TaaS)

(b) Communication as a Service (CaaS)

(c) Data as a Service (DaaS)

(d) API as a Service (APIaaS)

ANSWERS/SOLUTIONS

1.	**(a)**	**2.**	**(d)**	**3.**	**(a)**	**4.**	**(c)**	**5.**	**(d)**

CHAPTER 13

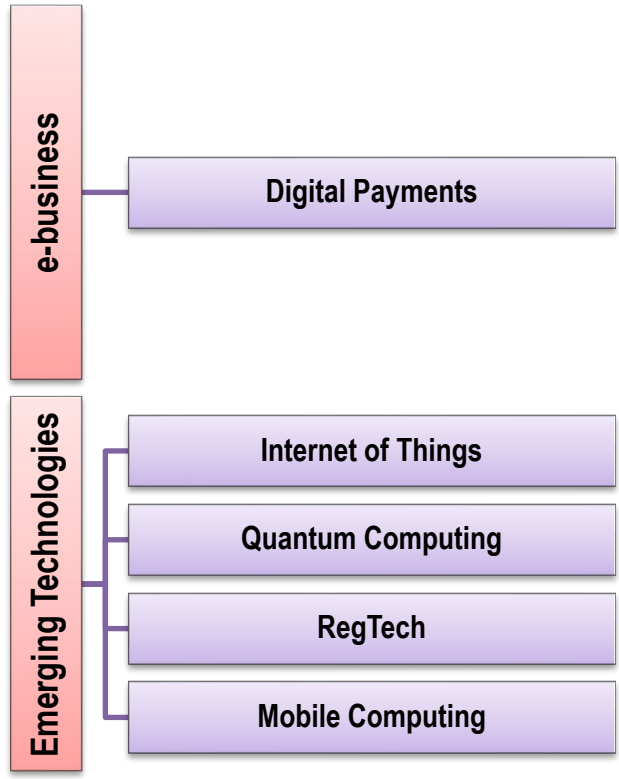
EMERGING TECHNOLOGIES

LEARNING OUTCOMES

After studying this chapter, you will be able to –

- understand e-business and associated risks and their controls.
- comprehend various digital payment used in today's world along with their advantages and disadvantages.
- acknowledge various paradigms of Internet of Things (IoT) with its application in Finance and Accounting.
- gain knowledge about Quantum Computing and its advantages in financial organizations.
- understand Regtech technology.
- conceptualize Mobile Computing and its benefits.

CHAPTER OVERVIEW



13.1 INTRODUCTION

Today's world is driven by technology. Each day brings a new emerging trend in the digital world to back up and support the businesses and society as a whole. Every day the world sees newly developed solutions - models designed to work closely with the physical and the digital world. Technologies such as Mobile Computing, 3D printing, Cloud Computing, Quantum Computing, etc. have changed our working style and made the work easier.

These emerging technologies are seen to have enormous potential to meet global challenges. These technologies are interrelated with each other such as mobile technology can leverage other technologies such as social media or predictive analysis. Through mobile apps, users can purchase and buy anything anytime. The relationship between financial transactions and the internet is triggered with the use of these emerging technologies. The digital finance or payment industry is promoted using technological innovation. Modern day transactions are constantly shifting from cash-

based technology to technology-based transactions. The most convenient way is to make the payment using digital cash or digital payment.

13.2 DIGITAL PAYMENTS

From booking a taxi to washing clothes and doing work in an office, technology has brought transition in every sector. Technology has not only made the work easier but also changed the way of payments. From contactless payment to mobile wallet, it becomes much easier to pay for any type of goods and services. The modern payment and e-business have made it simpler and more efficient not only businesses but also for consumers to exchange money and enhances the security. These technologies have implications on the financial system of businesses. The new digital payment system has enabled the organizations to expand their market presence. These new digital payments have truly revolutionized how we do business, thus showing how important technology is when it comes to modern day business.

The benefits of digital payments are as following:

(i) **Easy and convenient:** Digital payments are easy and convenient as the transactions made during are simple click based. Digital payment eradicates the security risks associated with handling cash. This ease of transaction is more secure as compared to making transactions including cash.

(ii) **Pay or send money from anywhere:** Digital payments are available 24/7, meaning users can make payments anywhere, anytime.

(iii) **Tax Discounts:** To encourage digital payments, the government consistently provides attractive discounts on specific commodities when purchased through digital channels. For instance, users can avail 0.75% discount on fuels and a 10% discount on insurance premiums from government insurers.

(iv) **Log maintenance:** User often forgets to note down his/her cash spending whereas digital payments are automatically recorded in passbook or inside E-Wallet app. This helps to maintain record, track spending and budget planning. Digital payments thus drive the development and add modernization to payment system, promote transparency in economy.

(v) **Less Risk:** Digital payments entail lower risks when used judiciously. In the event of a lost mobile phone or Debit Card/Credit Card/Aadhaar Card, users need not be overly concerned. Unauthorized access to someone else's funds is prevented by requiring MPIN, PIN, or fingerprint verification in the case of Aadhaar. It is advisable for users to promptly block their cards if they are misplaced.

(vi) **Competitive advantage to business:** Digital payment enables businesses to make sales to customers who choose to pay electronically and gain a competitive advantage over those who accept payment only through traditional methods. It helps businesses to grow their customers' base and resource pool throughout the globe.

(vii) **Environment Friendly:** Digital payments eliminate the need for paper, promoting environmentally friendly practices known as Green Computing.

National Payments Corporation of India (NPCI), an umbrella organization for operating retail payments and settlement systems in India, is an initiative of Reserve Bank of India (RBI) and Indian Banks' Association (IBA) under the provisions of the Payment and Settlement Systems Act, 2007, for creating a robust Payment & Settlement Infrastructure in India.

Various types of digital payment are as following (Refer Fig. 13.1):

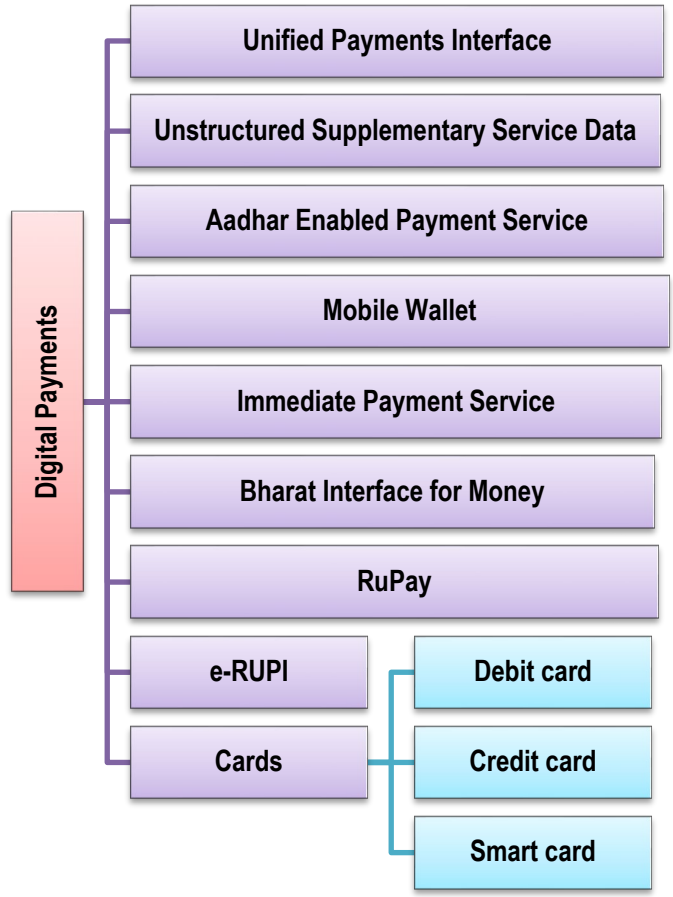


Fig. 13.1: Types of Digital Payments

A. Unified Payments Interface (UPI): It is a system that powers multiple bank accounts (of participating banks), several banking services features like fund transfer, and merchant payments into a single Mobile Application (of any participating bank), into one hood. The upper limit per UPI transaction is ₹ 1 lakh. There are many UPI apps available such as BHIM, SBI UPI app, HDFC UPI app, iMobile, PhonePe app, Axis app, UPI Collect etc. It can be used for various activities such as bill sharing with friends, payment to merchants, utility bill payments, Barcode based payments, donations, etc.

