Preface

This PDF has been created as a summarized compilation of all the chapters covered in the course. Over the course of two days, I worked diligently to condense and highlight the key concepts from the module. My aim was to capture the most essential information that would aid in understanding the material and help with exam preparation.

I found this summary to be very useful in my own preparation and it contributed significantly to my success in clearing the SPOM set. However, since I compiled this document in a short time frame, there is a slight chance that some concepts might be missing or not covered in as much depth as in the original study material.

I recommend cross-referencing this summary with the official study material whenever needed to ensure you have a comprehensive understanding of the topics.

I hope this document proves helpful to you as it did for me. Best of luck with your studies!

- Mansi Bhoir

Important Concepts to cover

1. Types of risks
2. Types of controls
3. CAAT
4. IMPS
5. E-Rupi
6. Sections of IT Act 2000 and penalties for non compliances
7. COBIT
8. GEIT
9. GRC
10. Risk Management strategies
11. COSO
12. CIA Triad
13. Complete Chp 4, 5 & 12
14. System development methodologies
15. IT Audit tools
16. Data security tools
17. Data analysis tools
18. Cloud computing models

Chapter 1 Governance and Management of Digital Ecosystem

Introduction

- Enterprises aim to deliver value to stakeholders while operating within acceptable value and risk parameters.
- **Governance** refers to decision-making processes that steer organizations, ensuring accountability, structure, and resource optimization.

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.

Key Principles of Governance Framework

1. **Based on Conceptual Model**: Consistent and allows automation.
2. **Open and Flexible**: Adapts to new issues.
3. **Aligned to Major Standards**: Conforms with global regulations and frameworks.

Enterprise Governance

- Framework ensuring strategic direction, risk management, and responsible use of resources.
- **Dimensions**:
    1. **Corporate Governance**: Focuses on conformance, regulatory compliance, and shareholder value.

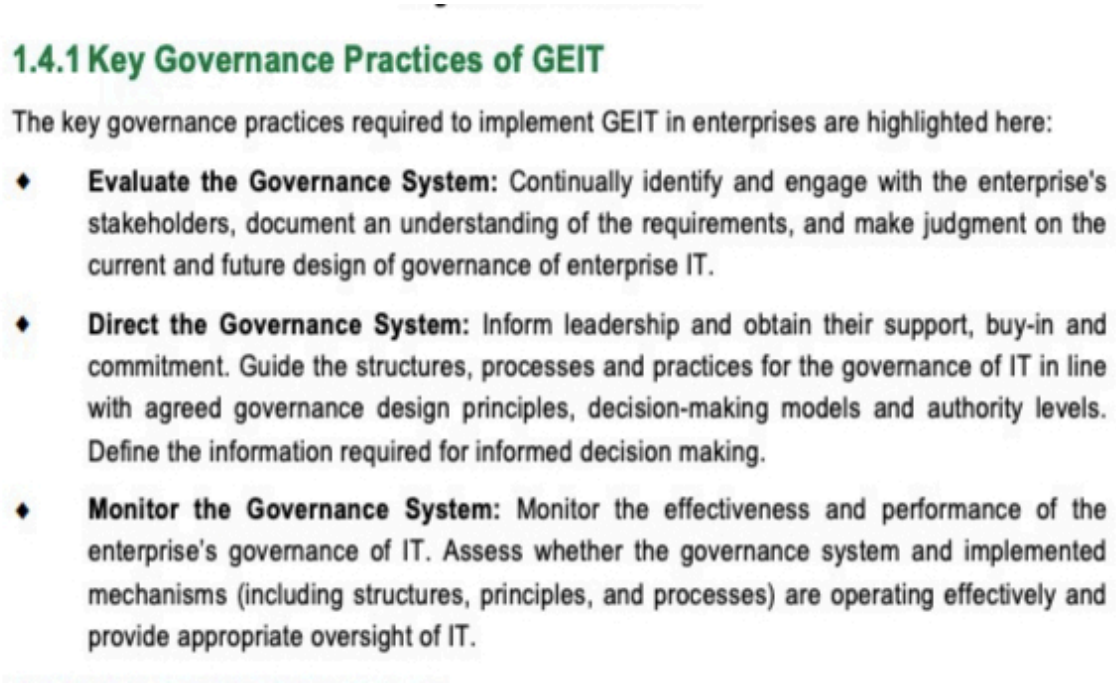
2. **Business Governance**: Proactive, strategy-focused, and emphasizes value creation.

IT Governance

- Aligns IT strategy with business goals.
- Objectives include increased value from IT, risk mitigation, and effective resource utilization.
- Key questions involve decision-making, monitoring, and exception handling.

Governance of Enterprise IT (GEIT)

- A subset of corporate governance focused on implementing IS controls.
- **Benefits**: Alignment with enterprise goals, transparent oversight, and compliance with regulations.



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.

Enterprise Governance of Information and Technology (EGIT)

EGIT emphasizes the importance of Information and Technology (I&T) in enterprise support, sustainability, and growth, especially in the context of digital transformation. This concept is

gaining traction as organizations recognize the necessity for effective governance structures that integrate I&T into enterprise risk management.

Key points include:

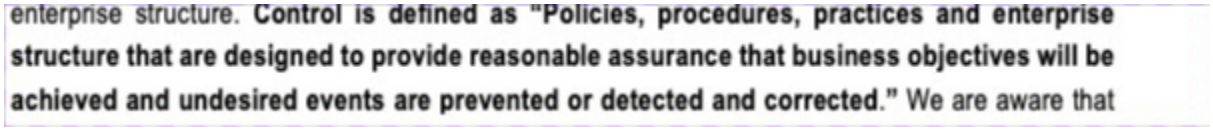
- **Definition**: EGIT involves defining and embedding processes that align business and IT responsibilities, enhancing value from IT investments.

- **Focus**: It goes beyond installing superior IT infrastructure, focusing on overall management and governance.

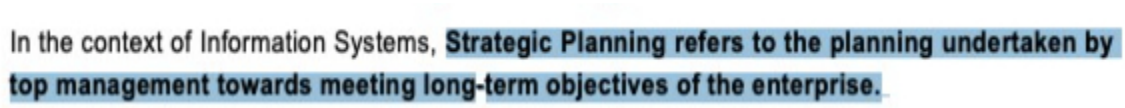
- **Role of Boards**: Governing boards are crucial in overseeing the integration of I&T processes to ensure that both business and IT align strategically and fulfill their roles effectively.

In summary, EGIT is vital for optimizing IT performance and managing risks related to IT dependencies, ensuring that organizations maximize the benefits of their IT-enabled initiatives.

Business and IT Strategy


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

- IT must integrate seamlessly with business strategies.
- **IT Steering Committee**: Guides IT deployment aligned with enterprise goals.
- **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.**

1. Enterprise Strategic Plan.
2. IS Strategic Plan.
3. IS Requirements Plan.

4. IS Applications and Facilities Plan.

1.5.5: Key Management Practices for Aligning IT Strategy with Enterprise Strategy

This section emphasizes aligning IT strategy with the overarching goals and strategies of an enterprise. The key practices include:

1. **Understand Enterprise Direction**
    - Analyze the enterprise's current environment, business processes, strategy, and future objectives.
    - Consider external factors like industry trends, regulations, and competition.
2. **Assess Current Environment, Capabilities, and Performance**
    - Evaluate the performance of internal business and IT capabilities, as well as external IT services.
    - Understand the enterprise architecture to identify improvement areas.
    - Include service provider differentiation, financial impact, and benefits analysis.
3. **Define Target IT Capabilities**
    - Set goals for future IT and business capabilities based on enterprise needs.
    - Leverage reference standards, best practices, and emerging technologies.
4. **Conduct Gap Analysis**
    - Identify gaps between current and desired IT states.
    - Assess alignment of assets with business outcomes to optimize investments.
5. **Define the Strategic Plan and Roadmap**
    - Create a strategic plan that ties IT goals to enterprise objectives.
    - Define initiatives, sourcing strategies, and measurements for monitoring progress.
6. **Communicate IT Strategy and Direction**
    - Share the IT strategy with relevant stakeholders to create awareness and alignment.

Success Metrics: Alignment is measured through stakeholder satisfaction, IT's support of strategic goals, and mapping IT value drivers to business outcomes.

1.5.6: Business Value from Use of IT

This section discusses ensuring that IT contributes value to the business by optimizing processes, services, and assets.

1. **Evaluation of Value Optimization**
    - Regularly assess IT-enabled investments, services, and assets for value creation at reasonable costs.
    - Adjust direction to maximize value realization.
2. **Direction of Value Optimization**
    - Use value management principles to achieve optimal returns from IT investments over their lifecycle.
3. **Monitoring Value Optimization**
    - Track goals and metrics to ensure the expected value is realized.
    - Address significant issues with corrective actions where necessary.

Success Metrics:

- Percentage of IT-enabled investments where benefit realization is monitored.
- Percentage of IT services delivering expected benefits.
- Accuracy and transparency of IT financial data.


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.

Frameworks for IT Governance

1. **COBIT**:
    - Framework for IT governance and management.
    - Organized into five domains: Evaluate, Align, Build, Deliver, and Monitor.
    - **Principles**: Stakeholder value, holistic approach, dynamic systems, tailored needs, End to end governance system and distinct governance from management.

(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.

2. **ITIL**: Information technology Infrastructure library
    - Service management framework aligning IT with business needs.
    - Includes practices in general, service, and technical management.
3. **ISO 27001**:
    - Focuses on information security management systems (ISMS).
    - Promotes risk management and compliance.

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.

Key Areas Identified in the MCQs

1. **COBIT 5 Domains**
    - **Align, Plan, and Organize (APO)**:
        - Covers overall organization, strategy, and supporting IT-related activities.
        - Focused on aligning IT strategy with business objectives.
    - **Build, Acquire, and Implement (BAI)**:
        - Focuses on acquiring and integrating IT solutions into business processes.
    - **Deliver, Service, and Support (DSS)**:
        - Emphasizes operational delivery, including incident and service management.
        - Example: DSS01 manages IT operations.
    - **Monitor, Evaluate, and Assess (MEA)**:
        - Monitors performance, compliance, and alignment with enterprise goals.
2. **Governance System Definition**
    - Refers to structured processes and mechanisms enabling stakeholders to meet enterprise objectives.
3. **COBIT Framework**
    - Provides a governance and management structure for enterprise information and technology.
    - Encompasses strategy, risk management, and operational efficiency.

Insights from the Questions

- **Focus on DSS Domain**: Operational aspects, like IT service delivery and support, are highlighted.
- **Governance Objectives**: COBIT 5 emphasizes separating governance and management functions.
- **Stakeholder Involvement**: Governance systems prioritize transparency and accountability.
- **Alignment of Goals**: IT processes are aligned with broader enterprise strategies.

Chapter 2 Governance, Risk, and Compliance (GRC)

Main Points and Sub-Points

2.1 Introduction to GRC (Governance Risk and Compliance)

- GRC integrates governance, risk management, and compliance processes.
- Provides a structured approach for aligning IT with business objectives.
- Helps organizations manage risks, reduce costs, and ensure compliance.

Fig. 2.2: GRC Processes

2.2 Risk Fundamentals

- **Key Concepts**:
  - **Asset**: Anything valuable to the organization, such as customer data, IT systems, or reputation.
  - **Vulnerability**: Weaknesses in systems that can be exploited (e.g., poor access control or outdated software).
  - **Threat**: Events or entities capable of harming systems (e.g., cyber-attacks, natural disasters).
  - **Risk**: Combination of vulnerabilities and threats leading to potential harm.
- **CIA Triad**: Confidentiality- only authorise users can access, Integrity- only authorise users can change, Availability - amt of time user can use a system of information must be maintained.

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.

Summary of 2.2.2: Vulnerability

- **Definition**:
  A vulnerability is a weakness in a system's safeguards that exposes it to threats. These weaknesses may exist in information systems, cryptographic systems, hardware designs, security procedures, or internal controls.

