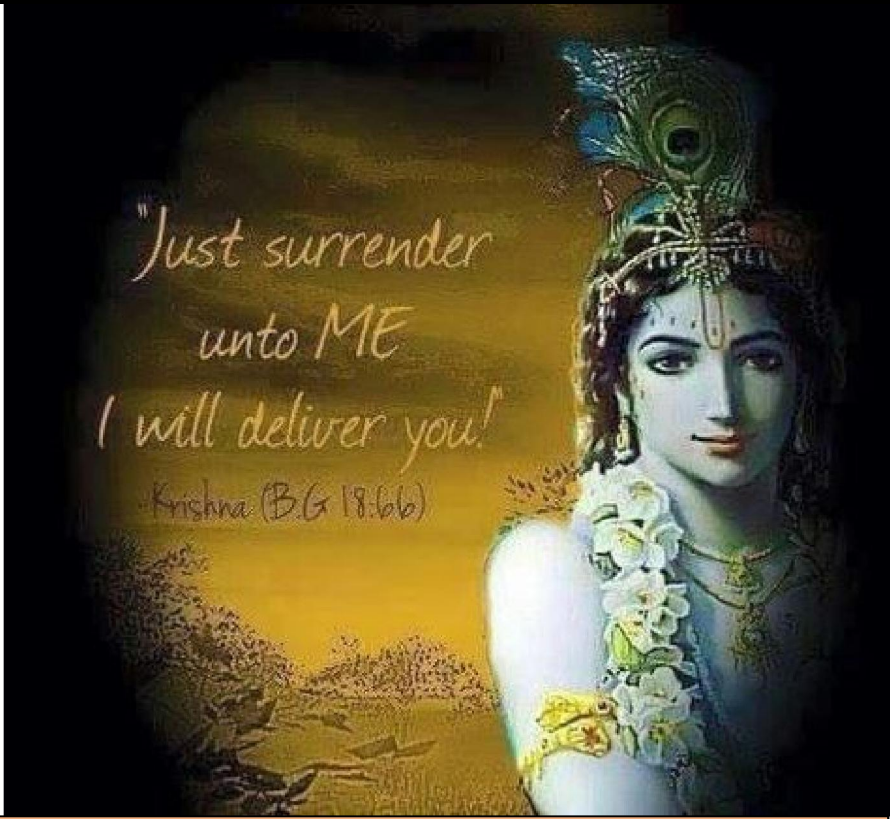
CA FINAL

PAPER 6: INFORMATION SYSTEMS CONTROL & AUDIT(ISCA)

NOTES

(Relevant for **MAY 2020 & NOV 2020** examination)



These Notes have been prepared by ***CA ATUL & AJAY AGARWAL*** (AIR 1 CA FINAL) from ***ICAI Material***. These notes cover Chapter No. "1,4,5,6,8" of Paper 6 ISCA of CA Final Old Course. Author scored **94 marks** in ISCA.

Join us at following links for any guidance and notes:-
•Telegram Channel – air1ca •Youtube – Atul Agarwal •Facebook/ Instagram/ Linkedin – 14atul15

In case of any query/ doubt/ suggestion, students can contact us at following:-
Email – air1icai@gmail.com
Mobile – 9024119090

Best Wishes… Radhe Radhe!!

Contents

Chapter No.	Chapter Name	No. of Pages
1	Concepts of Governance and Management of Information Systems	18
4	Business Continuity Planning and Disaster Recovery Planning	16
5	Acquisition, Development & Implementation of Information Systems	22
6	Auditing of Information System	14
8	Emerging Technologies	19

1

Concepts of Governance and Management of Information Systems

Key Concepts of Governance

Governance: The term "**Governance**" is derived from the Greek verb meaning "to steer". Governance refers to "**all processes of governing, whether undertaken by a government, market or network**. It relates to "the processes of interaction and decision-making. A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives. Governance is a **very general concept** that can refer to all manner of organizations and can be used in different ways.

Enterprise Governance can be defined as: '**The set of responsibilities and exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved,** ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.' Examples include codes on corporate governance and financial reporting standards.

Enterprise Governance has two dimensions: Corporate Governance or Conformance, and Business Governance or Performance

- **Corporate Governance or Conformance: Corporate Governance** is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of **increasing shareholder value by enhancing economic performance**. Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders

  Good corporate governance contributes to **sustainable economic development** by enhancing the performance of companies. Corporate Governance drives the corporate information needs to meet business objectives.

  Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of Audit Committee, risk management and compliance. These are intended to guide companies to achieve their business objectives to meet stakeholder needs without compromising the shareholders' interest. Directors of a Company are accountable to the shareholders for their actions in directing and controlling the business. Corporate governance is thus necessary for the purpose of monitoring and measuring their performance.