- It has transformed the landscape of banking by shifting a significant portion of banking activities to digital platforms through mobiles and apps. UPI is a payment mode that enables instant fund transfers from the sender's bank account to the receiver's bank account through a mobile app.
- It has enabled a seamless P2P (peer to peer) and P2M (peer to merchant) payment experience through a virtual address to push or pull payment using any third-party application provider authorized by the participating bank.
- UPI follows the one-click, two factor authentication protocol. When a transfer transaction is initiated using a smartphone, the device's fingerprint or other technical detail which is unique to the device is passed as the first factor of authentication. The second factor is the UPI PIN, which must be typed by the user on its mobile phone.
- In the year 2022, NPCI (National Payments Corporation of India) launched UPI123Pay, an instant payment system designed for feature phone users. This service allows them to utilize the Unified Payments Interface (UPI) in a safe and secure manner, indicating a broader adoption of digital transactions in rural areas where a significant portion of the population still does not own smartphones.
- It also caters to the 'Peer to Peer' collect request, which can be scheduled and paid as per requirement and convenience.
- Users must register for mobile banking to use UPI apps. Users can transfer funds between two accounts using UPI apps. They can use more than one UPI app on the same mobile and link them with the same as well as different accounts.
- As a fully digital system, UPI can be utilized 24/7, including on public holidays.
- Customers cannot link wallet to UPI, he can only add bank accounts. UPI provides only inter/intra bank accounts transfers.
- UPI also enables non-financial transactions such as Mobile Banking Registration, One Time Password (OTP) generation, UPI PIN Set/Change, UPI transaction status check, etc.

- Users need to download a UPI app and create a VPA (Virtual Payment Address) or UPI ID which can be used to transfer funds. It is not the actual payment address but act as the payment address. Hence, user can link many accounts with one VPA.

Fig. 13.2 shows the benefits of using UPI app by Customers, banks, and merchants.

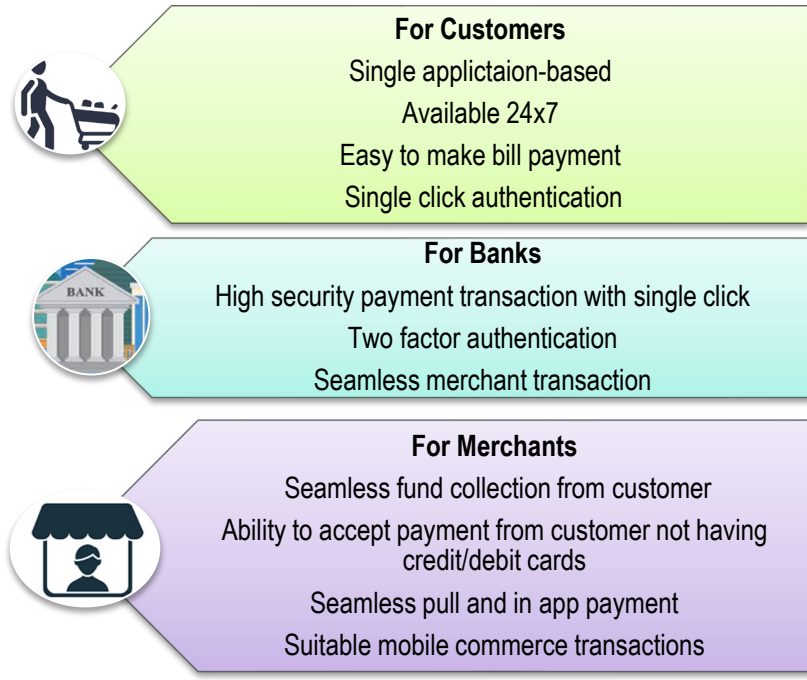


Fig. 13.2: Benefits of using UPI app

Illustration on Usage of UPI payment

Ms. Kavita has received a notification on her phone which was a message from a UPI ID of her younger brother who is studying in another city. He was asking her if she could instantly send him ₹ 4000. After calling her brother and checking with him, Ms. Kavita then uses her own HDFC net banking app to process the fund request, transfer the money and authenticate the transaction with her M-PIN. In a few seconds, she received a successful transaction notification SMS on her phone from her bank. Her brother also thanked her for the instant fund transfer.

B. Unstructured Supplementary Service Data (USSD): It is a revolutionary idea where to make payments through mobiles one neither needs to have internet nor any smart phone. USSD banking or *99# Banking is a mobile banking based digital payment mode. User does not need to have a smartphone or internet connection to use USSD banking.

- Users can easily use it with any normal feature phone and is as easy as checking mobile balance. Users can use this service for many financial and non-financial operations such as checking balance, sending money, setting/generating or changing Mobile Banking Personal Identification Number (MPIN) and getting Mobile Money Identifier (MMID).
- Users do not need to have a GPRS or any similar data connection on their mobile devices. They can use the service from any GSM mobile connection that includes calling features.
- The maximum amount that can be transferred is ₹ 5000 per day and only one transaction can be done per session.
- Various services can be used using USSD banking like *99*46*1# is used for Balance Inquiry, *99*46*2# is used for Mini statement and *99*46*3# is used for Instant Money Transfer

C. **Aadhar Enabled Payment Service (AEPS):** AEPS is an Aadhaar based digital payment mode offered by National Payments Corporation of India (NPCI) to banks and financial Institutions. The services offered by Aadhaar Enabled Payment Service are depicted in Fig. 13.3.

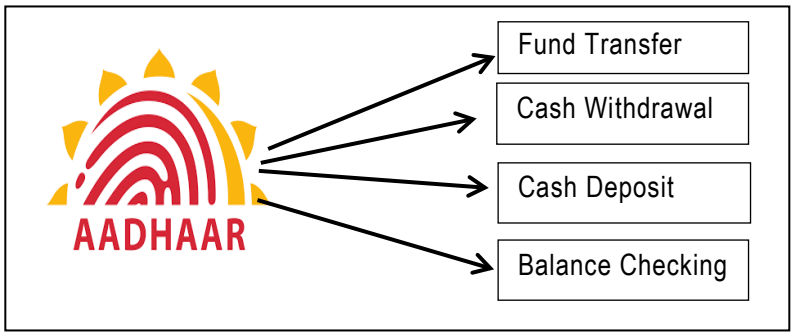


Fig. 13.3: Services Offered by Aadhaar Enabled Payment Service

- AEPS allows bank-to-bank transactions and customers need only their Aadhaar number to pay to any merchant.
- It is the bank led model that allows online financial inclusion transaction using the Aadhaar Authentication. It means the money the customer pays will be deducted from his/her account and credited to the payee's account directly.
- Customers are required to link their Aadhaar numbers to their bank accounts. Once launched, AEPS can also be used at Point of Sale (PoS) terminals.

- AEPS can be used for all banking transactions such as balance enquiry, cash withdrawal, cash deposit, payment transactions, Aadhaar to Aadhaar fund transfers, etc.
- All transactions are carried out through a banking correspondent based on Aadhaar verification. There is no requirement to go to a branch, provide debit or credit cards, or even make a signature on a document.
- It is one of the most cost-effective, safe, and secure means of paperless Know your Customer (KYC) to all Banks/non-bank entities in India which may save a lot of cost and effort related to storing physical KYC proofs.
- AEPS accounts can be opened based on simplified KYC guidelines. The bank with which the bank account of user is linked with Aadhar card would set the appropriate limit per transaction in a day. Few Indian banks that are members of AEPS are ICICI Bank, Union Bank of India, Bank of India. Fig. 13.4 describes the working of AEPS.

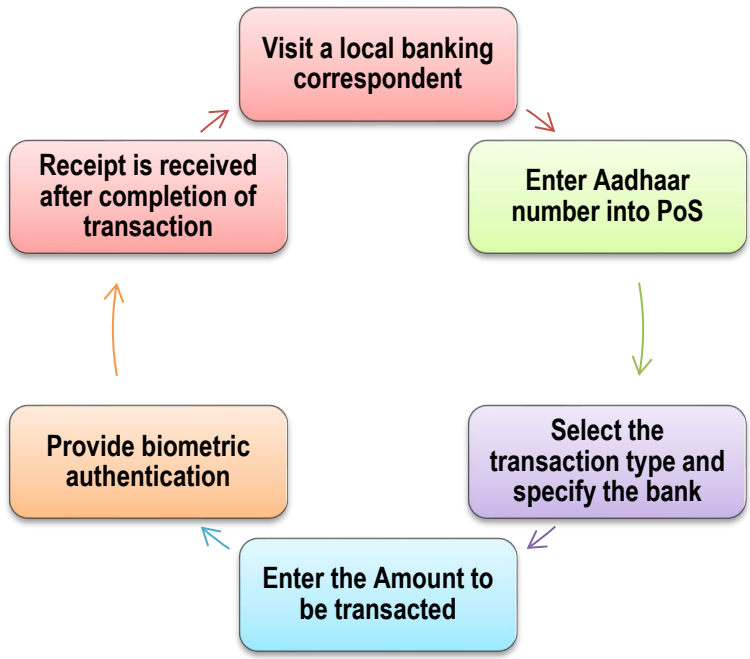


Fig. 13.4: How the transaction takes place in AEPS

Illustration for AEPS

Ms. Neha runs a small village handicrafts sourcing business where she buys items from many rural women's groups around the country that have different bank accounts than her own. As she doesn't always have access to her home bank branch account due to network issues. She is not able to see whenever someone make any transactions in her

bank account, hence, she preferred Aadhaar-enabled service through which wherever she can make a Balance Enquiry, so that she is aware of her receipts and expenditure as she travels.