- **Key Characteristics**:

  - It enables threats to exploit the system.
  - Missing safeguards contribute to vulnerability levels.
  - Examples include weak access control methods and short passwords.
- **Identification**:

  - Vulnerabilities are determined through security evaluations, such as penetration testing and safeguard analysis.
  - Vulnerabilities can originate from design flaws, implementation defects, or operational issues.

- **Examples**:
    - Leaving a door unlocked makes a house vulnerable to intruders.
    - Short passwords make a system susceptible to cracking or guessing.

Summary of 2.2.3: Threat

- **Definition**:
  A threat is any entity, event, or circumstance with the potential to harm a system or its components by unauthorized access, destruction, modification, or denial of service.

- **Key Characteristics**:
    - A threat targets an asset and correlates closely with vulnerabilities.
    - Threats exploit vulnerabilities to cause harm or disruption.
- **Types of Threats**:
    - **Disclosure Threats**: Unauthorized access to confidential data, such as a data breach or espionage.
    - **Alteration Threats**: Unauthorized modifications to data, compromising integrity.
    - **Denial of Service/Destruction Threats**: Rendering systems or data unavailable through attacks like DoS.
- **Examples**:
    - A hurricane threatening physical infrastructure.
    - A cyber-attack aiming to steal sensitive data.
- **Prevention**:
    - Protect assets by mitigating vulnerabilities, as threats cannot be fully eliminated.

2.3 Risk Management

- **Levels of Risk**: Risk = threat x vulnerability
    - **Inherent Risk**: Before any controls are applied.
    - **Current/Residual Risk**: After implementing controls.
    - **Target Risk**: Desired level of risk after applying additional controls.
- **Types of Risks**:
    - **Compliance Risks**: Fines/penalties for non-compliance with laws.
    - **Operational Risks**: Inefficiencies or system failures.
    - **Strategic Risks**: Challenges in meeting organizational goals.
    - **Reputational Risks**: Damage to brand due to ethical lapses or failures.

- **Technological Risks**: Failures in technology systems.

Summary of 2.3.3: Types of Risks

Risks faced by organizations can be broadly categorized as follows:

1. **Compliance Risks**:
    - Arise from non-compliance with laws, regulations, or internal policies.
    - Examples include penalties for data protection violations or environmental non-compliance.
2. **Hazard (Pure) Risks**:
    - Potentially harmful situations, such as natural disasters, theft, or health and safety hazards.
3. **Control (Uncertainty) Risks**:
    - Unpredictable risks associated with projects or new initiatives.
    - These involve unknown outcomes, costs, or delivery timelines.
4. **Opportunity (Speculative) Risks**:
    - Risks with potential positive or negative outcomes.
    - Example: Taking a new business opportunity that may succeed or fail.
5. **Examples of Real-World Risks**:
    - Operational risks like employee fraud.
    - Strategic risks from global market conditions or changing customer needs.

Summary of 2.3.4: Risk Management/Mitigation Strategies

Organizations use **risk management strategies**, often referred to as the **4T's**, to address identified risks:

1. **Transfer**:
    - Sharing risk with third parties like insurers or vendors.
    - Example: Purchasing insurance to mitigate financial risks.
2. **Tolerate**:
    - Accepting risks that are minor or costlier to mitigate.
    - Example: Planning for minor production delays.
3. **Terminate**:

    - Avoiding risks entirely by modifying or stopping activities.
    - Example: Replacing risky technology or vendors with safer alternatives.
4. **Treat**:
    - Mitigating risks by implementing controls to reduce impact.
    - Example: Installing firewalls or creating daily data backups.

Risk Matrix and Dominant Responses:

- **High Impact, Low Likelihood**: Transfer.
- **High Impact, High Likelihood**: Terminate.
- **Low Impact, Low Likelihood**: Tolerate.
- **Low Impact, High Likelihood**: Treat.

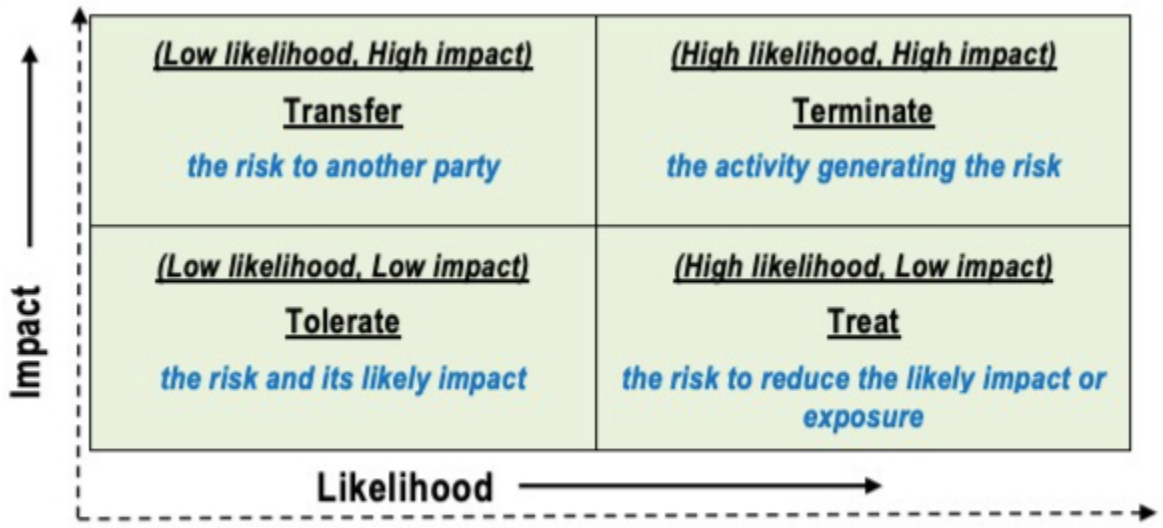


Fig. 2.6: Risk Matrix and 4T's of Risk Management Strategies

2.4 Malicious Attacks

- **Types of Threats**:
    - **Active Attacks**: Direct modification of systems (e.g., brute force, phishing).
    - **Passive Attacks**: Eavesdropping or monitoring transmissions.
- **Examples of Attacks**:
    - **IP Spoofing**: Disguising as an authorized entity.
    - **Phishing**: Tricking users to reveal confidential data.
    - **Replay Attacks**: Resending intercepted data packets.
    - **Man-in-the-Middle**: Intercepting and modifying communications.

Summary of 2.4: Malicious Attacks

Malicious attacks are threats to IT infrastructure, classified as **active** or **passive**:

Active Attacks

These involve direct modifications or intrusions into systems:

1. **Brute-Force Password Attacks**:
    - Attackers repeatedly try combinations to crack passwords.
    - Mitigation: Enforce complex passwords and account lockout policies.
2. **Dictionary Attacks**:
    - Common passwords are tested using dictionary words.
    - Mitigation: Avoid simple passwords and include mixed-case letters, numbers, and symbols.
3. **IP Address Spoofing**:
    - Attackers disguise themselves as legitimate users by altering IP addresses.
    - Mitigation: Configure network routers to block unauthorized traffic.
4. **Phishing**:
    - Fake emails or websites trick users into revealing sensitive information.
    - Mitigation: Educate users and avoid clicking suspicious links.
5. **Hijacking**:
    - **Browser Hijacking**: Redirects users to fake websites (e.g., typo-squatting).
    - **Session Hijacking**: Intercepts and takes over active communication sessions.
6. **Replay Attacks**:
    - Previously intercepted data packets are reused to disrupt systems.
    - Mitigation: Use session tokens and timestamp validation.
7. **Man-in-the-Middle (MITM) Attacks**:
    - Attackers intercept and modify communications between two parties.
    - Example: Web spoofing to collect sensitive data like passwords.

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.

Passive Attacks

Involve monitoring or eavesdropping without altering data:

1. **Eavesdropping**:
    - Unauthorized monitoring of network traffic to collect sensitive information.
    - Mitigation: Encrypt communications.
2. **Social Engineering**:
    - Attackers manipulate individuals to reveal confidential information.
    - Mitigation: Train employees on recognizing deceptive techniques.

Examples of Social Engineering

- Impersonating a technician to gain access to secure areas.
- Targeting untrained employees or those unfamiliar with security policies.

Mitigation Techniques for Malicious Attacks

- Educate employees on cybersecurity awareness.
- Implement firewalls and intrusion detection systems.
- Regularly update software to patch vulnerabilities.
- Enforce strict access controls and authentication protocols.

Malicious attacks exploit human and technical vulnerabilities, emphasizing the need for robust security measures and proactive monitoring.

2.5 Malicious Software (Malware)

- **Categories**:
  - **Infecting Programs**: Viruses, worms.
  - **Hiding Programs**: Trojan horses, rootkits, spyware.
- **Purpose**: Disrupt systems, steal data, or cause financial harm.

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.

Summary of 2.5: Malicious Software (Malware)

Malware refers to malicious software designed to infiltrate and harm systems, networks, or devices. It can cause data breaches, system crashes, or unauthorized access. Malware generally falls into two main categories: **Infecting Programs** and **Hiding Programs**.

Categories of Malware

1. Infecting Programs

These programs actively replicate themselves or infect other systems:

- **Virus**:
  - Attaches to or copies itself into another program.
  - Requires a host to spread and can replicate to other computers.
  - Causes harm by corrupting files, slowing systems, or crashing programs.
- **Worm**:
  - Self-contained program that replicates across networks without a host.
  - Can overload networks by consuming bandwidth or perform malicious actions.

---

2. Hiding Programs

These programs conceal themselves while executing malicious activities:

- **Trojan Horse**:
    - Disguised as legitimate software to trick users into executing it.
    - Often used to collect sensitive data, open backdoors, or upload/download files.
- **Rootkit**:
    - Modifies or replaces system programs to hide its presence.
    - Provides attackers with ongoing access to compromised systems.
    - Difficult to detect and can affect operating systems like Linux, UNIX, and Windows.
- **Spyware**:
    - Collects user information without consent, often for malicious purposes like identity theft.
    - Functions include monitoring keystrokes, scanning files, and reading browser cookies.

Effects of Malware

- Slowing down or crashing systems.
- Theft of sensitive information, such as credit card details and passwords.
- Unauthorized data modifications or deletions.

Examples of Malware Behaviors

- Monitoring user activity (e.g., keystroke logging).
- Exploiting security vulnerabilities.
- Manipulating system files to avoid detection.

Mitigation Strategies

- Install and update antivirus and anti-malware tools.
- Avoid downloading software from untrusted sources.
- Perform regular system scans and backups.
- Use firewalls to restrict unauthorized access.

Malware poses a significant threat to personal and business systems, emphasizing the importance of robust security measures and user education.

2.6 Countermeasures

- **Strategies to Mitigate Risks**:
    - Education and awareness programs.
    - Anti-malware tools and regular scans.
    - Implementation of firewalls and secure authentication.

2.7 Internal Controls

- **Key Components**:
    - **Control Environment**: Organizational ethics and standards.
    - **Risk Assessment**: Identifying risks and their impact.
    - **Control Activities**: Policies to mitigate risks (e.g., segregating duties, authorization systems).
    - **Information and Communication**: Transparent sharing of relevant data.
    - **Monitoring**: Ongoing evaluations of control effectiveness.
- **Limitations**:
    - Cannot provide absolute assurance due to human error or fraud.

2.8 Compliance

- Ensures adherence to laws, regulations, and internal policies.
- Non-compliance may lead to financial penalties, reputational damage, and operational setbacks.

Brief Description of Risks

- **Compliance Risks**: Result from non-adherence to regulatory or legal obligations.
- **Operational Risks**: Arise from failed internal processes, systems, or human errors.
- **Strategic Risks**: Linked to long-term organizational goals and market conditions.
- **Reputational Risks**: Damage caused by public perception due to ethical lapses or failures.
- **Technological Risks**: Failures in IT systems, leading to service disruptions.
- **Financial Risks**: Impact on revenue and asset loss due to market fluctuations or fraud.