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

The conformance dimension is **monitored by the audit committee. However, the performance dimension is the responsibility of the full board.**

Benefits of Governance

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

Corporate Governance and IT Governance

IT Governance is the system by which IT activities in a company or enterprise are directed and to achieve business objectives with the ultimate objective of meeting stakeholder needs.

IT Governance

The **objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT**. IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

Key practices to determine status of IT Governance

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

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

Benefits of IT Governance

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

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

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

Governance of Enterprise IT (GEIT)

Governance of Enterprise IT is a **sub-set of corporate governance** and facilitates implementation of a framework of IS controls within an enterprise and **encompassing all key areas**.

Benefits of GEIT

- It provides a **consistent approach** integrated and aligned with the enterprise governance approach.
- It ensures that **IT-related decisions** are made in line with the enterprise's strategies and objectives.
- It ensures that **IT-related processes are overseen effectively and transparently**.
- It confirms **compliance with legal** and regulatory requirements.
- It ensures that the **governance requirements** for board members are met.

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;
- **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; and

- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT.

Some of the best practices of corporate governance include the following:

- **Clear assignment of responsibilities** and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors;
- **Establishment of a mechanism for the interaction and cooperation** among the board of directors, senior management and the auditors;
- **Implementing strong internal control systems**, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
- **Special monitoring of risk exposures** where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. traders);
- **Financial and managerial incentives** to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- **Appropriate information flows internally and to the public.** For ensuring good corporate governance, the importance of overseeing the various needs to be properly understood, appreciated and implemented.

Enterprise Risk Management (ERM)

"Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity."

Internal Controls

The **(The US Security and Exchange Commission) SEC's** final rules define "Internal Control over financial reporting" as a "process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's Board of Directors, Management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with **generally accepted accounting principles** and includes those policies and procedures that:

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

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

Internal Controls as per COSO

According to COSO, Internal Control is comprised of five interrelated components:

- **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate.
- **Risk Assessment:** This includes the elements that identify and analyze the risks faced by an organisation and the way the risk can be managed.
- **Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded.
- **Information and Communication:** These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.
- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

Role of IT in Enterprises

Enterprises are using IT for strategic and competitive advantage too. IT has not only automated the business processes but also transformed the way business processes are performed. It is important to ensure that IT deployment is oriented towards achievement of business objectives.

Further, restructuring or business process re- engineering may be facilitated through IT deployments. IT could be a key enabler for providing strategic and competitive advantage.

IT Steering Committee

Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. **The key functions of the committee would include of the following:**

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

IT Strategy Planning

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

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources.
- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Classification of Strategic Planning

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

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

- Enterprise Strategic Plan,
- Information Systems Strategic Plan,

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

These aforementioned plans are discussed as follows:

i. **Enterprise Strategic Plan:** Business Planning determines the overall plan of the enterprise. The enterprise strategic plan provides the overall charter under which all units must operate. It is the primary plan prepared by top management of the enterprise.

ii. **Information Systems Strategic Plan:** The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities as well as ensuring its further accomplishment. Some of the enablers of the IS Strategic plan are:
   - Enterprise business strategy,
   - Definition of how IT supports the business objectives,
   - Inventory of technological solutions and current infrastructure,
   - Monitoring the technology markets,
   - Timely feasibility studies and reality checks,
   - Existing systems assessments,
   - Enterprise position on risk, time-to-market, quality, and
   - Need for senior management buy-in, support and critical review.

iii. **Information Systems Requirements Plan:** Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization. Some of the key enablers of the information architecture are as follows:
   - Automated data repository and dictionary,
   - Data syntax rules,
   - Data ownership and criticality/security classification,
   - An information model representing the business, and
   - Enterprise information architectural standards.

iv. **Information Systems Applications and Facilities Plan:** The information systems management can develop an information systems applications and facilities plan. This plan includes:
   - Specific application systems to be developed and an associated time schedule,
   - Hardware and Software acquisition/development schedule,
   - Facilities required, and
   - Organization changes required.

Key Management Practices for Aligning IT Strategy with Enterprise Strategy

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

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, enterprise strategy and future objectives. Consider also the external environment of the enterprise.

- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services.
- **Define the target IT capabilities:** Define the target business and IT capabilities. This should be based on the understanding of the enterprise environment.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets to optimize investment. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co- operation with relevant stakeholders. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives through communication to appropriate stakeholders and users throughout the enterprise.

Business Value from Use of IT

Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost.