D. **Mobile Wallet:** This is the new method of payment that has increased the prevalence in our lives. This innovation allows us to store the payment details and transaction history at one secure place.

- It also requires users to enter authenticated login details to make the transaction.
- Some banks also provide advanced security features, such as encryption and biometrics integrated into mobile payments, assuring users that their data is thoroughly protected against external threats.
- Users are not obligated to carry physical cards, making it a preferred choice for those who frequently travel and prefer not to carry cash or cards.
- Users can avail various offers such as cash back, discounts, coupons, etc., from the wallet provider while transacting.
- Only intra-wallet transfers are allowed, no inter-wallet transfer is allowed.
- Most of the mobile wallet service providers have a monthly limit of depositing amounts up to INR 10,000. Mobile wallets can have zero balance.

E. **Immediate Payment Service (IMPS):** It is an instant inter and intra-bank electronic fund transfer service through mobile phones. IMPS is an empathetic tool to transfer money instantly within banks across India through Mobile, Internet Banking and ATM, which is not only safe but economical also.

- It comprises of two methods for fund transfer:
  - i. Using Mobile number + Mobile Money Identifier (MMID)
  - ii. Using Account number + IFSC
- It provides robust and real time, 24x7 instant interbank electronic fund transfer service.
- It can be accessed through mobile, Internet, Branch, ATM and SMS.
- It also provides a foreign inward remittance facility for beneficiary customers.
- It also provides non-financial transactions such as checking of status, name of beneficiary, etc.

Transferring funds through IMPS

Follow the steps mentioned below to transfer funds through IMPS:

- **Step 1**: Install the mobile banking app of your bank. You can also use the internet banking facility for transferring money via IMPS and follow the steps given below.
- **Step 2**: Log in on your bank's mobile application using your credentials (Customer ID/ User ID and Password)
- **Step 3**: Once you have successfully logged in, select the 'Transfer' option and choose to add beneficiary. Alternatively, you can also choose the 'One Time Transfer' option.
- **Step 4**: Now, complete the process using IMPS by providing either MMID & mobile number details or account number & IFSC code.

Illustration of IMPS

Mr. Kamal, a senior manager in a software development company, had gone on an official visit to USA. His son had an accident, and his wife took their son to hospital. She needed to deposit a certain amount in the hospital. She was running short of money, so she called Mr. Kamal. He immediately transferred the money from his salary account to his home in India. He directly transferred the fund to his wife's bank account through net banking IMPS transfer. His wife got the money immediately when he transferred the amount.

F. Bharat Interface for Money (BHIM): It is a Mobile App developed by NPCI based on UPI (Unified Payment Interface). It is the launchpad for UPI platform and brought features like sending money, scan and pay, collect request, feature phone-based payments (*99# USSD Service), UPI LITE, RuPay, Aadhaar OTP, e-RUPI, etc. that banks could extend to their user base. Refer Fig. 13.5.

- It facilitates e-payments directly through banks and supports all Indian banks which use that platform. It is built on the Immediate Payment Service infrastructure and allows the user to instantly transfer money between the bank accounts of any two parties.
- It is also possible to link multiple bank accounts. BHIM works on all mobile devices and enables users to send or receive money to other UPI payment addresses by scanning QR code or using account number with Indian Financial Systems Code (IFSC) code or MMID (Mobile Money Identifier) Code for users who do not have a UPI-based bank account.

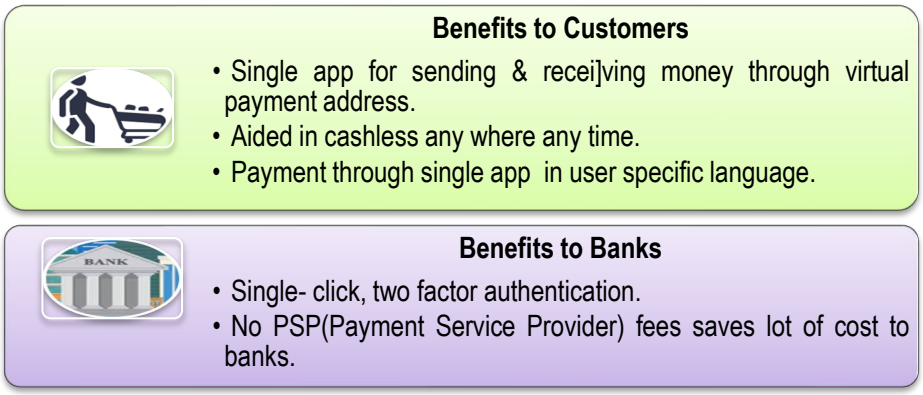


Fig. 13.5: Benefits of Bharat Interface for Money (BHIM)

G. RuPay: The term RuPay is coined from Rupee and Payment. This card system has become instrumental in driving the digitally led, cashless economy and enhancing financial enclosure while reducing the costs of cash, cheques, and manual transaction processing. It is adapted in India in 2012.

- It is accepted as a tool by retail outlets and e-commerce merchants.
- This card can be used to withdraw cash from ATMs network in India and at Point of Sale (PoS) at the merchant's need.
- It also supports reversal of transaction in case where the transaction is disputed within an applicable banking time frame.
- Transactions on a RuPay card can be made null and void by the merchant before the payment transaction is completed.
- The user can easily add money to the card to enable its usage for a wide range of transactions.
- Users can easily view debit, prepaid or balance amount as the card automatically updates the balance after each transaction.

Illustration

Mr. Amit decided to buy the latest mobile phone. He visited the local mobile store and purchased a mobile phone worth ₹ 20.00. After the purchase he handed over his RuPay card to the shopkeeper who inserted his card in a Point-of-Sale (PoS) terminal and entered the amount to be paid. Mr. Amit checked the amount and securely entered his card PIN and clicked the submit button on the terminal. The PoS terminal prints out a mini receipt and the merchant hands over a copy to Mr. Amit mentioning the bill amount.

H. **e-RUPI:** Recently, the Government of India has launched a new mode of cashless and contactless digital payment named e-RUPI based on UPI systems to ensure seamless transfer of benefits to the citizens in a "leak-proof" manner.

- It is an e-voucher, which will be delivered to beneficiaries in the form of a QR code and SMS-string-based voucher through which funds will be directly transferred to their bank account.
- These vouchers are person- and purpose-specific, meaning if they are released by the government for the purpose of vaccination, for instance, then they can be redeemed only for that.
- This contactless e-RUPI is easy, safe, and secure as it keeps the details of the beneficiaries completely confidential.
- The entire transaction process through this voucher is relatively faster and at the same time reliable, as the required amount is already stored in the voucher.
- Any government agency and corporation can generate e-RUPI vouchers via their partner banks.

Refer Fig. 13.6 highlights major benefits of e-RUPI.