Based on the **MCQs in Chapter 2 of the PDF**, the **key areas of focus** are as follows:

---

1. Governance, Risk, and Compliance (GRC) Framework

- Definition and objectives of GRC:
    - Integration of governance, risk management, and compliance.
    - Structured approach to align IT with business objectives.
    - Improves decision-making and performance.
- Features of GRC tools:
    - Workflow management.
    - Real-time dashboards for compliance and risk assessment.
    - Risk data management and analytics.

---

2. Risk Fundamentals

- **Asset Characteristics**:
    - Valuable to the organization.
    - Hard to replace without cost, time, or resources.
    - Examples: Customer data, IT infrastructure, intellectual property.
- **Vulnerability**:
    - Weaknesses in systems that threats can exploit.
    - Examples: Poor access controls, short passwords.
- **Threats**:
    - Events or entities capable of exploiting vulnerabilities.
    - Types:
        - **Disclosure Threats**: Unauthorized access to private information.
        - **Alteration Threats**: Unauthorized changes to data.
        - **Denial of Service/Destruction Threats**: Rendering resources unavailable.
- **Risk Definition**:
    - Interaction between threats, vulnerabilities, and potential impacts.
    - Example: Risk = Threat × Vulnerability × Impact.

---

3. Levels and Types of Risk

- **Levels of Risk**:
    - Inherent: Risk without controls.
    - Current/Residual: Risk after controls are applied.
    - Target: Desired level after further mitigation.
- **Types of Risks**:
    - Compliance Risks: Non-adherence to regulations.
    - Operational Risks: Failures in processes or systems.
    - Strategic Risks: Challenges in achieving business objectives.
    - Reputational Risks: Negative public perception due to ethical failures.
    - Technological Risks: Failures in IT systems.

---

4. Risk Management Strategies

- **4T's Framework**:
    - **Transfer**: Sharing risks with third parties (e.g., insurance, outsourcing).
    - **Tolerate**: Accepting minor risks where mitigation costs exceed benefits.
    - **Terminate**: Avoiding activities with high-risk potential.
    - **Treat**: Implementing controls to reduce risks to acceptable levels.

---

5. Malicious Attacks

- **Active and Passive Threats**:
    - **Active Threats**: Include brute force, phishing, and IP spoofing.
    - **Passive Threats**: Eavesdropping and monitoring transmissions.
- Examples of specific attacks:
    - **Phishing**: Tricking users into revealing sensitive information.
    - **Man-in-the-Middle**: Intercepting and modifying communication between two parties.
    - **Replay Attacks**: Reusing intercepted data packets.

---

6. Internal Controls

- Components:
    - **Control Environment**: Organizational ethics and governance.
    - **Risk Assessment**: Identifying and analyzing risks.
    - **Control Activities**: Policies and procedures to mitigate risks.
    - **Information and Communication**: Dissemination of data across the organization.
    - **Monitoring**: Ongoing evaluation of controls.
- Limitations:
    - Human error.
    - Collusion or management override.
    - Inability to cover unusual transactions.

---

7. Compliance

- Adherence to:
    - External laws and regulations.
    - Internal policies and standards.
- Examples:
    - GDPR for data protection.
    - PCI DSS for payment security.

CHAPTER 3

1. Enterprise Risk Management (ERM) Framework

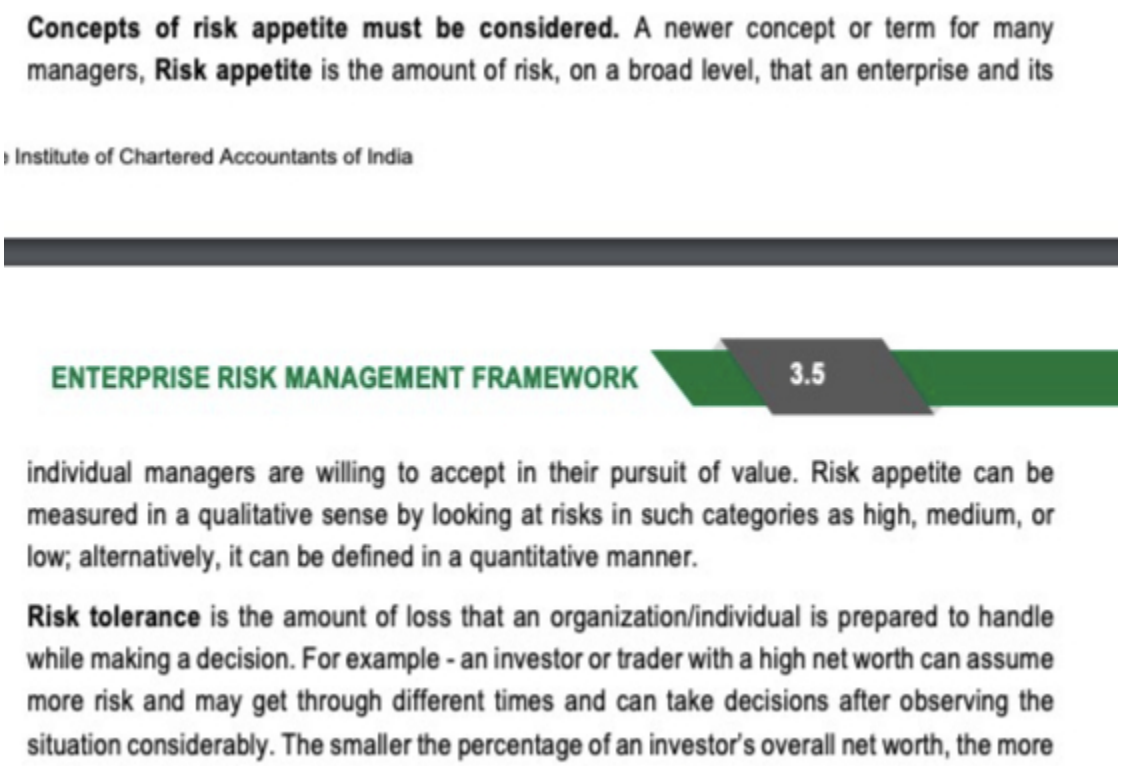
- **Definition**: A structured approach to managing risks and opportunities that affect an organization's objectives.
- **Importance**: Helps in creating and protecting value for stakeholders.
- The ERM Framework is designed to help organizations identify, assess, manage, and monitor risks that could impact their ability to achieve objectives. It aims to create and protect value for stakeholders by integrating risk management into the organization's processes.

2. Components of the ERM Framework (CRICkEt On Monitor)

- **Control Environment**
  - Sets the organizational tone regarding risk.
  - Includes risk management philosophy and risk appetite.
- **Objective Setting**
  - Objectives must align with the organization's mission and risk appetite.
  - Objectives must be SMART.
  -
- **Event Identification**
  - Identifies potential events that could impact objectives.
  - Distinguishes between risks and opportunities.
- **Risk Assessment**
  - Analyzes identified risks based on likelihood and impact.
  - Considers both inherent and residual risks.
- **Risk Response**
  - Management selects actions to align risks with risk tolerance.
  - Possible responses include avoiding, accepting, reducing, or sharing risks.
- **Control Activities**
  - Policies and procedures to ensure effective risk response implementation.
- **Information & Communication**
  - Relevant information must be captured and communicated effectively.
  - Ensures all levels of the organization are informed about risks.
- **Monitoring**
  - Continuous monitoring of the ERM process.
  - Adjustments made as necessary based on evaluations.

Management Objectives:

- The framework addresses four categories of management objectives: **Strategic, Operational, Reporting, and Compliance**. Each category reflects different aspects of organizational performance and risk management.



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

› Institute of Chartered Accountants of India

ENTERPRISE RISK MANAGEMENT FRAMEWORK 3.5

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

Integration and Implementation:

- Successful implementation of the ERM Framework requires integration into the organization's culture and processes. It emphasizes the need for a risk-aware culture and alignment with other organizational activities.

Benefits of ERM:

- By adopting the ERM Framework, organizations can enhance decision-making, improve resource allocation, increase resilience, and better manage uncertainties that could impact their objectives.

3. Management Objectives

- **Strategic**: Aligning risk management with strategic goals.
- **Operations**: Ensuring operational efficiency and effectiveness.

- **Reporting**: Accurate reporting of risk performance.
- **Compliance**: Adhering to laws and regulations.

4. Implementation of IT Controls

- Importance of IT in all enterprises.
- Need for both regulatory and management perspectives in IT controls.
- Focus on governance practices and their adequacy.

5. COSO Frameworks

- Emphasis on internal environment over external influences.
- Focus on loss prevention rather than risk-taking for returns.

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.

6. Learning and Improvement

- Evaluate effectiveness of existing controls.
- Embed a risk-aware culture within the organization.
- Monitor and report on risk performance indicators.

Fig. 3.3: Implementing Risk Management by PIML

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.

This structured summary captures the essential points and subpoints from the PDF, providing a clear overview of the ERM framework and its components.

Based on the multiple-choice questions (MCQs) provided in the PDF, here are the important topics summarized:

1. Components of the ERM Framework

- **Control Activities**: Policies and procedures established to ensure that risk responses are effectively carried out.
- **Risk Assessment**: The process of identifying and analyzing risks that could affect the achievement of objectives.

- **Information and Communication**: Ensures that relevant information is communicated effectively throughout the organization.
- **Monitoring**: Continuous evaluation of the ERM process to ensure its effectiveness and to make necessary adjustments.

2. Management Objectives

- **Strategic Objectives**: Aligning risk management with the organization's strategic goals.
- **Operational Objectives**: Ensuring efficiency and effectiveness in operations.
- **Reporting Objectives**: Accurate and timely reporting of risk performance.
- **Compliance Objectives**: Adhering to laws, regulations, and internal policies.

3. Risk Management Principles

- **Risk Appetite**: The level of risk that an organization is willing to accept in pursuit of its objectives.
- **Event Identification**: The process of identifying potential events that could impact the organization's objectives.
- **Risk Response**: Selecting appropriate actions to address identified risks, which may include avoiding, accepting, reducing, or sharing risks.

4. Benefits of Integrating ERM

- **Increased Positive Outcomes**: Enhancing the likelihood of achieving objectives.
- **Reduced Negative Surprises**: Minimizing unexpected adverse events.
- **Improved Resource Deployment**: Better allocation of resources to manage risks effectively.
- **Enhanced Enterprise Resilience**: Strengthening the organization's ability to withstand challenges.

5. COSO ERM Framework

- **Focus on Internal Environment**: Emphasizes the internal controls and governance practices within the organization.
- **Risk Response**: Addresses the need to manage risks not just to avoid losses but also to pursue opportunities for returns.

6. Implementation of ERM

- **Establishing Policies and Procedures**: Necessary for effective risk management and ensuring that selected risk responses are executed.
- **Embedding a Risk-Aware Culture**: Integrating risk management into the organizational culture and daily operations.

CHAPTER 4

Learning Outcomes

- Understand components and functioning of information systems.
- Recognize the need for protecting information systems.
- Identify security policies, standards, and guidelines.
- Analyze information security threats and countermeasures.

Chapter Overview

Case Study: XYZ Ltd.

- Challenges: Lack of a documented security policy, insufficient management support, absence of dedicated security personnel.
- Risks: Financial losses, productivity delays, loss of intellectual property, and reputation damage.
- Needs: Security training, awareness programs, defined roles, and responsibilities.

Introduction to Information Systems

- Defined as a combination of people, hardware, software, data, and networks.
- Aim: Transform data into meaningful information.
- Components include hardware, software, people, data resources, and networking systems.

Need for Protection of Information Systems

- Reliance on IT for business processes introduces security risks.
- Threats include hacking, viruses, denial of service (DoS) attacks, and natural disasters.
- Importance of safeguarding operations, data, applications, and technology assets.

Information System Security

- Focus: Protect data and system resources from loss, alteration, or disclosure.
- Key Components:

    - Logical safeguards (firewalls, passwords).
    - Physical safeguards (locks, secured premises).
- Ensures confidentiality, integrity, and availability (CIA triad).