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

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

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

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where **expected benefits** realized;
- Percentage of IT enabled investments where **claimed benefits met** or exceeded;
- Percentage of **investment business cases** with clearly defined and approved expected IT related costs and benefits;
- Percentage of IT services with **clearly defined and approved operational costs** and expected benefits; and

- **Satisfaction survey of key stakeholders** regarding the transparency, understanding and accuracy of IT financial information.

Sources of Risk

Some of the common sources of risk are as follows:

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

Broadly, risk has the following characteristics:

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

Related Terms

Various terminologies relating to risk management are given as follows:

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

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

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

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Some examples of vulnerabilities are given as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.

- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.
- Missing safeguards often determine the level of vulnerability.

Vulnerability can be referred as the weakness of the software, which can be exploited by the attackers. Some experts also define 'vulnerability' as opening doors for attackers. Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

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

Threat: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.

Threat has capability to attack on a system with intent to harm. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

Exposure: An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example - loss of business, loss of reputation, violation of privacy and loss of resources etc.

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

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

Basically, it is a set of actions designed to compromise **CIA (Confidentiality, Integrity or Availability**). It is the act of trying to defeat Information Systems (IS) safeguards.

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

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

mechanism should be used.

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

Any risk still remaining after the counter measures are analyzed and implemented is called **Residual Risk**. An organization's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards.

Risk Management Strategies

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

- **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate.
- **Terminate/Eliminate the risk**. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk**. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider
- **Treat/mitigate the risk**. Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back**. Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

Key Governance Practices of Risk Management

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

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

Key Management Practices of Risk Management

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

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

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

Metrics of Risk Management

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

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks

COBIT 5 Business Framework – Governance and Management of Enterprise IT

Control Objectives for Information and Related Technology (COBIT) is a set of best practices for Information Technology management developed by **Information Systems Audit & Control Association (ISACA)** and IT Governance Institute.

COBIT 5 is the only business framework for the governance and management of enterprise Information Technology. This version incorporates the latest thinking in enterprise governance and management techniques. As per COBIT 5, Information is the currency of the 21st century enterprise.

Components in COBIT

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

Benefits of COBIT 5

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

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

Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just five principles. The five key principles for governance and management of enterprise IT in COBIT 5 enable the enterprise to build an effective governance and management framework that optimizes information technology investment and use for the benefit of stakeholders. These principles are discussed below:

- **Principle 1: Meeting Stakeholder Needs:** Enterprises **exist** to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources.
- **Principle 2: Covering the Enterprise End-to-End:** COBIT 5 **integrates** governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function'.
- **Principle 3: Applying a Single Integrated Framework:** There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework.
- **Principle 4: Enabling a Holistic Approach:** Efficient and effective governance and management of enterprise IT require a holistic approach. COBIT 5 defines a set of enablers to support the implementation for GEIT. Enablers are anything that can help to achieve the objectives of the enterprise.
- **Principle 5: Separating Governance from Management:** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

Seven Enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work. Enablers are driven by the goals cascade. The COBIT 5 framework describes seven categories of enablers are discussed as follows:

- **Principles, Policies and Frameworks** are the **vehicle** to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an **organized set** of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT -related goals.
- **Organizational structures** are the **key decision-making** entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.
- **Information** is **pervasive** throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed. Information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are **linked to people** and are required for successful completion of all activities and for making correct decisions and taking corrective actions

Using COBIT 5 Best Practices for GRC

GRC program implementation requires the following:

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

However, specific success of a GRC program can be measured by using the following goals and metrics:

- The reduction of redundant controls and related time to execute (audit, test and remediate);
- The reduction in control failures in all key areas;
- The reduction of expenditure relating to legal, regulatory and review areas;
- Reduction in overall time required for audit for key business areas
- Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
- Improvement in timely reporting of regular compliance issues and remediation measures; and
- Dashboard of overall compliance status and key issues to senior management on a real - time basis as required.

Key Management Practices of IT Compliance

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

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

Key Metrics for Assessing Compliance Process

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

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

Evaluating IT Governance Structure and Practices by Internal Auditors

IT Governance can be evaluated by both external as well internal auditors. Internal audit activities in evaluating the IT governance structure and practices within an enterprise can evaluate several key components that lead to effective IT governance. These are briefly explained here:

- **Leadership:** The following aspects need to be verified by the auditor:
  - Evaluate the relationship between IT objectives and the current needs of the organization.