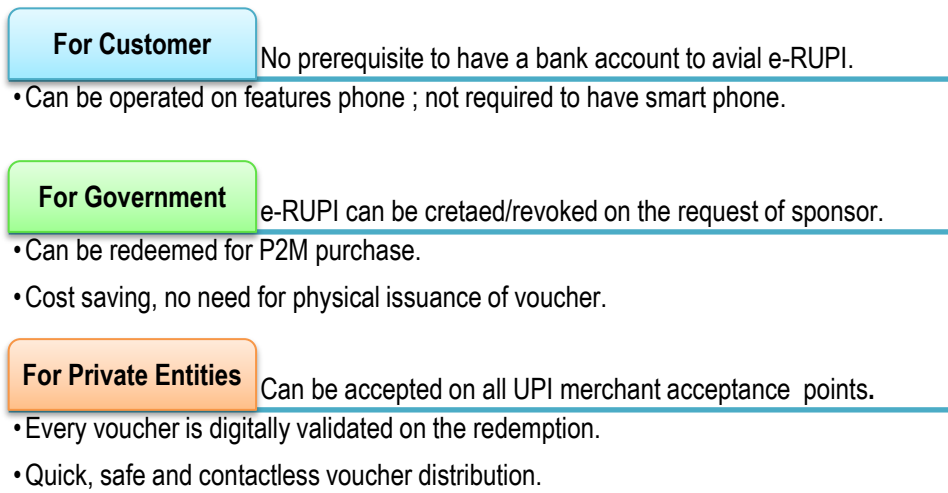


Fig. 13.6: Benefits of e-RUPI

I. **Cards:** Cards are provided by banks to their account holders. These have been the most used digital payment modes till now. These cards are the mode of digital payment the enables the users to make transactions without spending cash. Plastic money refers to the payments made via debit or credit card and is versatile and convenient. The invention of plastic money was made possible by technology. Various types of cards are as follows:

- **Credit Cards:** A small plastic card issued by a bank, or issuer etc., allowing the holder to purchase goods or services on credit. It contains a unique number linked with an account. It also has a magnetic strip embedded in it which is used to read credit card via card readers. In this mode of payment, the buyer's cash flow is not immediately impacted. Users of the card make payment to the card issuer at the end of billing cycle. Credit Card issuer charge customers per transactions/fixed amount as transaction fees.
- **Debits Cards:** Debit cards are also small plastic cards with a unique number linked with a bank account number. It is required to have a bank account before getting a debit card from the bank. It enables the cardholder to pay for his/her purchases directly through his/her account. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should be sufficient balance in bank account for the transaction to get completed, whereas in case of credit card, there is no such compulsion.
- **Smart Cards:** Smart cards are prepaid cards similar to credit cards and debit cards in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store customer's personal information such as financial facts, private encryption keys, credit card information, account information, and so on. Smart cards combine the advantages of both debit card and credit card and are available to anyone, regardless of credit ratings or income of applicant of smart card. Moreover, these are not linked to any bank account. For this reason, smart card holders are not mandated to have a bank account. It is also used to store money which is reduced as per usage. Example - Visa Cash.

  The smart card holder has to load money onto the card by paying cash or through transfer from his/her bank account. After loading the money onto the card, the cardholder can use the card to spend money up to the limit of loaded amount in the same way as using a credit or debit card. Once the loaded amount is spent, the cardholder may reload money onto the card.

13.3 E-BUSINESSES ASSOCIATED RISKS AND THEIR CONTROLS

E-Commerce: "Sale/Purchase of goods/services through electronic mode is e-commerce." This could include the use of technology in the form of Computers, Desktops, Mobile Applications, etc. The greatest change due to technological innovations in last five years has been the way users perform their daily chores/activity of life. E-Commerce and its related technologies are unquestionably the current leading-edge business and finance delivery systems.

The explosion in the application of technologies and the delivery of these technologies into the hands of consumers has made the vision, the dream, the fantasy of conducting business electronically, anywhere in the global community, a reality.

E-Commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers, and its business partners. In e-commerce, the buyers and sellers interact electronically using telecommunication networks rather than through physical contact or exchange. It is a new way of conducting, managing, and executing business transactions using computer and telecommunication networks.

E-commerce is not merely a concept; it has evolved into a formidable market force. With the increasing number of organizations launching Internet and World Wide Web (WWW) home pages and intranets to share company/product information and broaden their customer base, numerous yet unnamed companies are now beginning to explore this alternative. These companies are realizing that business via the Internet is inevitable that they will not be able to ignore. The lure of reaching additional customers, expanding market shares, providing value added services, advancing technological presence, and increasing corporate profits is just too valuable to disregard, and will eventually attract companies to electronic commerce like moths to a flame.

Benefits of e-Business

E-business benefits individuals, businesses, government, and society at large. The major benefits from e-business are as follows:

A. Benefits to Customer/Individual/User

- **Convenience:** Every product/service is easily available at the tip of an individual's fingertips on internet.

- **Time saving:** Some products such as e-books, recharge of mobile can be delivered online through internet, which reduces the time. Buyers must wait to begin enjoying their purchases.
- **Various options for comparison:** Customers have several options that are not only easy to compare but are also offered by different players in the market. This wide array of choices enables buyers to consider numerous products and services from a diverse range of sellers.
- **Easy to find reviews:** There are often reviews about a particular site or product from previous customers which provide valuable feedback.
- **Coupon and Deals:** There are discount coupons and reward points available for customers to encourage online transaction.
- **Anytime Access:** The customers can evaluate the products 24 hours a day, each day as per their convenience.

B. Benefits to Business/Seller

- **Increased Customer Base:** The exponential growth in online users has resulted in the creation of not only new customers but also the retention of existing ones. E-commerce allows businesses to offer their products and services to almost everyone worldwide with an internet-enabled device. It enables reaching narrow market segments that may be widely scattered geographically.
- **Recurring payments made easy:** Each business has several operations that are homogeneous in nature. This brings in uniformity of scaled operations.
- **Instant Transaction:** The interaction with the system occurs in real time, enabling customers to respond quickly. This capability has facilitated the successful execution of numerous deals.
- **Provides a dynamic market:** With multiple players in the market, a dynamic environment is created, fostering improved quality and business growth.
- **Reduction in:**
  - ❖ costs to buyers from increased competition in procurement as more suppliers can compete in an electronically open marketplace.
  - ❖ costs to suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.

- ❖ overhead costs through uniformity, automation, and large-scale integration of management processes.
- ❖ advertising costs.

- **Efficiency improvement due to:**
  - ❖ reduction in time to complete business transactions, particularly from delivery to payment.
  - ❖ reduction in errors, time for information processing by eliminating requirements for re-entering data.
  - ❖ reduction in inventories and reduction of risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.
- **Creation of new markets:** This is done through the ability to reach potential customers easily and at low cost.
- **Easier entry into new markets:** This is especially into geographically remote markets for enterprises regardless of size and location.
- **Low barriers to entry**: Homepages provide equal footing for small organizations alongside large international firms. Both small and large organizations have an equal opportunity to establish a presence on the World Wide Web and conduct business online.
- **Better quality of goods:** Standardized specifications and competition have increased and improved the variety of goods through expanded markets and the ability to produce customized goods.
- **Elimination of Time Delays:** Faster time to market as business processes are linked, thus enabling seamless processing, and eliminating time delays.

C. Benefits to Government

- **Instrument to fight corruption:** In line with Government's vision, e-commerce provides pivotal hand to fight corruption. The Information Technology Act, 2000 provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures.
- **Reduction in use of ecologically damaging materials:** There has been reduction in the use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects.

Clearly, the benefits of corporate-wide implementation of e-business are many, and this list is by no means complete. With the benefits, however, also come the risks. An organization should be cautious not to leap blindly into e-business, but rather first develop an e-business strategy, and then organize a corporate-wide team to implement that strategy.

Disadvantages of e-Business

Following are the disadvantages of e-business:

- **Internet Connection:** Internet connectivity is a pre-requisite to perform online transactions. Internet connectivity may not be available in rural or remote areas. Many people may not have Internet connectivity due to which they may not be able to do online transactions.
- **High start-up costs:** The various components of costs involved with e-commerce are due to the following factors:
- **Connection:** Connection costs to the Internet (i.e., direct link or connection provider).
- **Hardware/software:** This includes the cost of sophisticated computers, modems, routers, etc.
- **Set up:** This includes employee work hours involved in the processes of setting up the systems.
- **Maintenance:** This includes the costs involved in training employees and maintenance of webpages.
- **Legal issues:** Legal issues are a significant impediment to conducting business on the Internet. It is almost uncertain to ascertain the legal issues that will start to pop up as business on the Internet progresses. Legal issues may also arise if customer-sensitive data falls into the hands of strangers. The legal environment in which e-commerce is conducted is full of unclear and conflicting laws.
- **Some business processes may never be suitable for e-commerce:** Items like perishable foods and high-cost items such as jewelry and antiques may prove challenging to inspect adequately from a remote location, regardless of future technological advancements.
- **Cultural impediments to e-business:** Some customers are still somewhat fearful of sending their credit card numbers over the Internet. Moreover, many customers are simply resistant to change and are uncomfortable viewing merchandise on a computer screen rather than in person.
- **Security Concerns:** One of the primary drawbacks of conducting online business is the issue of security. Technical challenges, including concerns related to the security and reliability of

networks and the internet, are significant factors in online transactions. The fear of compromised safety and security of personal information persists due to the prevalence of spyware and malware on the internet.