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):

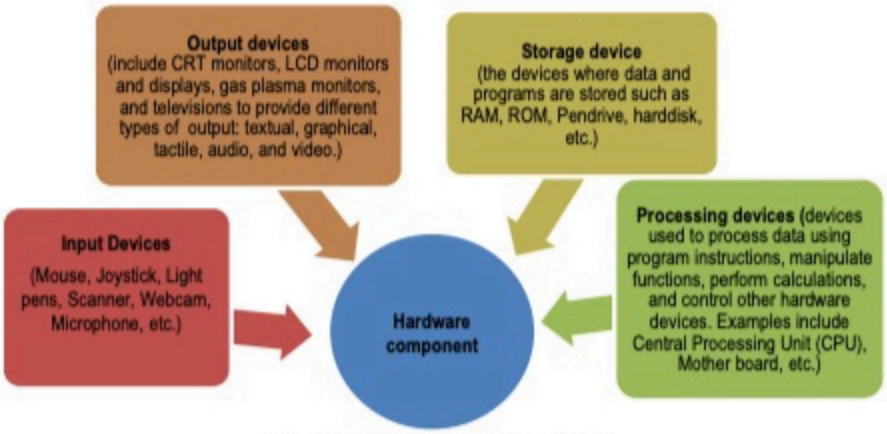


Fig. 4.4: Hardware components

- **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.

Principles of Information Security

1. **Confidentiality**: Protect information from unauthorized access.
2. **Integrity**: Prevent unauthorized modifications.

3. **Availability**: Ensure timely and reliable access to information.

Information Security Policy

- Formal statement outlining protection measures for information assets.
- Components:
    1. Purpose, scope, and audience.
    2. Incident response and monitoring mechanisms.
    3. Roles and responsibilities.
- Types of Policies:
    1. User Security Policies.
    2. Organization Security Policies.
    3. Network and System Security Policies.

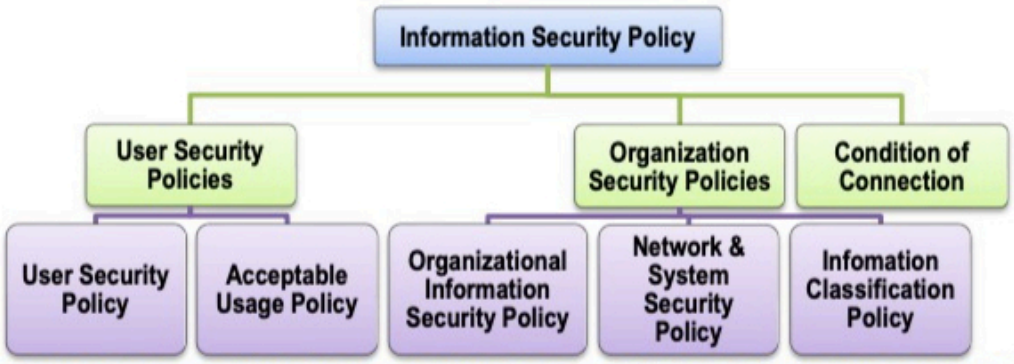
4.6.4 Information Security Policies and their Hierarchy

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.



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.

Tools to Implement Information Security

1. **Standards**: Define technologies and methodologies.
2. **Guidelines**: Provide flexible implementation approaches.
3. **Procedures**: Step-by-step instructions for specific tasks.

- Framework aligns policies with organizational goals.

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.

Monitoring and Auditing

- Regular checks to ensure policies align with business strategies.
- Importance of adapting to evolving risks.
- Internal and external audits assess effectiveness.

Case Studies

Case A: XYZ Ltd.

- No formal policy, reactive approach to risks.
- Issues: Lack of training, ad hoc security measures, and no disaster recovery plan.

Case B: JK Pvt. Ltd.

- Comprehensive policy with management support.
- Initiatives: Employee training, regular audits, and layered security architecture.

Key Concepts and Questions

- Addressed topics: Confidentiality, integrity, access control, and compliance.
- CIA triad and hierarchical policies emphasized.

Summary

- Information security is essential for safeguarding organizational assets.
- Policy implementation and monitoring improve risk management.
- Regular audits and training foster a culture of security awareness.

Chapter 5: Business Continuity Planning and Disaster Recovery Planning

---

Learning Outcomes

After studying this chapter, learners will:

- Understand Business Continuity Management (BCM).
- Comprehend the key phases of developing a Business Continuity Plan (BCP).
- Grasp the BCM process and its cycle.
- Learn about various types of plans and backups.
- Understand Incident Management Plans (IMP) and Disaster Recovery Procedural Plans (DRPP).

Key Concepts

Introduction

- BCM helps enterprises manage disruptions due to outages or disasters.
- Ensures continuity of operations, reducing revenue and reputation loss.
- Regular audits ensure BCM aligns with policy and regulatory requirements.

---

1. Business Continuity Management (BCM)

Need for BCM

- Protects critical business functions during disruptions like power outages or disasters.
- Ensures recovery with minimal impact.

Scope

- Involves top management defining BCM scope, obligations, and control over outsourced activities.

Advantages

- Proactive threat assessment.
- Planned responses to minimize disruption.
- Regular testing for readiness.

---

2. Business Continuity Policy

- A high-level guide to reduce losses in revenue, reputation, and productivity.
- Defines scope, guidelines, and responsibilities for continuity.
- Ensures regular testing, revision, and training.

---

3. Business Continuity Planning (BCP)

Key Areas

1. **Business Resumption Planning:** Operational response.
2. **Disaster Recovery Planning:** Technical recovery aspects.
3. **Crisis Management:** Organizational coordination during crises.

Objectives

- Ensure safety, minimize disruptions, coordinate recovery, and identify critical processes.

Development Phases

1. **Pre-Planning:** Scope definition and scheduling.
2. **Vulnerability Assessment:** Risk mitigation strategies.
3. **Business Impact Analysis (BIA):** Assess criticality and impact.
4. **Detailed Requirements:** Resource profiles for recovery.
5. **Plan Development:** Documentation of recovery strategies.
6. **Testing/Exercising:** Validation of BCP.
7. **Maintenance:** Keeping plans current.
8. **Implementation:** Initial testing and integration.

---

4. BCM Process & Cycle

1. **Information Collection:** Identify interdependencies and risks.
2. **BCM Strategies:** Develop response measures.
3. **Implementation:** Structure incident management teams.
4. **Testing & Maintenance:** Regular evaluations to identify gaps.
5. **Training & Awareness:** Ensure all stakeholders are prepared.

---

5. Types of Plans

1. **Emergency Plan:** Immediate actions post-disaster.
2. **Backup Plan:** Data recovery procedures.

3. **Recovery Plan:** Long-term restoration of operations.
4. **Test Plan:** Identifies gaps in other plans via simulations.

---

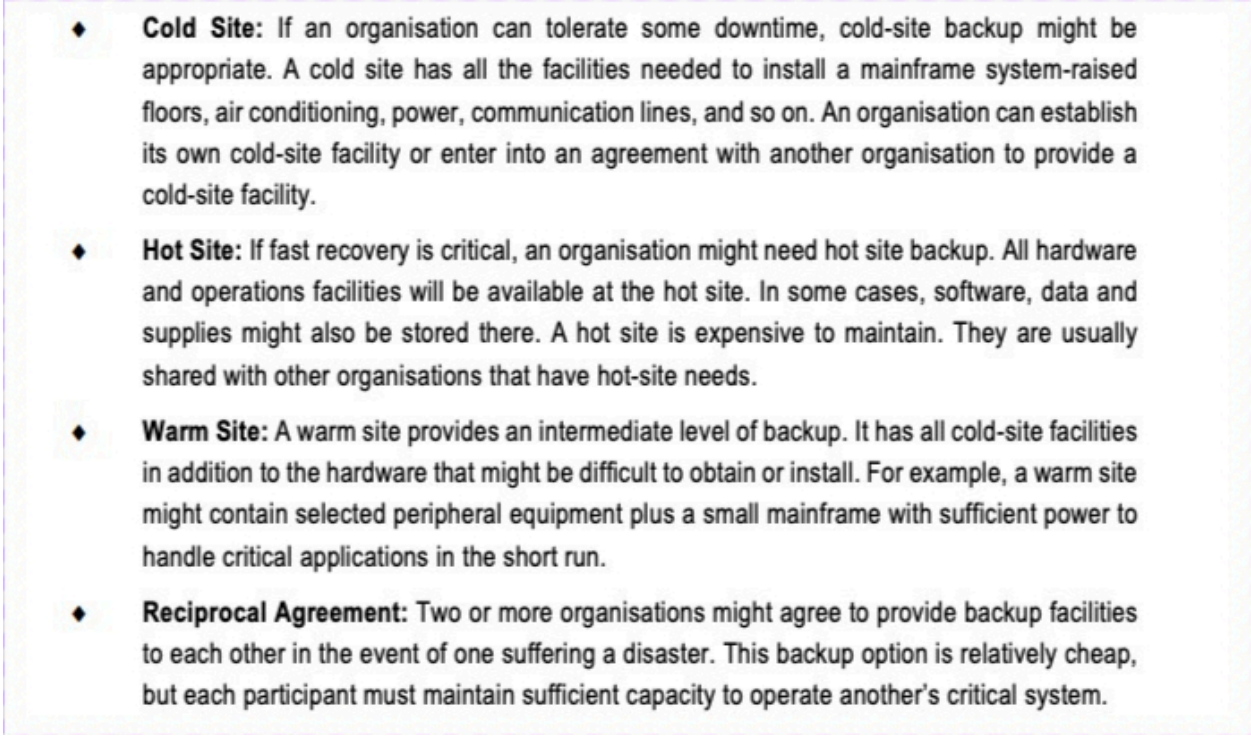
6. Types of Backups

1. **Full Backup:** Entire dataset backup.
2. **Incremental Backup:** Only changes since the last backup.
3. **Differential Backup:** All changes since the last full backup.
4. **Mirror Backup:** Real-time replication without compression.
5. **Cloud Backup:** Off-site storage for redundancy.

---

7. Alternate Processing Facilities

1. **Cold Site:** Basic setup for recovery; slower activation.
2. **Warm Site:** Includes hardware for partial operations.
3. **Hot Site:** Fully functional facilities for quick recovery.
4. **Reciprocal Agreements:** Shared resources with another organization.



- **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.

---

8. Disaster Recovery Procedural Plan

Includes:

- Activation conditions, fallback, and resumption procedures.
- Testing and maintenance schedules.
- Emergency contacts, medical procedures, and vendor lists.
- Alternate manual processes.

Summary

- BCM ensures operational continuity, safeguarding revenue and reputation.
- Plans and policies must be tested, updated, and communicated regularly to maintain effectiveness.

Key Areas for Focus Based on MCQs in Chapter 5

---

1. Business Continuity Management (BCM)

- **Definition and Importance:** Focus on BCM's role in ensuring continuity during disruptions like power outages, natural disasters, or cyberattacks.
- **Scope and Advantages:**
    - Identification of key products/services.
    - Risk accountability for outsourced services.
    - Proactive threat assessment and damage minimization.

---

2. Business Continuity Policy (BCP)

- **Objectives:**
    - Minimize revenue, reputation, and productivity loss.
    - Ensure critical service delivery during disruptions.
- **Key Components:**
    - Scope and guidelines for continuity.
    - Ongoing testing and responsibility assignment.

---

3. Business Continuity Planning (BCP)

- **Primary Objectives:**
    1. Ensure critical operations resume within an acceptable timeframe.
    2. Establish emergency powers and recovery coordination.
- **Key Phases:**

1. Pre-planning and project initiation.
2. Vulnerability assessment and security controls.
3. Business Impact Analysis (BIA) to identify critical systems.
4. Recovery strategy definition.

---

4. Types of Plans

- **Emergency Plan:** Immediate actions post-disaster (e.g., fire evacuation).
- **Backup Plan:** Specifies frequency, type (full, incremental, differential), and recovery locations.
- **Recovery Plan:** Long-term restoration strategy.
- **Test Plan:** Regular testing to identify gaps in preparedness.