  - Assess the involvement of IT leadership in the development of the organization's strategic goals.
  - Determine how IT will be measured in helping the organization achieve these goals.
  - Review how roles and responsibilities are assigned within the IT organization.
  - Review the role of senior management and the board in helping strong IT governance.
  - Organizational Structure: The following aspects need to be assessed by the auditor:
  - Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
  - This should include the existence of necessary roles and reporting to meet the needs of the organization. In addition, how IT mirrors the organization should also be included.
- **Processes:** The following aspects need to be checked by the auditor:
  - Evaluate IT process activities and the controls in place to mitigate risks
  - What processes are used by the IT organization to support the IT environment?
- **Risks:** The following aspects need to be reviewed by the auditor:
  - Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks
  - Additionally, determine the accountability that personnel have within risk management.
- **Controls:** The following aspects need to be verified by the auditor:
  - Assess key controls to support the overall organization.
  - Ownership, documentation, and reporting of self-validation aspects should be reviewed.
  - Control set should be robust to address identified risks based on the risk appetite
- **Performance Measurement/Monitoring:** The following aspects need to be verified by the auditor:
  - Evaluate the framework and systems in place to measure and monitor organizational outcomes.

Sample Areas of GRC for Review by Internal Auditors

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

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

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

Sample Areas of Review of Assessing and Managing Risks

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

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

- Risk assessment methodology; and
- Risk action plan and Timely reassessment.

Evaluating and Assessing the System of Internal Controls

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

- **Monitor Internal Controls:** Continuously monitor the IT control environment and control to meet organizational objectives
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including monitoring and test evidence. This provides the business with the assurance of control effectiveness.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through self – assessment.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions and recommendations for improvement relating to external compliance and internal control system residual risks.

4

Business Continuity Planning and Disaster Recovery Planning

Need of Business Continuity Management (BCM)

Business continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities. Let us understand some key terms related to BCM.

- **Business Contingency:** A business contingency is an event with the **potential to disrupt computer operations**, thereby disrupting critical mission and business functions. Such an event could be a **power outage, hardware failure**, fire, or storm. If the event is **very destructive, it is often called a disaster**.
- **BCP Process:** BCP is a process designed to reduce the risk to an enterprise from an **unexpected disruption of its critical functions,** both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations. The purpose of BCP is to ensure that vital business functions are recovered and operationalized within an acceptable timeframe. The purpose is to **ensure continuity of business and not necessarily the continuity of all systems**, computers or networks.
- **Business Continuity Planning (BCP)**: It refers to the **ability of enterprises to recover from a disaster and continue operations with least impact**. It is imperative that every enterprise whether profit-oriented or service-oriented has a business continuity plan. It is not enough that enterprise has a BCP but it is also important to have an **independent audit** of BCP.

BCP Manual

A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. The BCP is expected to provide:

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

The BCP Manual is expected to specify the responsibilities of the BCM team. The BCM Team serves as liasioning teams between the functional area(s) affected and other departments providing support services.

BCM is business-owned, business-driven process that:

- **Proactively improves** an enterprise's resilience to achieve its key objectives;
- **Provides a rehearsed method** of restoring an enterprise ability to supply its key products and services;

- **Delivers a proven capability** to manage a business disruption and protect the enterprise's reputation and brand.

Advantages of Business Continuity

The **advantages of BCM** are that the enterprise:

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

BCM Policy

The **objective** of this policy is to provide a structure through which:

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

The **BCM policy defines** the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability

Business Continuity Planning

Business Continuity Planning (BCP) is the **creation and validation of a practical logistical plan** for how an enterprise will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

Business continuity covers the following areas:

- **Business Resumption Planning:** This is the operation's piece of business continuity planning.
- **Disaster Recovery Planning:** This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses.
- **Crisis Management:** This is the overall co-ordination of an organization's response to a crisis in an effective timely manner.

Objectives and Goals of Business Continuity Planning

The primary objective of a Business Continuity Plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re- establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. **The key objectives of the contingency plan should be to:**

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

Therefore, the goals of the Business Continuity Plan should be to:

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

Developing a Business Continuity Plan

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

- Providing management with a **comprehensive understanding** of the total efforts required to develop and maintain an effective recovery plan;
- Obtaining **commitment** from appropriate management to support and participate in the effort;
- **Defining recovery requirements** from the perspective of business functions;
- **Documenting** the impact of an extended loss to operations and key business functions;
- **Focusing** appropriately on disaster prevention and impact minimization, as well as orderly recovery;
- **Selecting** business continuity teams that ensure the proper balance required for plan development;
- **Developing** a business continuity plan that is understandable, easy to use and maintain; and
- **Defining how business continuity considerations** must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

The **eight phases** are given as follows:

(i) Pre-Planning Activities (Business Continuity Plan Initiation)

(ii) Vulnerability Assessment and General Definition of Requirements

(iii) Business Impact Analysis

(iv) Detailed Definition of Requirements

(v) Plan Development

(vi) Testing Program

(vii) Maintenance Program

(viii) Initial Plan Testing and Plan Implementation

Each of these phases are described below:

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

  During this phase, a **Steering Committee should be established**. The committee should have the overall responsibility for providing direction and guidance to the Project Team.