Risks and controls associated with e- business

Table 13.1 details the various risks vis-a-vis the controls to mitigate the risks that are associated with e-business.

Table 13.1: Risks and their controls in e-business

Aspects	Risks	Controls
Data privacy and Online Security Risks	Hackers and Malicious actors can enter the system through phishing, malware, or ransomware.	• There is requirement to establish strong data privacy and online security policy, training to staff and incentivize the employees to make them learn about data security.
Unauthorized Access	Unauthorized access can lead to significant amount of data loss. It may also lead to data security breach.	• Restricted access should be given to employees. • Two factor authentication should be used for login procedure. • Regular updation of password to mitigate the unauthorized access.
Exploitation of Vulnerabilities	Vulnerabilities such as unpatched software, legacy system, etc. may benefit malicious actors to attack the system.	• Regular updation of system is required. • Remove and uninstall incompatible plugins. Use firewall and anti-virus software. • Perform periodic security audit.
Human Error	Human mistake can cause loss of data.	• Implement data backup and data recovery solution.
Platform downtime	Lengthy downtime to update the server can impact the reputation and productivity of e-business.	• Efficient SaaS providers are required to be chosen. • Less dependencies on third party for updation of software.
Non-Compliance	The hefty penalties would be imposed in case of no compliance with regulatory framework.	• It is required to understand all applicable data privacy laws. • Regular updation of website can prevent the financial loss due to noncompliance of regulatory framework.
Loss due to Disaster	Disaster may cause loss and ruin the e-business.	• Design and implementation of proper Disaster Recovery Plan that may cover every possible scenario.

13.4 EMERGING TECHNOLOGIES

I Internet of Things (IoT)

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Embedded with electronics, Internet connectivity, and other forms of hardware (such as sensors), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled. The goal of this interconnection is to make all these devices communicate with each other and therefore, be more intelligent and independent. One of the characteristics of IoT devices is that they are able to produce large amounts of data. This data can be particularly used in applications such as Artificial Intelligence and Machine Learning.

IoT is an integrated part of the future that can be defined as dynamic and global. The main objective of IoT is to create an intelligent and smart world where physical, virtual, and digital are joining to create an intelligent and smart environment that provide more intelligence to the energy, healthcare, transport, cities, manufacturing, building and many other areas of our routine life. IoT is used to connect devices or objects to access information anytime, anywhere and anyone. Wireless sensors interconnect the devices and provide the relevant information to the user whatever is the location of user.

Everything from toothbrush to washing machine, entrance gate, whatever is in the communication range is today's internet and tomorrow's Internet of Things. (IoT) systems and applications provide security, privacy, safety, integrity, trust, anonymity, and these are bound to ethics constraints. This can be achieved by having the objects connected with sensing, identification, and positing technologies.

IoT is generally associated with sensors and used to collect the data from sensing devices attached to various objects. The analysis of this collected data is done to provide useful information to the users. However, IoT is not only used for collection of data and making analysis, but also used in financial and accounting industry.

A. Applications of IoT in Finance and Accounting (Refer Fig. 13.7)

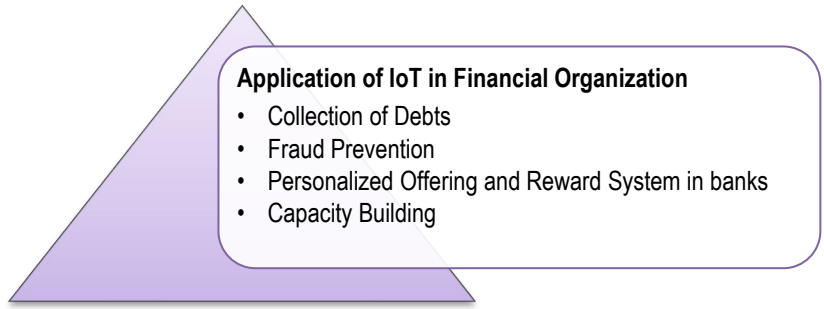


Fig. 13.7: Use of IoT in Financial Industry

- **Collection of Debts:** This is a very crucial task that requires considerable efforts and overhead costs to the lending financial institution. Using IoT sensors and network operations and supply chain activities of debtors, businesses can be monitored that may help Financial Investigators (FIs) to determine their readiness to pay without involvement of overhead cost and the cost associated with cancellation and failure of cheques. IoT network of ATM and various points of sales devices can allow to assess the borrower's expenditure and income, their ability and intent to repay and expenditure by defaulters can be curbed until repayment.

- **Fraud Prevention:** This is one of the major worries for the financial organization. IoT is the game changer in this area. IoT enabled security systems at various Point of Sale (PoS) especially at ATM can prevent the misuse of debit/credit cards. The financial organizations which constantly invest the money or support the startups, small businesses with money, generally require to seek the various methods to stop the misuse of their money. AI and IoT based systems allow financial organizations to control the misuse of their money. HSBC bank has already successfully implemented an AI based anti-fraud system.

- **Personalized Offering and Reward system in banks**: With the promotion of cashless activities, customers prefer to pay with debit/ credit card/internet banking/ paytm etc. Banks generally give incentives or reward points to their customers who make payment using different modes of e-payments. These points can be redeemed in specific ways. Sometimes these rewards are not alluring to customers as either process of redemption is tough, or the customers may not be able to get sufficient points required for redemption. IoT along with Artificial Intelligence are used to attract the customers by rewarding relevant redeemable options based on shopping activity or demographics. For example - a customer who spends most on food would be given

points redeemable to food outlets and the customer who spends more on clothing would give points or discounts redeemable on apparel.

- **Capacity building:** IoT enabled systems monitor and track the number of customers visit per day and can keep track on average queue time to measure the optimal number of employees or personnel to take care of customers. The decision regarding the new branch can be made easier by using distribution data from the customer or geographical location. Similarly in banks the number of ATMs present and the requirement to open new ATM centers can be easily monitored at any time.

B. Changes brought by IoT in Finance and Accounting

IoT with an innovative redesign, can bring change in financial services. Interact IoT, the first ever IoT based financial service platform helps users in saving money by connecting their bank accounts/cards to IoT enabled objects. Benefits can also be exploited by combining the interconnectivity of IoT with blockchain for a reliable and secure network.

- **Product Planning & Management:** The data is collected from various like mobile apps, banks and other financial organization can launch better and more targeted service offerings. It provides answers to following questions using data about the past service offerings and the reaction of customers for the same:
  - ❖ What services and products to launch?
  - ❖ Who will be the key targets?
  - ❖ When is the right time to launch the products?
- **Tailored Marketing:** Customers across the industries are demanding personalized solutions for their varying needs and Banking Financial Services and Insurance (BFSI) is no different. To tailor a financial solution to a client, information is needed about his present economic condition, buying behaviors & individual needs. IoT has made it possible for banks to keep a track of all consumer activities and present a solution specific to the needs and desires of the client.
- **Proactive Service:** IoT in financial industries can help to control service faults and upcoming products changes. If there is an underlying concern about a product then it will come to notice quite easily, and steps can be taken to handle the issue before it becomes too serious. Along with this, a record of the past actions of the customer can help service representatives provide better solutions.
- **Other changes bought by IoT in financial services** Wearable technologies of IoT bought another big change in financial services. Due to its popularity and easy

availability, wearables have become a primary target for such service providing organizations across the world. For example- smart watch.

Along with wearables, remote devices like Amazon Alexa are also a focus area where innovation in banking is necessary. Basic banking like balance check and transaction history are some must haves in every wearable and remote assistant device.