---

5. Backup Types

- **Full Backup:** All data backed up every time; high storage use.
- **Incremental Backup:** Only new/changed files since the last backup.
- **Differential Backup:** All changes since the last full backup.
- **Mirror Backup:** Real-time, exact replication of files.
- **Cloud Backup:** Offsite, accessible backup for redundancy.

---

6. Alternate Processing Facilities

- **Cold Site:** Basic infrastructure; slow recovery.
- **Warm Site:** Partial infrastructure with some hardware.
- **Hot Site:** Fully equipped for immediate recovery.
- **Reciprocal Agreements:** Shared recovery resources.

---

7. Disaster Recovery Procedural Plan

- **Key Elements:**
    - Conditions for plan activation.
    - Emergency, fallback, and resumption procedures.
    - Regular maintenance and awareness activities.

---

8. Business Continuity Management Cycle

1. **Information Collection:** Identify critical activities, assets, and risks.
2. **BCM Strategies:** Develop appropriate response measures.
3. **Implementation:** Establish incident management teams.
4. **Testing and Maintenance:** Evaluate and refine plans.
5. **Training and Awareness:** Ensure readiness across stakeholders.

Specific Focus Areas (MCQ Context)

1. **BCM Cycle:** Understanding all stages (e.g., Information Collection, Development & Implementation, Testing).
2. **Backup Methods:** Characteristics, advantages, and disadvantages of full, incremental, differential, and mirror backups.
3. **Plan Testing:** Importance of periodic testing and types of tests (e.g., desk checks, simulations).
4. **Processing Facility Options:** Differences between cold, warm, and hot sites.
5. **Key Documents in BCM:** BIA report, risk assessment, incident logs, and business continuity strategies.

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

Chapter 6: System Development Life Cycle (SDLC)

Learning Outcomes

After studying this chapter, you will:

- Understand the need for a System Development Life Cycle (SDLC).
- Learn the phases and activities involved in SDLC.
- Recognize the importance of testing, implementation, and maintenance of information systems.

Key Concepts

1. Introduction

- **Definition:** SDLC provides a structured framework for developing and maintaining systems.
- **Purpose:** Ensures better planning, control, and quality of system development.
- **Barry Boehm's W5HH Principle:** Helps project managers address objectives, schedules, responsibilities, and resource needs.

Table 6.1: W5HH Principle

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

---

2. Need for SDLC

- New service delivery opportunities or problems in existing systems.
- Strategic management focus shifts (e.g., mergers, new delivery channels).
- Technology advancements or competitor strategies involving automation.
- **Advantages:** Better planning, quality compliance, and documentation.
- **Shortcomings:** Cumbersome for small projects, prolonged timelines.

---

3. Phases of SDLC

1. **Preliminary Investigation:**
    - Evaluates system feasibility (technical, financial, operational, legal, etc.).
    - Results in a feasibility study and recommendations to management.
2. **System Requirements Analysis:**
    - Gathers and documents end-user requirements.
    - Tools: Data Flow Diagrams, E-R diagrams, system modeling, and questionnaires.
    - Delivers the **System Requirements Specification (SRS)**.
3. **System Design:**
    - Logical design (blueprint) and physical construction (hardware, software, databases).
    - Key activities: User interface design, database design, and control measures.
4. **System Development:**
    - Converts design into functional systems via coding, debugging, and documentation.
    - Includes coding standards, programming languages, and debugging processes.

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.
- **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.

5. **System Testing:**
    - Types of testing:
        - Unit Testing: Tests individual components.
        - Integration Testing: Tests combined modules.
        - Regression Testing: Ensures changes don't introduce new issues.
        - System Testing: Tests the system as a whole.
        - Final Acceptance Testing: Includes User Acceptance Testing (UAT) and Quality Assurance Testing (QAT).
6. **System Implementation:**
    - Involves hardware installation, user training, and system conversion strategies:
        - **Direct Changeover:** Replaces the old system entirely.
        - **Phased Changeover:** Gradual implementation.
        - **Pilot Changeover:** Testing in a small area before full rollout.
        - **Parallel Changeover:** Running old and new systems simultaneously.
7. **Post-Implementation Review and Maintenance:**
    - **Review:** Assesses the system's success and identifies improvements.

- **Maintenance Types:**
  - Scheduled: Planned updates.
  - Rescue: Immediate troubleshooting.
  - Corrective: Fixing bugs.
  - Adaptive: Adapting to environmental changes.
  - Perfective: Enhancing functionality.
  - Preventive: Improving maintainability.

---

4. Operational Manuals

- Provides users with system operation guidelines.
- Includes FAQs, troubleshooting sections, and contact details for support.

Chapter 7 System Acquisition and Development Methodologies.

Learning Outcomes

- Understanding systematic approaches to system acquisition and their phases.
- Learning about software procurement, IT proposal evaluation, and external acquisitions.
- Analyzing systems for requirement understanding.
- Comparing various SDLC (Software Development Life Cycle) models for suitability.
- Evaluating the pros and cons of system development models.

Illustrative Case Study

An issue with an online ticketing system is highlighted, leading to the conceptualization and implementation of an automated solution for better efficiency and accuracy. This case serves as a framework to introduce the chapter's topics.

Introduction

- **Information Systems (IS):** Defined as a combination of people, hardware, software, networks, and data resources that process information.
- **Need for IS:** IS enhances organizational processes, customer interaction, and data management. It ensures data input, processing, output, and feedback mechanisms.

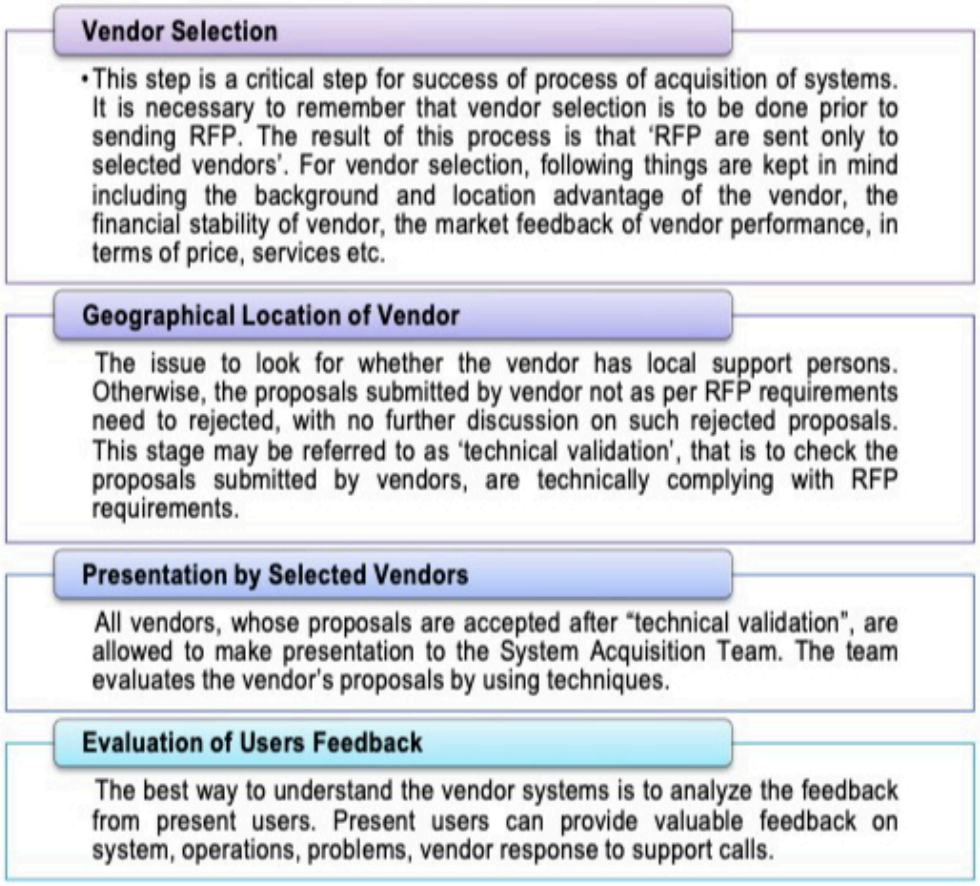
7.2 Information System Acquisition

(A) Acquisition Standards - Management shall introduce acq. Std. that address :

- Importance of security, reliability, and compatibility with existing systems.
- Use of **RFPs (Request for Proposals)** for selecting vendors.
- Emphasis on defining functional, security, and operational requirements in acquisition standards.

(B) Acquiring System Components from vendors

- Formation of a **System Acquisition Committee** to oversee procurement.
- Vendor selection considers factors like location, financial stability, and user feedback.
- Benchmarking is vital to test hardware and software compatibility and performance.



(C) Other Acquisition Aspects

- **Hardware Acquisition:** Emphasizes long-term vendor relationships for support and expansion.
- **Software Acquisition:** Deciding between in-house development or vendor solutions based on system needs.
- **Legal Considerations:** Contracts must clearly outline rights, responsibilities, and intellectual property terms.
- **Compliance:** Ensure systems meet security certifications and legal regulations like GDPR.
- **Proposal Validation:** Evaluates vendor solutions using criteria like compatibility, maintainability, and performance.

(D) System Acquisition Cycle

1. **Defining Requirements:** Includes inputs, processes, and expected outputs.
2. **Identifying Alternatives:** Exploring off-the-shelf, custom, or outsourced solutions.
3. **Feasibility Analysis:** Evaluating economic, technical, operational, and legal constraints.
4. **Risk Analysis:** Identifying vulnerabilities and controls.
5. **Selection Process:** Matching solutions to requirements.

6. **Procuring Software:** Negotiating terms and ensuring compliance with contracts.
7. **Final Acceptance:** Stipulating deliverables and acceptance criteria in agreements.

7.3 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:

General Characteristics

- Phased processes with starting and ending points.
- Deliverables for accountability.
- Approvals and testing at each stage.
- User training and post-implementation reviews.

Models

1. **Waterfall Model**

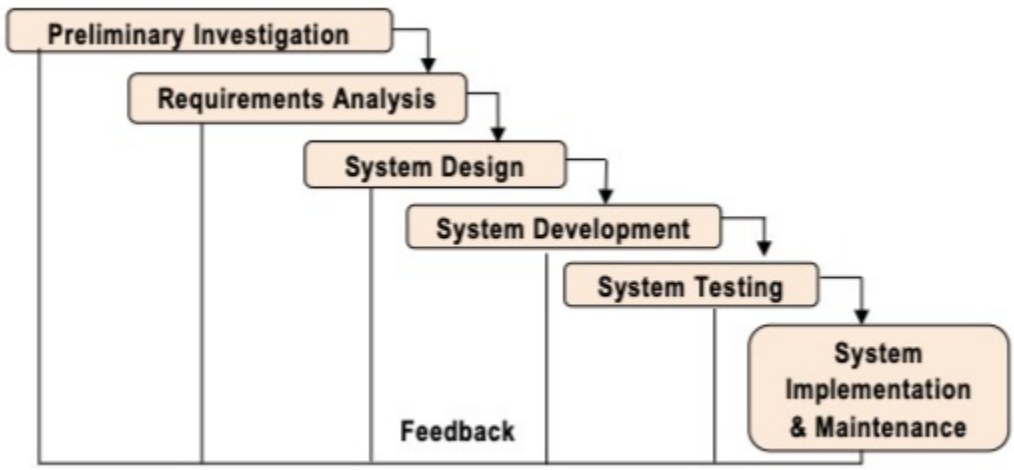


Fig. 7.4: Waterfall Approach

   - Sequential phases.
   - Strengths: Clear documentation, measurable progress.
   - Weaknesses: Rigid, inflexible, and slow to adapt to changes.