  Two other key deliverables of this phase are:
  - The **development of a policy** to support the recovery programs; and
  - An **awareness program** to educate management and senior individuals who will be required to participate in the project.

- **Phase 2 – Vulnerability Assessment and General Definition of Requirements:** Security and controls within an organization are continuing concern. It is preferable to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence.

  This phase will include the following key tasks:
  - **A thorough Security Assessment** of the computing and communications environment including personnel practices; physical security; systems development and maintenance; database security; data and voice communications security; software security; insurance; application controls; and personal computers.
  - The **Security Assessment** will enable the project team to **improve any existing emergency plans** and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
  - **Present findings and recommendations** resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
  - **Define** the **scope** of the planning effort.
  - **Analyze**, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
  - **Develop** a Plan Framework.
  - **Assemble** Project Team and conduct awareness sessions.

- **Phase 3 – Business Impact Assessment (BIA):** A Business Impact Assessment

(BIA) of all business units that are part of the business environment enables the project team to:

- identify **critical systems,** processes and functions;
- assess the **economic impact** of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
- Assess the "**pain threshold,"** that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee.

- **Phase 4 – Detailed Definition of Requirements:** During this phase, a profile of recovery requirements is developed.

- **Phase 5 – Plan Development:** During this phase, recovery plans components are defined and plans are documented. Recovery standards are also developed during this phase.

- **Phase 6 – Testing/Exercising Program:** The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established and alternative strategies are evaluated. On-going testing program should be established.

- **Phase 7 – Maintenance Program:** Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environment. Existing change management processes are revised. Where change management does not exist, change management procedures will be recommended and implemented.

- **Phase 8 – Initial Plan Testing and Implementation:** Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made.

Components of BCM Process

- **BCM – Process**

  The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.

- **BCM – Information Collection Process**

  The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them.

- **BCM – Strategy Process**

  Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level within an acceptable timeframe for each product or service.

- **BCM – Development and Implementation Process**

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

- **BCM – Testing and Maintenance Process**

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

- **BCM – Training Process**

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

These components are explained below in detail:

Business Continuity Management Process

➢ Implementing Business Continuity in the Enterprise and Maintenance

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

- Defining the **scope & context**;
- Defining **roles and responsibilities**;
- Engaging and **involving all stakeholders**;
- **Testing** of program on regular basis;
- **Maintaining the currency** & appropriateness of business continuity program;
- Managing **costs and benefits** associated; and
- **Convert** policies and strategies into action.

➢ BCM Documentation and Records

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

- The business continuity policy;
- The business continuity management system;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.

BCM records should be retained for a minimum period of 1 year. Retention is a statutory, regulatory or customer requirement.

BCM Information Collection Process

In order to design an effective BCM, it is pertinent to understand the enterprise from all perspectives of interdependencies of its activities, external enterprises and including:

- **enterprise's objectives,** stakeholder obligations, statutory duties and the environment in which the enterprise operates;
- **activities**, **assets and resources** that support the delivery of these products and services;
- **impact and consequences** over time of the failure of these activities, assets and resources; and
- **Perceived threats** that could disrupt the enterprise's key products and services and the activities, assets and resources that support them.

The pre-planning phase of Developing the BCP also involves collection of information.

Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions and assess the "pain threshold, "that is, the length of time business units can survive without access to the system, services and facilities. **For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:**

- **assess the impacts** that would occur if the activity was disrupted over a period of time;
- identify the **maximum time period** after the start of a disruption within which the activity needs to be resumed;
- Identify **critical business processes**;
- assess the **minimum level** at which the activity needs to be performed on its resumption;
- identify the **length of time** within which normal levels of operation need to be resumed; and
- Identify any **inter-dependent activities**, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

BCM Testing and Maintenance Process

Various aspects of BCM Testing and Maintenance Process are given as follows:

➢ **BCM Testing**

An exercise program should leads to objective assurance that the BCP will work as anticipated when required. In addition, it might lead to the improvement of BCM capability by:

- **Practicing** the enterprise's ability to recover from an incident;
- **Verifying** that the BCP incorporates all activities and their priorities;
- **Highlighting assumptions**, which need to be questioned;
- **Instilling confidence** amongst exercise participants;
- **Raising awareness** of business continuity throughout the enterprise by

publicizing the exercise;

- **Validating the effectiveness** and timeliness of restoration of critical activities; and
- **Demonstrating competence** of the primary response teams and their alternatives.