C. Challenges in IoT Implementation

The Fig. 13.8 represents the challenges in IoT implementation:

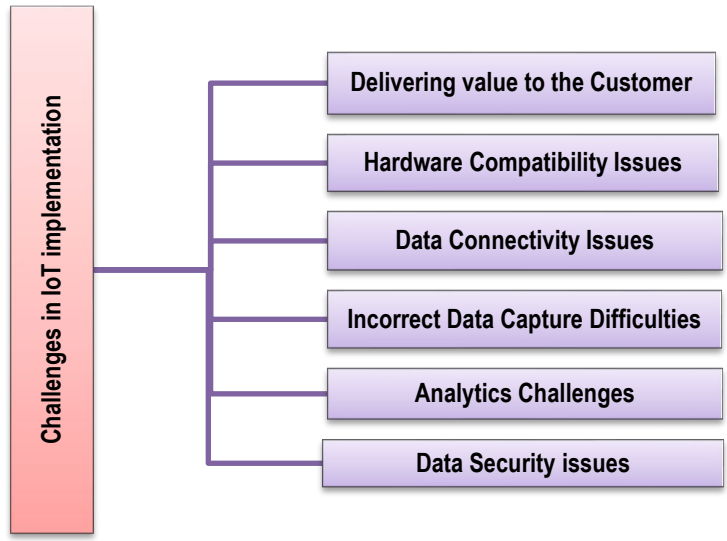


Fig. 13.8: Challenges in IOT implementation in financial industry

- **Delivering Value to the customer:** The success of an IoT implementation depends on the clear definition of the problem statement. However, this is the area missed by most IoT service providers. It is necessary to know how these solutions can impact efficiency, customer satisfaction and productivity in the long run. Therefore, it is important to figure out the key performance indicators to measure and improve through an IoT solution.
- **Hardware Compatibility Issues**: Data is captured through various sensors connected, IoT gateways collect & transmit data to the cloud. When existing legacy machines do not have the required sensors, the IoT implementation becomes a challenge. Adding external sensors to the machines becomes a challenging task.
- **Data Connectivity Issues:** This is the most concerning challenge in an IoT implementation. Most IoT devices available are compatible with GPRS and Wi-Fi, but

few devices depend on sensors, and telemetry systems to generate data. So, there need is for a suitable edge layer that translates transport and data format protocols to send data to the IoT platform.

- **Incorrect Data Capture Difficulties:** Due to some unpleasant incident or the inability of the software to handle certain anomalies, incorrect data may get recorded. This results in inaccurate analytics that would not be useful in taking better decisions.
- **Data Security issues:** The various attacks like ransomware attacks made the organizations more skeptical about data security. Data breaches and the stealing of intellectual properties have been increased.

II. Quantum Computing

The study of quantum computing is basically focused on the development of computer-based technologies based on the principles of quantum theory. Quantum theory explains the nature and behavior of energy and matter at the quantum level.

Every computer works on bits (0 and 1), and these bits represent the **ON** and **OFF** position (Fig. 13.9). The various ways to enter the data are in the form of program, website, app or photograph. User enters the data in his own language, whereas the computer through various software converts it to in the language of 0 and 1 to the input understandable to system. Through these bits, the computer understands the program and data sent to it as input. Every program, website, app, photograph etc. is made up of millions of bits which are the combination of 0 and 1. It can be at one position at a time.

The quantum computer uses quantum bits or Qubits. Qubits can be in a quantum superposition which means they can be in on and off position at the same time or between the two (Fig. 13.10). The qubits can also be inseparably linked together. The result is that, where there are a large number of possible combinations, quantum computers can consider them simultaneously. This is what makes quantum computing device so powerful that it could do in four minutes what it would take a traditional supercomputer 10,000 years to accomplish.

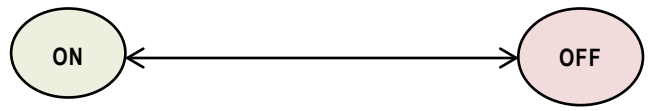


Fig. 13.9: Bits (can be at ON or OFF position at a time)

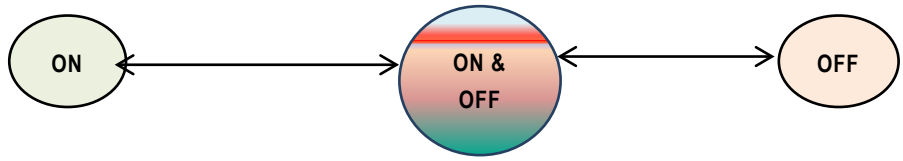


Fig. 13.10: Quantum Bits

Quantum computers can solve various types of problems in a faster and more efficient manner than traditional computing.

A. Advantages of Quantum computing in Financial Organization

Many problems in the financial sector can be expressed as optimization problems. Banks and financial institutions are the most benefitted sectors and accessible sectors that quantum computing can bring. These organizations have complex probability calculations for various financial transactions like pricing securities, interest calculation, portfolio management, etc. Accuracy and integrity of the data is very much required for security purposes. However, due to their complexity, such activities can be extremely time-consuming.

Unlike traditional computers that use binary bit technology (1 ON, 0 OFF), quantum technology uses qubits that allow them to assume both the on-off states and interact and influence each other regardless of medium or distance between them. Now many companies like IBM, Google, and Microsoft are developing general purpose quantum processors.

Quantum finance is a newly developed interdisciplinary field that serves as a gateway to financial technology, addressing fundamental challenges in finance. The following areas highlight significant improvements and opportunities that quantum computing has brought to banks and financial industries.

- **Targeting and Prediction Modeling:** Financial organizations such as banks, brokerage firms, Insurance companies, portfolio management companies, etc. need to have analytical models which help to overcome the struggle in managing the target and demand of their customers. It should encourage their ability to target what products their customers require in almost real-time. The issue with current customer targeting and prediction modeling can be the inaccurate fraud detection systems that often provide false positives, thus delaying the onboarding of new customers. In such cases, Quantum computing acts as a game changer for target and prediction modeling. The capabilities of Quantum computing machines allow us to meet the challenges of complex data structures and make predictions that are simply not possible with present computers.

- **Trading Optimization:** Trading activity is one of the complex activities in financial organization that requires regulatory elements, such as great transparency and proper validation processes. The key concern for any investment manager is incorporating real-life limitations and issues into portfolio optimization, and market volatility. Rebalancing portfolios and simulating numerous scenarios and investment options are fast-changing market movements which are dependent on transaction costs and computational limitations. Quantum computing helps the investment managers to improve portfolio diversification. They can also rebalance portfolio investment in a better way as per the rapidly changing market conditions. Simultaneously, it also allows us to meet investor goals with more cost-effective and streamlined processes for trading settlement.
- **Risk Profiling:** In general, Banks and financial organization are highly on risk because these are under high pressure to meet the terms with regulatory requirements. It is difficult to correctly manage the risk costs on trades because risk management, derivatives pricing and liquidity management are complex and difficult calculations to perform. It is expected going forward that amendments to regulations, directives and standards will continue to add to compliance costs. The faster data-processing capabilities of quantum computing speeds up risk scenario simulations that are more accurate in case of testing potential outcomes.

B. Threats that financial organizations face from Quantum Computing

The increased popularity of digital banking has made financial organizations the prime targets for cyber-attacks. Most of the applications running on the Internet today are protected by various sets of protocols. These protocols are reliable in protecting data in the most powerful traditional computers. However, these may not be strong enough to stand up to a future quantum computer: it is expected that quantum computers could easily break most of these protocols and leave data unprotected.

This is a significant concern for many financial organizations. To safeguard valuable financial data, these organizations must ensure that their systems adhere to the highest standards of security, trustworthiness, reliability, and interoperability. Currently, every financial institution relies on various cryptographic algorithms to secure software and hardware used for authentication, encryption, and decryption of payments. However, all these measures could be compromised by a single powerful quantum computer.

III. RegTech

Technology is changing the finance world at a high rate, simultaneously it is raising new risks. Financial regulators must develop new approaches to regulation, using technology, and benefits of innovation for economic development with financial stability and consumer protection.

Technology plays an ever-increasing role in regulating itself, particularly financial regulation. The intensive use of technology in finance puts pressure on the regulators to move from regulations designed to control human behavior to regulations that seek to supervise automated processes. This generates the need for RegTech. This is the contraction of terms "Regulatory" and "Technology" and describes the use of Information Technology (IT), in the context of regulation, monitoring, reporting and compliance in financial organizations.

RegTech also known as Regulatory Technologies, is one of the emerging technologies that deals in the management of regulatory processes through technology within financial sector. This is a vibrant dimension of FinTech. The term "RegTech" was coined by the United Kingdom's Financial Conduct Authority (FCA) as, **"RegTech is any range of applications of FinTech for regulatory and compliance requirements and reporting by regulated financial institutions"**.

This technology is used for the purpose of regulatory monitoring, reporting and compliance for the betterment of financial organizations. RegTech with the help of technological innovation has enabled the companies to find out solutions that address the regulatory compliance issues. RegTech is mainly focused on the digitalization of regulatory reporting and compliances which facilitates enormous cost savings for not only the financial sector but for the regulators as well.

RegTech delivers technological solutions that are involved in financial activities to ensure regulatory compliances. This technology is used in either ways ie. How the new technology helps industry comply with regulations or as "RegTech for regulators," which represents the use of new technology by regulatory bodies themselves.