2. **Prototyping Model**

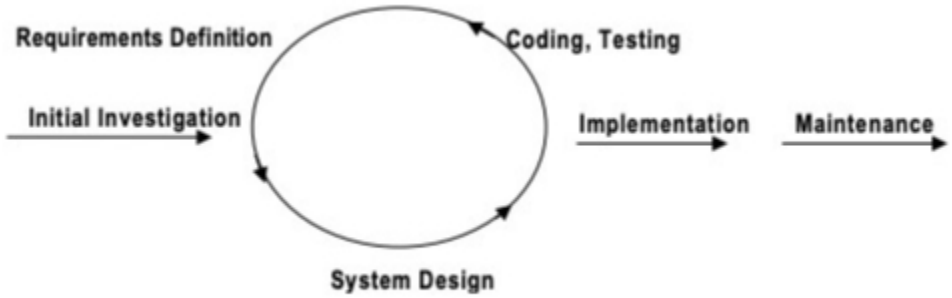
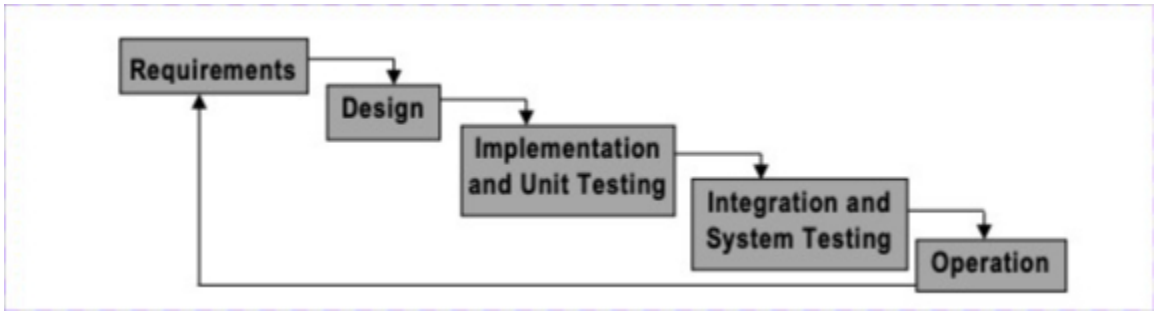


Fig. 7.6: Prototyping Model

- Iterative development of prototypes.
- Strengths: Encourages user feedback, quick iterations.
- Weaknesses: Inadequate documentation, potential for incomplete analysis.

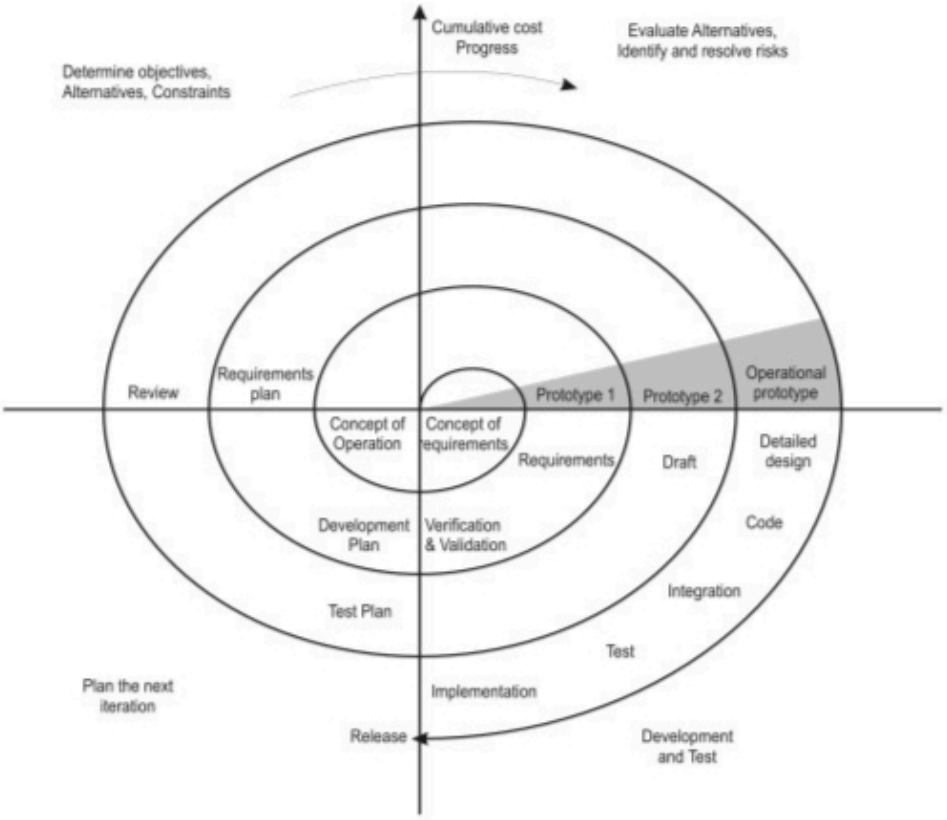
3. **Incremental Model**



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.

- Combines Waterfall and Prototyping methods. **Iterative waterfall**
- Strengths: Risk reduction, early deliverables.
- Weaknesses: Architectural challenges and rigid phase boundaries.

4. **Spiral Model**



   - Combines design and prototyping in stages.
   - Strengths: Risk avoidance and flexibility.
   - Weaknesses: Complexity, dependency on experienced project managers.
5. **Rapid Application Development (RAD)**

   - Focus on rapid prototyping and iterative delivery.
   - Strengths: Quick implementation, user involvement.
   - Weaknesses: Potential quality issues, inconsistency risks.
6. **Agile Model**

   - Iterative and incremental, promoting collaboration and flexibility.
   - Strengths: Adaptive to change, high-quality outcomes.
   - Weaknesses: Lack of documentation and challenges in long-term planning.

Chapter 8 Information Systems Controls and Classification

---

1. Learning Outcomes

- Understand the **Internal Control Framework** and its components.
- Classify various types of controls under different criteria, including objectives, resources, audit perspectives, and control activities.
- Analyze controls aimed at safeguarding assets, maintaining data integrity, and ensuring efficient use of resources.
- Evaluate the role of auditors in assessing and enforcing these controls.

---

2. Illustrative Case Study

- **ABC Multispecialty Hospital** faced operational challenges, resulting in:
    - Reduction in profits due to regulatory changes.
    - Implementation of Business Process Reengineering to cut operating costs.
    - Internal control issues, such as hiring based on nepotism and lack of adherence to policies, led to fraud within the financial system.
    - Discovery and resolution of fraud emphasized the importance of stringent controls and auditor roles in maintaining system integrity.

---

3. Introduction to Information Systems Control

- **Definition of Controls:** Policies, procedures, and organizational structures designed to provide assurance in achieving objectives.
- **Objectives of Information Systems (IS) Controls:**
    - Safeguarding assets.
    - Maintaining data integrity.
    - Achieving organizational objectives efficiently.
- **Internal Control Framework:** Combines preventive, detective, and corrective measures to manage risks.

---

4. Classification of Controls

Controls are classified based on objectives, nature of resources, audit perspectives, and activities.

4.1 Based on Objectives of Controls

- **Preventive Controls:**
    - Designed to prevent errors or malicious acts.
    - Examples: Firewalls, antivirus software, and segregation of duties.
- **Detective Controls:**
    - Identify and report errors or incidents that elude preventive controls.
    - Examples: Intrusion detection systems, internal audits.
- **Corrective Controls:**
    - Address errors or incidents after detection.
    - Examples: Backup restoration, updating IT access rights.
- **Directive Controls:**
    - Provide guidance to manage risks.
    - Examples: SOPs, training manuals.

4.2 Based on Nature of Information System Resources

- **Environmental Controls:**
    - Mitigate risks from fire, electrical surges, water damage, and pollution.
    - Examples: Smoke detectors, UPS systems, water-proofing measures.
- **Physical Access Controls:**
    - Protect physical resources and facilities.
    - Examples: Security guards, CCTV, biometric authentication.
- **Logical Access Controls:**
    - Restrict access to data and systems.
    - Examples: Password policies, encryption, firewalls.

4.3 Based on Audit Perspective

- **Management Control Framework:**
    - Involves senior management's role in planning, organizing, leading, and controlling IS functions.
    - Covers strategic IT policies, security management, and disaster recovery plans.
- **Application Control Framework:**
    - Focuses on controls within specific software applications.
    - Examples: Input controls, processing controls, output controls.

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.

4.4 Based on Control Activities

- **IT Controls:**

    - Focus on safeguarding information systems through hardware, software, and network management.
- **Physical Controls:**
    - Secure assets like documents and infrastructure.
- **Application Controls:**
    - Ensure accuracy and consistency in application-specific operations.

Summary

1. **User Training and Qualification of Operations Personnel**: Staff must possess the necessary skills and competencies to monitor and operate the IT environment, with training as a tool for further skill development.

2. **Change Management**: IT solutions undergo change to adapt to new technology and business needs. A structured change management process is crucial to manage transitions effectively.

3. **Backup, Recovery, and Business Continuity**: Given the dependence on IT, organizations must ensure resilience through proper backup and recovery strategies to minimize disruption.

4. **Application Software Development and Implementation**: Controls during software development are essential for alignment with organizational standards, maintaining budget, and ensuring security and quality.

5. **Confidentiality, Integrity, and Availability of Data**: Security should safeguard sensitive information, ensuring that controls are in place to protect data integrity and availability.

6. **Incident Response Management**: It's vital to have procedures for addressing system failures promptly to mitigate impacts.

7. **Monitoring Applications and Supporting Services**: Continuous oversight of servers and applications is necessary to ensure they perform as per established standards.

8. **General IT Controls**:

- **Information Security Policy**: A comprehensive policy to protect information assets across the organization.

- **Access Controls**: Measures to restrict system access to authorized users only.

- **Separation of IT Functions**: Clear demarcation of roles within the IT Department to avoid conflicts.

- **Management of Systems Acquisition**: Establish protocols for the secure acquisition and implementation of IT systems.

Summary of Section 8.4: Role of Auditors

Auditors play a critical role in evaluating and ensuring the effectiveness of information systems (IS) and related controls. Their responsibilities span various stages of system evaluation and auditing, focusing on both technical and procedural aspects.

Key Responsibilities of Auditors

1. Ensuring Asset Safeguarding

- Verify that organizational assets such as hardware, software, data, and infrastructure are protected against unauthorized access or misuse.
- Evaluate the implementation of physical and logical access controls.

2. Assessing Data Integrity

- Ensure the accuracy, completeness, and reliability of data throughout its lifecycle (input, processing, storage, and output).
- Evaluate systems for proper error detection, validation checks, and consistent data handling.

3. Evaluating System Effectiveness

- Review whether the information system meets user needs and supports decision-making processes.

- Ensure that the system facilitates timely and accurate reporting for stakeholders.

4. Promoting System Efficiency

- Analyze whether resources such as system time, labor, and peripherals are being optimally utilized.
- Recommend improvements to reduce resource wastage and enhance system performance.

5. Monitoring Compliance

- Verify that the organization adheres to relevant legal, regulatory, and internal policy requirements.
- Check for adherence to frameworks like ISO standards, GDPR, or other compliance regulations.

6. Conducting Risk Assessments

- Identify potential risks in system design, implementation, and operation.
- Evaluate controls in place to mitigate risks like unauthorized access, data breaches, or system failures.

7. Providing Recommendations

- Offer actionable suggestions for improving system controls, efficiency, and compliance.
- Advise management on optimizing IT governance frameworks and processes.

Skills and Tools Utilized by Auditors

- Proficiency in **Computer-Assisted Audit Techniques (CAATs)** to automate testing and data analysis.
- Expertise in evaluating both management and application controls.
- Use of techniques like **Integrated Test Facility (ITF)**, transaction tagging, and simulations to validate system performance.

Chapter 9 Information Technology Tools and Digital Ecosystem Controls

---

1. Learning Outcomes

- **Distinguishing Information Systems and IT:** Understand their components and roles in auditing.
- **Information Systems Audit (ISA):** Learn the steps, objectives, and factors influencing IS audits.
- **IT Tools Overview:** Comprehend tools like CAATs (Computer Assisted Audit Techniques) and their applications.
- **Risks and Controls:** Analyze risks in specific business processes (P2P, O2C, HR, CASA, etc.) and related controls.