In case of Development of BCP, the objectives of performing BCP tests are to ensure that:

- The **recovery procedures** are complete and workable.
- The **competence** of personnel in their performance of recovery procedures can be evaluated.
- There **sources** such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- The **manual recovery procedures** and IT backup system/s are current and can either be operational or restored.
- The **success or failure** of the business continuity training program is monitored.

➢ BCM Maintenance

The maintenance tasks undertaken in Development of BCP are to:

- Determine the **ownership** and responsibility for maintaining the various BCP strategies within the enterprise;
- Identify the **BCP maintenance triggers** to ensure that any organizational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date;
- Determine the **maintenance regime** to ensure the plan remains up-to-date;
- Determine the **maintenance processes** to update the plan; and
- Implement **version control procedures** to ensure that the plan is maintained up-to-date.

➢ Reviewing BCM Arrangements

An audit or self-assessment of the enterprise's BCM program should verify that:

- **All key products and services** and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- The **enterprise's BCM policy, strategies, framework** and plans accurately reflect its priorities and;
- The **enterprise' BCM competence and its BCM capability** are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- The **enterprise's BCM solutions are effective**, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
- The **enterprise's BCM maintenance and exercising programs** have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;

- The enterprise has an **ongoing program for BCM training** and awareness;
- BCM procedures have been **effectively communicated** to relevant staff, and that those staff understand their roles and responsibilities; and
- **Change control processes** are in place and operate effectively.

BCM Training Process

Awareness and Competency

While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined. These are consistent with the **competencies** required by the organization of the relevant role and are given as follows:

- **Actively listens to others**, their ideas, views and opinions;
- **Provides support** in difficult or challenging circumstances;
- **Responds constructively** to difficult circumstances;
- **Adapts leadership style** appropriately to match the circumstances;
- **Promotes a positive culture** of health, safety and the environment;
- Recognizes and acknowledges the **contribution of colleagues**;
- Encourages the taking of **calculated risks**;
- Encourages and actively responds to **new ideas**;
- Consults and **involves team members** to resolve problems;
- Demonstrates **personal integrity**; and
- **Challenges established ways** of doing things to identify improvement opportunities.

Types of Plans

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

Emergency Plan

The emergency plan specifies the **actions to be undertaken immediately when a disaster occurs**. Management must identify those situations that require the plan to be invoked e.g., **major fire, major structural damage**, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs.

When the situations that evoke the plan have been identified, **four aspects of the emergency plan must be articulated**. First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

Back-up Plan

The backup plan **specifies the type of backup to be kept**, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system.

The **backup plan needs continuous updating as changes occur**. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly. Indeed, it is prudent to have more than one person knowledgeable in a backup task in case someone is injured when a disaster occurs.

- ### Recovery Plan

The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans **set out procedures to restore full information system** capabilities. **Recovery plan should identify a recovery committee** that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first.

Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organization, **new members must be appointed immediately** and briefed about their responsibilities.

- ### Test Plan

The **final component of a disaster recovery plan is a test plan**. The purpose of the test plan is to **identify deficiencies in the emergency, backup, or recovery plans** or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. **Periodically, test plans must be invoked.** Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, **a phased approach can be adopted**. First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs. Next, a disaster can be simulated at a convenient time -for example, during a slow period in the day. Anyone, who will be affected by the test (e.g. personnel and customers) also, might be given prior notice of the test so they are prepared. Finally, disasters could be simulated without warning at any time. These are the acid tests of the organization’s ability to recover from a catastrophe.

Types of Back-ups

When the back-ups are taken of the system and data together, they are called total system’s back-up. Various types of back-ups are given as follows:

(i) **Full Backup:** A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed.

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

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

Advantages

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

Disadvantages

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

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

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

Advantages

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

Disadvantages

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

(iii) **Differential Backup:** Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

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

Advantages

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

Disadvantages

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

(iv) **Mirror back-up:** Mirror backups are, as the name suggests, a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup.

Further, a mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

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

Advantages

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

Disadvantages

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

Alternate Processing Facility Arrangements

Security administrators should consider the following backup options:

- **Cold Site:** If an organization 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 organization can establish its own cold-site facility or enter into an agreement with another organization to provide a cold-site facility.
- **Hot Site:** If fast recovery is critical, an organization 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 organizations 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 organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

- how **soon the site** will be made available subsequent to a disaster;
- the **number of organizations** that will be allowed to use the site concurrently in the event of a disaster;
- the **priority** to be given to concurrent users of the site in the event of a common disaster ;
- the **period** during which the site can be used;
- the **conditions** under which the site can be used;
- the **facilities and services** the site provider agrees to make available;
- What **controls will be in place** and working at the off-site facility.