RegTech can be applicable to any industry, however, the technology has evolved in the financial arena, being the most pervasively and complexly regulated industry in the world. This technology escalates the development of new financial infrastructure, inclusive of digital identification systems and frameworks for payments and other transactions. To meet the compliance obligations, the financial organizations gain the potential for substantial cost savings using RegTech. Similarly, it provides the opportunity for regulators to perform their functions more effectively. The combination of FinTech and RegTech offers the potential to frame the development of a very different financial system from what exists today.

A. Advantages of RegTech in financial organization

Innovation in technology is increasing on a daily basis, spreading across geographical clusters, which makes monitoring new technologies challenging. The rapid growth of FinTech and RegTech underscores the crucial role of technology and innovation in development and sustainability. The self-learning nature of these new technologies is swiftly transforming the scope and potential for automated regulation.

Technology in addition to its impact on finance, RegTech is also increasing its impact on regulations including by industry and by regulators themselves, increasingly using technology to enhance performance of their own mandates.

Further, market participants are beginning to consider how technology can be used to redesign financial systems. This is the new step that will hold new smart and digitized regulatory systems and a new approach to regulation that appeals to all available technology, in a sequenced structured manner, to achieve the balancing act required of regulators. Both finance and financial regulation have always presented intractable problems that have persisted, despite the best efforts of policymakers, for decades and sometimes even centuries. The Policymakers of financial organization generally use regulation to pursue following basic goals:

- **Consumer Protection and Financial Inclusion**

  Among various organizations around the world, global financial inclusion can never be achieved without RegTech. Thousands of people are entering the financial services marketplace be it to purchase something or to invest in their future. The speed and scale of this shift has overpowered the traditional regulatory infrastructure. This escalating fast speed can be controlled by using RegTech.

  RegTech work has opened financial inclusion in other ways. The potential for Big data and Machine Learning to fine tune assessment of customer risk profiles in both credit decisioning and in KYC screening, thus giving more consumers access to the financial system and to loans. The financial organizations will not be able to move to widespread adoption of such techniques unless regulators become comfortable with these techniques. To do so, they will have to deploy RegTech that can evaluate whether these systems are reliable and fair. Now, new solutions are available with automated analysis of lending patterns for compliance with fair lending laws with an aim to enhance financial inclusion. The substantial potential of RegTech to reduce compliance costs, and risks, will expand financial inclusion by making services more affordable and widely available, and by helping to foster more Fintech innovation that generates other consumer benefits.

- **Credit discrimination and UDAAP**

There is a clear risk that new technologies may be intensify-bias and use unfair practices in the financial system, intentionally, unintentionally, or both. However, when regulators are empowered with massively more data and the techniques of AI, also has the opposite potential and becomes easier to catch the patterns of bias and unfair treatment that currently go undetected. Federal law bans lending discrimination based on factors like race, gender, and religion. It also prohibits financial organizations from engaging in Unfair, Deceptive or Abusive, Acts and Practices (UDAAP).

RegTech can bring to bear the power of more data and AI analytical tools on solving these challenges. It could help the regulators to detect and prove violations more easily. It might also enable them to issue clearer and concrete guidance, including more sophisticated standards on statistical modelling, to help organizations avoid discrimination and UDAAP noncompliance. That in turn could help in reducing regulatory risks and also better serving the customers.

New methodology could also help risk managers to identify possible problems early that may reduce scenarios in which undetected non-compliance accumulates over years and triggers large fines and reputation damage. This technology also helps new startups and tech companies to enter the world of financial sector establish high-quality compliance tools from the outset, rather than relying on less effective traditional methods.

- **Anti-Money Laundering (AML)**

One of the main objectives of RegTech is its usage in Anti-Money Laundering, or AML. The reasons that make the law enforcement agencies find key material and detect patterns of crime are that the data they receive today is low in value and contains too much unimportant information.

Many Government agencies and financial companies are working on bringing better technology into this regard. They are seeking to improve and ease customer identification through Know Your Customer, strengthen the monitoring machanisum of transactions for patterns of crime, and automate and ease investigation processes.

As financial companies are obligated to collect and track comprehensive information on financial transactions, there is an opportunity to combat illicit activities through RegTech. If AI identifies patterns matching crime typologies, it can alert authorities, triggering the necessary due process steps to permit the disclosure of complete data.

- **Synthetic identity fraud**

  Many anti-money laundering RegTech solutions are developed by the financial industry to identify fraud. One of the anti-fraud methods used in RegTech interest is the growing use of fake identities. These are created by combining real customer information with fake data in a series of steps that can fool normal detection systems but can often be caught by RegTech analysis and machine learning. The efforts of financial organizations taken on added urgency have shifted to functioning mostly online, where fraud rates are comparatively high.

- **Monitoring conduct risk and illegal practices**

  Certain regulatory areas are overseen to determine whether organizations and individuals are directing themselves within purview of law. In the securities market, both regulators and financial organizations are gradually using AI-based technology to run market surveillance aimed at detecting signs of financial misconduct, such as insider trading. The combination of big data and other algorithmic techniques seek out patterns such as unusual behavior by brokers.

- **Avoid Phoenixing**

  One of the major challenges in regulatory licensing work is the difficulty of tracking companies that have been barred from operating in the financial system. Governments shut down illegal entities, imposing fines and sometimes banning their principals from future financial activities. A prolonged problem can be when many of these players may rise again, phoenix-like, doing business under a new name and resuming illegal activities until caught again. They tend to inhabit the margins of the industry, in shadowy spaces that are difficult for regulators to see into. RegTech has the potential to solve three big problems at once.

- It can address this acceleration problem, which, if unresolved, will pose an existential threat to the system.

- It may improve the existing performance of the regulatory system, fixing problems that were beyond the reach of older technologies.

- It can drive down costs to both organization and government, with all the subsidiary benefits that reduced expense would generate in market efficiency, competitiveness, innovation, improved affordability of services, and widened access.

IV. Mobile Computing

Mobile computing is described as the ability to use computing capability without a pre-defined location and connection to a network to publish and subscribe to information. It is the interaction between humans and computers by the mean of which computer is expected to be transported during normal usage. This is the generic term that describes the ability to use the technology to connect wirelessly to use centrally located information and application software through the application of small, portable, and wireless computing devices.

This technology enables the mobile worker to create, access, process, store and communicate information without being constrained to a single location. Mobile computing establishes interaction among various personnel of organization which was previously disconnected. This technology creates an information management platform, which is free from spatial and temporal constraints. This freedom allows the users to access and process the desired information from anywhere. It is independent of the stage of user whether static or mobile. Users may use cell phones, laptops, palmtops etc. as mobile devices for mobile computing. Mobile connectivity between two devices can exist if these devices are continuously connected through wireless channels. Mobile computing involves mobile hardware, mobile software, and mobile communication. A primitive scenario of mobile computing in practice is shown in Fig. 13.11.

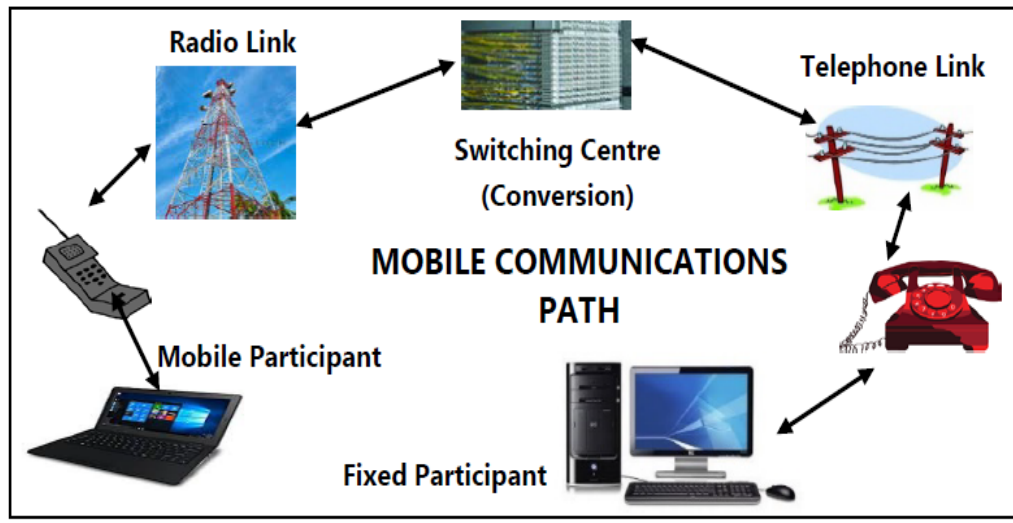


Fig. 13.11: Mobile Computing

A. Components of Mobile Computing

The key components of Mobile Computing are as follows:

- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies. The type and availability of communication medium significantly impacts the type of mobile computing application that can be created. There are many communications technologies available that make mobile devices to communicate. Some of the most common of these technologies are Wireless Local Area Networks (WLANs), Satellite, Cellular Digital Packet Data (CDPD), Personal Communications Systems (PCS), Global System for Mobile communications (GSM), Internet etc.
- **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and 4Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers, and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network. The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability, and durability of the device.
- **Mobile Software:** It is an actual program that runs on mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operate. Mobile applications popularly called Apps are being developed by organizations for use by customers, but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

The most common operating system used on mobile computers includes Android, iOS etc. Each operating system/environment has some form of Integrated Development Environment (IDE) for application development. Most of the operating environments provide more than one development environment option for custom application development.