---

2. Key Concepts

2.1 Information Systems vs. Information Technology

- **Information Systems (IS):** Comprise people, processes, and technology to manage data.
- **Information Technology (IT):** Hardware, software, and communication elements within IS.
- **Auditor Skills:** Auditors require proficiency in IT tools for financial, internal security, and compliance audits.

2.2 Importance of IT Auditing

- **Objective:** Evaluate systems to ensure they meet data processing, control, and security needs.
- **Methods:** Utilize tools like internal control questionnaires, interviews, and document reviews.

---

3. Controls and Inspection of Information Systems

Factors Influencing Controls

1. **Data Loss Costs:** Accurate data enhances adaptability and prevents substantial losses.
2. **Incorrect Decision Costs:** Decisions rely on MIS reports; errors can impact stakeholders.
3. **Computer Abuse Costs:** Includes unauthorized access, malware, and data leaks, harming reputation.

4. **Hardware/Software Value:** IT infrastructure disruptions can affect business competitiveness.
5. **High Costs of Errors:** Errors in processing (e.g., incorrect orders) can lead to significant financial damage.
6. **Privacy Maintenance:** Adhering to regulations like the Digital Personal Data Protection Act ensures security.
7. **Controlled Evolution:** Regular monitoring and updating of IT systems are critical for reliability.

---

4. Information Systems Auditing (ISA)

Objectives

- **Safeguarding Assets:** Protect hardware, software, data, and facilities from unauthorized access.
- **Data Integrity:** Ensure accuracy, reliability, and transparency throughout the data lifecycle.
- **System Effectiveness and Efficiency:** Align systems with user needs while minimizing resource use.

Audit Approaches

1. **Auditing Around the Computer:** Focus on inputs and outputs without reviewing program logic.
2. **Auditing Through the Computer:** Evaluate system controls using techniques like embedded modules, transaction tagging, and simulations.

---

5. Steps in Information Systems Audit

1. **Scoping and Pre-Audit Survey:** Identify focus areas and collect preliminary data.
2. **Planning:** Develop a risk-control matrix and work plan.
3. **Fieldwork:** Gather evidence through interviews and process observations.
4. **Analysis:** Use methods like SWOT or PEST analysis to evaluate findings.
5. **Reporting:** Share findings with management and obtain explanations for observations.
6. **Closure:** Prepare for follow-up audits and ensure action on recommendations.

(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.

---

6. IT Audit Tools

6.1 Computer-Assisted Audit Techniques (CAATs)

- **Usage:** Automate audit processes, analyze data, and validate application controls.
- **Examples:** ACL, IDEA, Excel for data analysis, and regression.

6.2 Integrated Test Facility (ITF) Tally me dummy company open karke entries karna

- **Purpose:** Test application systems using dummy entities to verify processing.
- **Advantages:** Continuous monitoring during regular operations.

6.3 Test Data

- **Method:** Test valid and invalid transactions to evaluate system responses.
- **Applications:** Detect flaws in credit card processing or inventory adjustments.

6.4 Parallel Simulation

- **Concept:** Maintain a copy of production programs to validate processing accuracy.
- **Advantage:** Ensures program logic consistency without disrupting operations.

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

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

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.

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.

CIS - Exception trapping

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.

7. Business Processes – Risks and Controls

7.1 Procure to Pay (P2P)

- **Risks:** Unauthorized changes to supplier data, delayed processing, and inaccurate entries.
- **Controls:** Access restrictions, validation of requisitions, and timely processing.

7.2 Order to Cash (O2C)

- **Risks:** Invalid customer data, unauthorized credit approvals, and incorrect invoicing.
- **Controls:** Credit checks, accurate data transfers, and system-generated reports.

7.3 Inventory Cycle

- **Risks:** Mismanagement of inventory records, delayed updates, and incorrect transactions.

- **Controls:** Regular updates to master files, validation of shipments, and segregation of duties.

7.4 Human Resources

- **Risks:** Unauthorized access, incorrect payroll entries, and outdated master files.
- **Controls:** Restrict access to payroll systems, ensure timely updates, and conduct regular reviews.

7.5 Fixed Assets

- **Risks:** Inaccurate asset records, missed depreciation entries, and unauthorized disposals.
- **Controls:** Validate acquisitions, ensure proper depreciation, and track disposals accurately.

General ledger

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.

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.

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.

CHAPTER 10

UNIT IV: DIGITAL DATA AND ANALYSIS

1. Introduction

- Organizations gather data during operations for effective analysis and decision-making.
- Data analysis transforms raw data into actionable insights, enhancing productivity, HR policies, and expense optimization.

---

2. Data Protection

- **Definition:** Protection of digital data against unauthorized access or loss.
- **Components:**
    - **Data Privacy:** Guidelines for proper data handling and accessibility.

    - **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:** Techniques for preventing unauthorized data access or misuse.
    - **Data Protection Strategies:** Encryption, access control, and multifactor authentication.

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.

---

3. Fair Information Practices

- Principles for ethical data handling:
  - **Collection Limitation:** Standardized and minimal data collection.
  - **Data Quality:** Accurate and relevant data collection.
  - **Purpose Specification:** Clear usage objectives with encryption.
  - **Use Limitation:** Restricted data use through authentication.
  - **Security Safeguards:** Encryption during data storage and transit.
  - **Individual Participation:** Rights to data access, correction, and erasure.
  - **Accountability:** Data handlers ensure these practices are followed.

---

4. Data Security Tools

- **Encryption:** Secures data by converting it into unreadable formats.
- **Firewalls:** Monitors and filters network traffic.
- **Two-Factor Authentication (2FA):** Adds an extra verification step for access.
- **Access Control:** Limits access to authorized personnel.
- **Data Loss Prevention (DLP):** Protects data from unauthorized deletion or copying.

---

5. Data Analysis

- Types of data:
    - **Internal Data:** Business operations and performance metrics.
    - **External Data:** Consumer and market trends.
    - **Qualitative Data:** Non-statistical insights (e.g., interviews, documents).
    - **Quantitative Data:** Measurable data (e.g., surveys, metrics).

Stages of Data Analysis

1. **Requirement Gathering:** Define objectives.
2. **Data Collection:** Identify data sources.
3. **Data Cleaning:** Eliminate irrelevant data.
4. **Data Analysis:** Use techniques like data mining or predictive analytics.
5. **Data Visualization:** Represent data via charts and graphs.

---

6. Data Analysis Tools

- Examples:
    - **Microsoft Power BI:** For visualization and analytics.
    - **Tableau:** For data dashboards.
    - **Python & R:** For programming-based analytics.
    - **KNIME:** Open-source data mining.
    - **MS Excel:** Widely used for basic analysis.

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.

---

7. Data Analytics

- **Definition:** Turning analyzed data into actionable insights.
- **Types:**
    - **Descriptive Analytics:** Summarizes past data.
    - **Diagnostic Analytics:** Explains causes of past events.
    - **Predictive Analytics:** Forecasts future trends.
    - **Prescriptive Analytics:** Recommends actions for specific goals.

---

8. Data Assurance

- Ensures data quality through:
    - **Data Governance:** Managing data standards and policies.
    - **Data Profiling & Matching:** Identifying issues and duplicates.
    - **Data Quality Reporting:** Enforcing rules and monitoring data integrity.
    - **Master Data Management (MDM):** Centralizing key data.
    - **Customer Data Integration:** Consolidating customer data for analytics.

- **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.

9. Information Technology Act, 2000

- Governs cybercrimes, electronic records, and digital signatures.
- Key sections:
    - **Section 43:** Penalties for unauthorized data access.
    - **Section 66:** Punishment for cyber offenses like identity theft.
    - **Section 67:** Penalties for obscene material online.
- 2008 amendments introduced stricter cybersecurity measures and data protection.

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?

- **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.

10. Digital Personal Data Protection Act, 2023

- **Applicability:** Covers all digital personal data in India and data related to services offered in India.
- **Key Features:**
    - **Consent:** Data processed only with individual consent.
    - **Rights:** Access, correction, and erasure of personal data.
    - **Obligations of Data Fiduciaries:** Safeguards to prevent data breaches.
    - **Exemptions:** For government activities and legal obligations.
    - **Data Protection Board:** Ensures compliance and imposes penalties.

Summary of the General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)**, a unified data privacy law across the European Union (EU) and European Economic Area (EEA), focuses on protecting personal data and clarifying rules for organizations handling such data. Below are the key aspects of GDPR:

Objectives of GDPR

- Protect individuals' personal data from unauthorized access, use, or destruction.
- Strengthen individual rights in the digital age.
- Ensure organizations collect and process data responsibly.

Principles of GDPR

1. **Lawfulness, Fairness, and Transparency:**
    - Data must be processed lawfully and transparently, with individuals informed about its purpose.
2. **Purpose Limitation:**
    - Data must be collected for specific, explicit, and legitimate purposes only.
3. **Data Minimization:**
    - Data collection must be limited to what is strictly necessary.
4. **Accuracy:**
    - Data must be kept accurate and up-to-date, with errors corrected promptly.
5. **Storage Limitation:**

    - Personal data should only be stored as long as necessary for its intended purpose.
6. **Integrity and Confidentiality:**
    - Adequate security measures must be taken to protect data from breaches.
7. **Accountability:**
    - Organizations must demonstrate compliance with GDPR by implementing appropriate measures.

GDPR and the European Data Protection Board

- GDPR established the **European Data Protection Board (EDPB)** to ensure consistent application of rules across member states.
- National bodies in European countries are tasked with protecting personal data at the local level.

Similarities Between GDPR and India's Digital Personal Data Protection Act (DPDPA)

- Both laws regulate organizations handling personal data.
- Provisions for reporting data breaches and imposing penalties for non-compliance.
- Data subjects have rights such as access, correction, and deletion of their data.

Differences Between GDPR and DPDPA

1. **Geographical Scope:**
    - GDPR applies to organizations processing data of individuals within the EU, regardless of the organization's location.
    - DPDPA applies to organizations processing personal data within India or offering goods and services to Indian residents.
2. **Scope of Data:**
    - GDPR includes data available publicly and has special categories like racial origin or political views.
    - DPDPA excludes publicly available data and lacks these special categories.
3. **Processing Basis:**

- GDPR includes broader legitimate interests for data processing.
- DPDPA is more consent-centric.

4. **Consent Age:**

    - GDPR allows member states to set the age of consent between 13-16 years.
    - DPDPA sets the age of consent at 18 years, requiring parental consent for minors.

5. **Digitized vs. Non-Digitized Data:**

    - GDPR applies to all personal data, whether digital or non-digital.
    - DPDPA focuses only on digitized personal data.

CHAPTER 11 Business Intelligence

Learning Outcomes

- Understand the concept and functionalities of Business Intelligence (BI).
- Appreciate the usage of BI tools in organizations.

---

1. Introduction

- **Definition:** BI is the process of analyzing raw data to generate insights that inform business decisions.
- **Functions:** Helps businesses understand marketing strategies, financial performance, market trends, and consumer behavior.
- **Modern BI:** Employs advanced tools like dashboards, graphs, and data visualizations to empower decision-making.

---

2. Functionalities of Business Intelligence

1. **Analytics:** Extracts insights from historical and current data using techniques like trend analysis and modeling.
2. **Dashboards:** Displays role-relevant data using visualizations and key performance indicators (KPIs).
3. **Data Mining:** Uses machine learning and statistical tools to find patterns in large datasets.
4. **ETL (Extract, Transform, Load):** Processes raw data into a data warehouse for analysis.
5. **Model Visualization:** Converts raw data into charts, graphs, and other visuals.
6. **OLAP (Online Analytical Processing):** Analyzes multi-dimensional data for tasks like financial forecasting.
7. **Predictive Modeling:** Uses statistical methods to predict trends and outcomes.
8. **Reporting:** Provides comprehensive reports and visualizations for better business understanding.
9. **Scorecards:** Measures KPIs and tracks business progress.
10. **Real-Time Monitoring:** Offers tools to analyze data in real-time for quick decision-making.
11. **Collaborative BI:** Shares insights with stakeholders for team collaboration.
12. **Mobile BI:** Makes BI data accessible on mobile devices.