These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

Disaster Recovery Procedural Plan

The disaster recovery planning document may include the following areas:

- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liasioning

with appropriate public authorities e.g. police, fire, services and local government.

- Fallback procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
- Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back -up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.
- Primary computer centre hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

Audit of the BCP/DRP

Sample list of BCP Audit steps are given below:

(i) **Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:**

- Identification and prioritization of the activities, which are essential to continue functioning.
- The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.

- Operations managers and key employees participated in the development of the plan.
- The plan identifies the resources that will likely be needed for recovery and the location of their availability.
- The plan is simple and easily understood so that it will be effective when it is needed.
- The plan is realistic in its assumptions.

(ii) Interview **functional area managers or key employees** to determine their understanding of the disaster recovery/ business resumption plan. Do they have a clear understanding of their role in working towards the resumption of normal operations?

- Does the disaster recovery/ business resumption plan include provisions for Personnel?
- Have key employees seen the plan and are all employees aware that there is such a plan? Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?
- Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?
- Does the disaster recovery/ business resumption plan include provisions for people with special needs?
- Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?

(iii) **Building, Utilities and Transportation**

- Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?
- Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
- Review any agreements for use of backup facilities.
- Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
- Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested?
- Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

(iv) **Information Technology**

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.

- Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications?
- Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.

5

Acquisition, Development and Implementation of Information Systems

Business Process Design

Business process design means structuring or restructuring the tasks, functionalities and activities for improvising a business system. Business process design involves a sequence of the steps as follows:

- **Present Process Documentation**
- **Proposed Process Documentation**
- **Implementation of New Process**

System Development

Systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods. System development has **two major components** described briefly as follows:

- **System Analysis** is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.
- **System Design** is the process of planning and structuring a new business system or to replace or complement an existing system.

Achieving System Development Objectives

Achieving the objectives of the system development is essential but many times, such objectives are not achieved as desired. **An analysis on 'why organizations fail to achieve their systems development objectives' reveals bottlenecks.** Some of the most notable ones are described briefly as follows:

(i) **User Related Issues:** It refers to those issues where user is reckoned as the primary agent. *Some of the aspects with regard to this problem are mentioned as follows:*

- **Shifting User Needs:** User requirements for IT are constantly changing. *When these changes occur during a development process*, the development team faces the challenge of developing systems.
- **Resistance to Change:** People have a natural tendency to resist change, changes - often radical - in the Workplace. Development project is doomed to failure.
- **Lack of Users' Participation**: Users must participate in the development efforts to resolve development problems. User participation also helps to reduce user resistance to change.
- **Inadequate Testing and User Training:** New systems must be tested before installation. Users must be trained to effectively utilize the new system.

(ii) **Developer Related Issues**: It refers to the issues and challenges with regard to the developers. *Some of the critical bottlenecks are mentioned as follows:*

- **Lack of Standard Project Management and System Development Methodologies:** Some organizations do not formalize their project management and system development methodologies, making it very difficult to complete projects on time or within budget.
- **Overworked or Under-Trained Development Staff:** System developers often lack sufficient educational background and skills. Furthermore, training plan and training budget do not exist.

(iii) **Management Related Issues:** It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals. *Some of such bottlenecks are mentioned as follows:*

- **Lack of Senior Management Support and Involvement:** Developers and users of information systems watch senior management to determine 'which systems development projects are important'.
- **Development of Strategic Systems:** Because strategic decision making is unstructured, objectives are difficult to define.

(iv) **New Technologies:** When an organization tries to create a competitive advantage by applying advance technologies, attaining system development objectives is more difficult because personnel are not as familiar with the technology.

System Development Team

Several people in the organization are responsible for systems development. A project management team generally consists of both computer professionals and key users.

Accountants' Involvement in Development Work

An accountant can help in various related aspects during system development; some of them are as follows:

(i) **Return on Investment (referred as ROI):** This defines the return, an entity shall earn on a particular investment i.e. capital expenditure. This financial data is a prime consideration for any capital expenditure entity decides to incur. For this analysis following data needs to be generated.

(a) **Cost:** This includes estimates for typical costs involved in the development, which are given as follows:

- ***Development Costs:*** Development Costs for a CBIS include costs of the system development process, like salaries of developers.
- ***Operating Costs:*** Operating Costs of a CBIS including hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.
- ***Intangible Costs:*** Intangible Cost that cannot be easily measured. For example, the development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale.

(b) **Benefits:** The benefits, which result from developing new or improved information systems that can be subdivided into tangible and intangible benefits.