B. Benefit of Mobile Computing

This emerging technology offers a quick and easy way to increase efficiency, productivity and profitability while gaining better control of the operations. The power and data storage capacity of today's handheld PCs and Personal Digital Assistants (PDAs) has made mobile computing a practical reality with low-cost and ease to use. Today's world mobile computing is serving its benefits in various fields. Few of them are discussed below:

- Mobile computing has empowered users to work from any location as long as they are connected to a network. Employees can access the organization's database from remote locations, allowing them to work without being confined to a fixed position. This flexibility in working, such as enabling remote work or work while traveling, enhances overall work flexibility.
- Mobile computing has reduced the travelling time from different locations or to the office and back. Employees of a company can now access all the important documents and files over a secure channel or portal and work as if they were on their computer.
- Employees' productivity has been enhanced by the fact that a worker can simply work efficiently and effectively from whichever location they see comfortable and suitable. Users can work in comfortable environments. It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- Mobile computing enables the organization to improve the services offered to its customers. For example, by using a wireless payment terminal the customers in a restaurant can pay for their meal without leaving their table.
- Increased information flow enables in improving management effectiveness that integrate the technology into their information systems. It enables the computing power and information system to be structured around the optimum workflow of a mobile worker, instead of altering the mobile worker's workflow to meet the optimum configuration for computing.
- Mobile computing facilitates excellent communication and information accessibility. This technology provides a wide range of options that can be combined together according to the needs of each individual mobile computing application. This results in improved information flow both to and from the central fixed information system in a quick and efficient manner. The ability allows employees to access the information they need to complete the job.

- It provides the 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 may improve efficiency in saving time, reducing waste, reducing cycle times, reducing rework, enabling business process reengineering, improving accuracy, decreasing time spent on customer complaints, and reducing unnecessary travel.
- Whenever there are emergency services involved it becomes necessary to receive information. Information regarding the address, type and other details of an incident can be dispatched quickly, through Cellular Digital Packet Data (CDPD) system using mobile computers, to one or several appropriate mobile units, which are in the vicinity of the incident.
- This technology can improvise the transaction process and relieve congestion at the POS terminals. when customers use their credit/debit cards for any type of transactions, the intercommunication is required between the bank central computer and the POS terminal, to make effective verification of the card usage, it may take place quickly and securely over cellular channels using a mobile computer unit.
- Nowadays, Defense counsels can take their mobile devices to court. During the hearing in the court, they may use mobile computing to get direct, real-time access to on-line legal database services, where they can gather information on the case and related precedents.
- Using mobile computing, the operations of an entire transportation fleet can be managed from a central location. The central office may control the location, status, and condition of all vehicles, and operators have two-way communication with the operations center.
- Using this information, vehicles can be optimally dispatched to maximize efficiency as measured by time, fuel consumption, and delivery priority. The mobile computers enable significant performance improvements, achieved simultaneously with operational cost reductions.
- Mobile computing along with Global Positioning System (GPS) and Geographical Information System (GIS) data makes significant improvements in the operational efficiency of various dispatch related operations.

- General businesses are immensely benefitted from mobile computing. E-mail, Spreadsheets, word processing, presentations, and many more applications can be used through mobile computing by the businessmen anytime anywhere.

SUMMARY

This chapter highlights the digital payment ecosystem. This chapter has given an overview of various payment methods that are used in bank transfers, mobile money, QR codes, etc. The digital payment methods are used in buying anything, anywhere, anytime. It makes the payment hassle free and does not require users to carry cash. This chapter has provided a brief overview on UPI Apps, USSD, APES, IMPS, BHIM, RuPay, e-RUPI, cards, etc. This chapter also discussed various emerging technologies such as IoT, Quantum Computing, RegTech, and Mobile computing etc. These technologies are automating human tasks and creating options to carry those tasks which could not have been executed previously.

TEST YOUR KNOWLEDGE

Multiple Choice Questions (MCQs)

1. Mr. X is buying clothes for his kids at Royal's Showroom. He makes payment using BHIM (Bharat Interface for Money) App which is an example of _____.

   (a) UPI App

   (b) Mobile Hardware

   (c) Digital Library

   (d) Mobile Wallet

2. An IoT network is a collection of _____ devices.

   (a) Interconnected

   (b) Machine to Machine

   (c) Network to Network

   (d) Sensor

3. Which of the following statements are true, while using credit card……

i. No immediate payment is required

ii. linked with bank account of user

iii. Cash flow is immediately impacted

iv. Payment can be made on end of month

Choose the correct option from following

(a) i, ii

(b) iii, iv

(c) i, ii, iii

(d) i,iii,iv

4. Which of the following is not the disadvantages of e-business?

(a) High start-up costs

(b) Cultural impediments to e-business

(c) Low barrier to entry

(d) Security concern

5. Which of the following is not true about mobile computing?

(a) enables the organization to improve effectiveness of management.

(b) Improvise the transaction process

(c) Facilitate excellent communication and information accessibility

(d) Prevent the fraud transaction

ANSWERS/SOLUTIONS

1.	(a)	2.	(a)	3.	(a)	4.	(c)	5.	(d)

REFERENCES

BOOKS

1. Ron Weber, 'Information Systems Control and Audit', Pearson Education, Third impression, 2009.
2. Angel R Otero, 'Information Technology Control and Audit', CRC Press, Fifth Edition 2018.
3. Jake Kouns and Daniel Minoli, 'Information Technology Risk Management', Wiley Publication, 2010.
4. Alan Calder and Steve Watkins,' IT Governance An international guide to data security and ISO27001/ ISO27002', KoganPage, Sixth edition, 2015.
5. K Chandrasekaran, Essentials of Cloud Computing, CRC Press.
6. Thomas F. Wallace and Michael H. Kremzar, 'ERP: Making It Happen: The Implementers' Guide to Success with Enterprise Resource Planning'.
7. Sandra Senft and Frederick Gallegos, 'Information Technology Control and Audit', CRC Press, Third edition.
8. Miklos A. Vasarhelyi, 'Artificial Intelligence in Accounting and Auditing: Towards New Paradigms,Markus Wiener Publisher, Volume 4.
9. LinekeSneller RC,'A Guide to ERP Benefits, Implementation and Trends'.
10. Ellen Monk and Bret Wagner,'Concepts in Enterprise Resource Planning'.
11. Yusufali F. Musaji,'Integrated Auditing of ERP Systems'.
12. Castells, Manuel. 'The Rise of the Network Society.' 2nd ed. Cambridge, MA: Blackwell Publishers, 2000.
13. Valacich, Joseph, and Christoph Schneider, 'Information Systems Today: Managing in the Digital World' NJ: Prentice-Hall, Fourth edition.

14. Chui, Michael, Markus Loffler, and Roger Roberts, 'The Internet of Things.' McKinsey Quarterly, March 2010.

15. Gallagher, Sean, 'Born to Be Breached: The Worst Passwords Are Still the Most Common', Arstechnica, 2012.

16. McCallister, Erika, Tim Grance, and Karen Scarfone, 'Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)'.

17. Donal O'Mahoney, Michael Peirce, and Hitesh Tewari, 'Electronic Payment Systems for E-Commerce', Artech House

18. Roger S pressman,' Software engineering', Mcgraw Hill International, 2017

WEB RESOURCES

1. Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.

2. Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.), Supreme Court of India, November 13, 2019.

3. Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021.

4. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.

5. www.meity.com

6. www. cloudian.com

7. www.prsindia.org

8. www.cio.com

9. www.sebi.com

10. www.rbi.com

11. www.isaca.org

12. www.razorpay.com

13. www.cleartax.in

14. www. economictimes.indiatimes.com

15. www.freshworks.com

16. www.iso.org

17. www.coso.org

18. www.careerfoundry.com

19. www.investopedia.com