---

3. Business Intelligence Life Cycle

1. **Analyze Business Requirements:** Identify business needs and required analysis.
2. **Design Data Model:** Create a logical model to represent data relationships.
3. **Design Physical Schema:** Build a schema to define data warehouse structure.
4. **Build Data Warehouse:** Populate the warehouse with structured data.
5. **Create BI Project Structure:** Develop metadata for mapping tables and processes.
6. **Develop BI Objects:** Create dashboards, reports, and metrics for data analysis.
7. **Administer and Maintain:** Continuously monitor and update BI projects.

---

4. Business Intelligence Tools

- BI tools aggregate and analyze data from various sources like CRM systems, ERP systems, and external databases.
- **Advantages:**
    - Centralized data.
    - Automated reporting.
    - Real-time access and easy exports.
    - Compatibility with other systems.
    - Cost reduction and predictive insights.
- **Popular BI Tools:**
    - **Microsoft Power BI:** Integrates with multiple data sources, offers real-time monitoring, and provides predictive analytics.
    - **Tableau:** Known for intuitive data visualization and supports various databases.
    - **QlikSense:** Focuses on self-service analytics and user-friendly interfaces.
    - **Dundas BI:** Flexible and allows independent data analysis.
    - **Sisense:** Simplifies analytics with customizable dashboards.
    - Other tools: SAS Visual Analytics, Zoho Analytics, SAP Business Objects, Google Data Studio.

---

5. Chart Types in Power BI

1. **Line Charts:** Show trends over time.
2. **Bar Charts:** Represent absolute data and can display negative values.
3. **Pie Charts:** Divide data into proportional slices.
4. **Doughnut Charts:** Similar to pie charts but with a hole in the middle.
5. **Funnel Charts:** Visualize data flow through stages.

---

6. Business Intelligence vs Data Analytics

Business Intelligence	Data Analytics
Provides decision-making support.	Modifies raw data into meaningful formats.
Focuses on past data for strategy.	Uses past data for forecasting.
Utilizes structured data.	Uses structured and unstructured data.
Primarily for leadership teams.	For analysts and data scientists.

---

7. Case Studies

- **Heathrow Airport:**
    - Used Microsoft Power BI and Azure for real-time data visualization and operational efficiency.
    - Improved passenger flow and pre-empted potential disruptions.
- **SkullCandy:**
    - Adopted Sisense for data integration and real-time reporting.
    - Improved departmental collaboration and reduced data inaccuracies.

---

8. Benefits of BI in Retail

1. **Improved Customer Experience:** Ensures customer satisfaction at every stage.
2. **Predictive Modeling:** Combines data to identify trends and predict customer preferences.
3. **Price Optimization:** Adjusts prices based on supply, demand, and trends.

Chapter 12 – ABCD of FinTech

Learning Outcomes

After studying this chapter, learners will:

1. Comprehend the ABCD technologies (AI, Blockchain, Cloud Computing, Big Data) used in FinTech.
2. Understand the real-time usage of Artificial Intelligence.
3. Grasp Blockchain concepts in financial institutions.
4. Explore the role of Cloud Computing and Big Data in finance.

12.1 Introduction to FinTech

- **Definition:** FinTech refers to the innovative use of technology in financial services/products like lending, insurance, investment management, and payments.
- **FinTech Segments:**
    1. **Business-to-Consumer (B2C):** Services offered to end consumers.
    2. **Business-to-Business (B2B):** Services designed for businesses.
- **Key Technologies in FinTech:** Artificial Intelligence (AI), Blockchain, Cloud Computing, and Big Data.
- **Examples of FinTech Products:**
    1. Peer-to-Peer (P2P) Lending: Matches lenders and borrowers directly using technology.
    2. Crowdfunding: Raises small amounts from multiple investors via online platforms.
    3. Distributed Ledger Technology (DLT): Decentralized databases where all participants maintain identical copies of shared ledgers (e.g., blockchain).
    4. Robo-Advisors: Algorithm-driven platforms offering financial planning with minimal human intervention.

Objectives and Advantages of FinTech

1. **Objectives:** Simplify financial transactions and provide services efficiently via smartphones.
2. **Why FinTech Over Banks:**
    - Lower fees, better rates, and greater convenience.
    - Advanced technology (e.g., AI and big data) for market analysis and credit scoring.
3. **Trends in FinTech:**

- Growth in digital banking, blockchain adoption, and AI/ML technologies for fraud detection and automation.

12.2 Artificial Intelligence (AI)

- **Definition:** AI involves building smart systems capable of human-like tasks (e.g., speech recognition, decision-making).
- **Applications in Finance:**
  - Robotic Process Automation (RPA) for repetitive tasks like reconciliation.
  - Fraud detection, risk management, and customer satisfaction enhancement.
- **Types of AI:**
  - **Based on Capabilities:**
    1. Weak/Narrow AI: Performs specific tasks (e.g., Siri).
    2. General AI: Mimics human intelligence (currently theoretical).
    3. Super AI: Surpasses human intelligence (hypothetical).
  - **Based on Functionalities:**
    1. Reactive AI: Focuses on current tasks (e.g., chess programs).
    2. Limited Memory AI: Learns from past experiences (e.g., self-driving cars).
    3. Theory-of-Mind AI: Understands emotions (in research).
    4. Self-Aware AI: Machines with consciousness (future concept).

12.3 Blockchain

- **Definition:** A decentralized digital ledger that securely records transactions across a peer-to-peer network.
- **Structure:**
  - **Block:** A record of transactions.
  - **Chain:** Cryptographic linking of blocks.
  - **Network:** Decentralized nodes validating transactions.
- **Types of Blockchain:**
  - Permissioned (Private and Consortium), Permissionless (Public), and Hybrid Blockchain.
- **Applications:**
  - Cryptocurrencies (e.g., Bitcoin).
  - Supply chain management for transparency.
  - Real estate, healthcare, and cross-border payments.

12.4 Cloud Computing

- **Definition:** Delivery of computing resources (e.g., storage, applications) over the Internet.
- **Characteristics:**
    - On-demand self-service, scalability, broad network access, and resource pooling.
- **Service Models:**
    - Software as a Service (SaaS). - software application
    - Platform as a Service (PaaS). - operating system, programming language, database
    - Infrastructure as a Service (IaaS). - hardware
- **Deployment Models:**
    - Private, Public, Hybrid, and Community Clouds.
- **Advantages:**
    - Cost efficiency, flexibility, backup, and global accessibility.
- **Drawbacks:**
    - Internet dependency, security risks, and vendor-specific limitations.

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 quaranteed 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.

12.5 Big Data

- **Definition:** Analysis of massive datasets for insights.
- **Usage in Finance:**
    - Predicting market trends, customer behavior, and fraud prevention.
- **Obstacles:**
    - Complexity, integration challenges, and privacy concerns.

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.

Benefits and Challenges of FinTech

Benefits:

1. Increased speed and efficiency in transactions.
2. Financial inclusion in underserved regions.
3. Improved insights through big data analytics.
4. Resilient systems with distributed ledger technology.

Challenges:

1. Lack of regulatory protections for consumers.
2. Risks of scams, fraud, and data misuse.
3. Exclusion of non-tech-savvy populations.
4. Technical failures disrupting services.

This summary includes all key points and subpoints from the chapter. Let me know if you'd like to delve deeper into any section!

Chapter 13 - Emerging Technologies

Learning Outcomes

1. Understanding **e-business**, its risks, and controls.
2. Comprehending **digital payments** along with their advantages and disadvantages.
3. Exploring paradigms of **Internet of Things (IoT)** and its application in finance and accounting.
4. Gaining knowledge about **quantum computing** and its advantages for financial organizations.
5. Understanding **RegTech** technology and its role.
6. Conceptualizing **mobile computing** and its benefits.

Digital Ecosystem and Controls

1. Introduction

- Emerging technologies like Mobile Computing, Quantum Computing, 3D Printing, and Cloud Computing are transforming work styles and global challenges.
- Technologies are interlinked; e.g., mobile technology integrates with social media for predictive analysis.
- The transition to **technology-based financial transactions** boosts transparency and efficiency.

---

2. Digital Payments

- **Overview**: Digital payment systems revolutionize business transactions, making them easier and safer.

Benefits:

1. **Convenience**: Click-based, secure transactions.
2. **24/7 Accessibility**: Payments anytime, anywhere.
3. **Government Incentives**: Tax discounts for using digital channels.
4. **Log Maintenance**: Automatic recording of transactions.
5. **Low Risk**: MPIN and PIN provide security.
6. **Business Edge**: Increases customer base.
7. **Environmentally Friendly**: Encourages "Green Computing."

Types of Digital Payments:

1. **Unified Payments Interface (UPI)**: Instant transactions via mobile apps, supporting P2P and P2M transfers.
2. **Unstructured Supplementary Service Data (USSD)**: Payments without smartphones or internet.
3. **Aadhar Enabled Payment Services (AEPS)**: Aadhaar-based fund transfers and KYC verification.
4. **Mobile Wallets**: Store payment data securely; cashback and discounts offered.
5. **Immediate Payment Service (IMPS)**: Real-time, 24/7 fund transfer service.
6. **Bharat Interface for Money (BHIM)**: UPI-based app for seamless transactions.
7. **RuPay Cards**: Promotes a cashless economy; includes ATM withdrawal and PoS transactions.
8. **e-RUPI**: QR code or SMS-based digital voucher for specific purposes.

---

3. E-Business

- **Definition**: The sale/purchase of goods and services electronically.
- **Benefits**:
    - Convenience, time-saving, comparison options, and 24/7 accessibility for customers.
    - Increased market reach, reduced costs, and operational efficiency for businesses.
    - Governments benefit through reduced corruption and ecologically friendly practices.
- **Disadvantages**: High startup costs, legal issues, cultural resistance, and security concerns.
- **Risks & Controls**: Address unauthorized access, downtime, data privacy, and compliance through robust policies and disaster recovery plans.

---

4. Emerging Technologies

4.1 Internet of Things (IoT)

- **Definition**: Interconnected devices collect and transmit data over networks.

- **Applications in Finance and Accounting**:

    - **Debt Collection**: Monitors debtor activities via IoT-enabled devices.
    - **Fraud Prevention**: Secures PoS systems using IoT.
    - **Personalized Rewards**: Tailors offers based on consumer behavior.
    - **Capacity Planning**: Optimizes branch and ATM operations.

- **Challenges**:
    - Hardware compatibility, connectivity, and data accuracy issues.
    - Data security concerns.

4.2 Quantum Computing

- **Concept**: Utilizes qubits that exist in multiple states simultaneously, solving complex problems much faster.
- **Advantages**:
    - **Targeting Models**: Better customer insights and fraud detection.
    - **Trading Optimization**: Simulates scenarios for portfolio management.
    - **Risk Profiling**: Faster simulations for risk assessments.
- **Threats**: Quantum computers can potentially break cryptographic protocols.

4.3 RegTech (Regulatory Technology)

- **Definition**: Uses IT to handle compliance, monitoring, and reporting in finance.
- **Advantages**:
    1. Enhances **financial inclusion** through automation.
    2. Detects unfair practices and fraud.
    3. Strengthens **AML** (Anti-Money Laundering) processes.
    4. Tracks illegal phoenixing activities.
    5. Reduces compliance costs.

4.4 Mobile Computing

- **Definition**: The ability to work remotely using mobile devices.
- **Components**:
    - **Mobile Communication**: WLAN, satellite, GSM, etc.
    - **Mobile Hardware**: Smartphones, laptops, and servers.
    - **Mobile Software**: Apps and operating systems (e.g., Android, iOS).
- **Benefits**:
    - Enhances flexibility, productivity, and real-time communication.
    - Improves operational efficiency and customer service.