(ii) **Computing Cost of IT Implementation and Cost Benefit Analysis:** For analysis of ROI, accountants need the costs and returns.

(iii) **Skills expected from an Accountant:** An accountant must possess skills to understand the system development efforts and nuances of the same.

Systems Development Methodology

A **System Development Methodology** is a formalized, standardized, well-organized and documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. **The methodology is characterized by the following:**

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

Waterfall Model

The waterfall approach is a **traditional development approach** in which each phase is carried in sequence or linear fashion. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release.

Some of the **key characteristics** are the following:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation.

(a) **Strengths:** Major strengths are given as follows:

- It is ideal for **supporting less experienced** project teams and project managers.
- The **orderly sequence** helps to ensure the quality, reliability, adequacy and maintainability of the developed software.
- **Progress** of system development is measurable.
- It enables to **conserve resources**.

(b) **Weaknesses:** Weaknesses including the following:

- **Written specifications** are often difficult for users to read and thoroughly appreciate.
- It leads to **excessive documentation**, whose updation to assure integrity is an uphill task and often time-consuming.

- It promotes the **gap** between users and developers with clear vision of responsibility.
- It is difficult to **respond to changes** occur in the life cycle, it proves costly.
- It is criticized to be **inflexible**, slow, costly, and cumbersome due to significant structure and tight controls.
- There is a little to **iterate**, which may be essential in situations.
- **Problems** are often not discovered until system testing.
- It depends upon **early identification** and specification of requirements.
- **System performance** cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.

The Prototyping Model

The **goal** of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a **usable system** or system component that is built quickly and at a lesser cost, and with the intention of modifying or even replacing it by a full -scale and fully operational system. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Prototyping can be viewed as a series of four steps. **The generic phases of this model are explained as follows:**

- **Identify Information System Requirements:** In traditional approach, the system requirements are to be identified before the development process starts. Under prototype approach, the design team needs only fundamental system requirements to build the initial prototype.
- **Develop the Initial Prototype:** The designers create an initial base model and give little or no consideration to internal controls, but emphasize system characteristics such as simplicity, flexibility, and ease of use. These characteristics enable users to interact with tentative versions.
- **Test and Revise:** After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and ask users to record their likes and dislikes and recommend changes.
- **Obtain User Signoff of the Approved Prototype:** Users formally approve the final version of the prototype and establishes a contractual obligation. Prototyping is not commonly used for developing traditional applications.

(a) **Strengths:** Some of its strengths identified by the experts and practitioners include the following:

- It helps to **easily identify,** difficult functions and missing functionality.
- It provides for **quick implementation** of an incomplete, but functional, application.
- It is especially useful for resolving **unclear objectives**.
- It encourages **innovation** and flexible designs.
- **Potential** exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- **Errors** are hopefully detected and eliminated early in the developmental process. Information system should be more reliable and less costly to develop.
- A very **short time period** is normally required to develop and start experimenting with a prototype.

- It typically results in a **better definition** of these users' needs and requirements than does the traditional systems development approach.
- It improves both **user participation** in system development and communication among project stakeholders.
- It enables to **generate specifications** for a production application.

(b) **Weaknesses:** Some of the weaknesses identified by the experts include the following:

- **Approval** process and control are not strict.
- Incomplete or inadequate **problem analysis** may occur.
- **Requirements** may frequently change significantly.
- Identification of **non-functional elements** is difficult to document.
- **Designers** may prototype too quickly resulting in an inflexible design.
- Prototype may not have **sufficient checks** and balances incorporated.
- Prototyping can only be successful if the system users are willing to **devote significant time** in experimenting with the prototype. Users may not be able or willing to spend the amount of time required.
- The **interactive process** of prototyping causes the prototype to be experimented with quite extensively. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
- Prototyping may cause **behavioral problems** with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands as well as impatience by users when too many interactions.

The Incremental Model

The Incremental model is a method of software development where the **model is designed, implemented and tested incrementally** 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 Figure.

A few pertinent **features** are listed as follows:

- A series of **mini-waterfalls** are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.
- **Overall requirements** are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.
- The **initial software concept** and system core are defined using the Waterfall approach, followed by iterative Prototyping.

(a) **Strengths:** Some of its strengths identified by the experts and practitioners include the following:

- **Potential** exists for exploiting knowledge gained in an early increment as later increments are developed.
- **Moderate control** is maintained over the life of the project through the use of written documentation.
- Stakeholders can be given **concrete evidence** of project status throughout the life cycle.

- It is **more flexible** and less costly to change scope and requirements.
- It helps to **mitigate integration** and architectural risks earlier in the project.
- It allows the **delivery of a series** of implementations that are gradually more complete.
- **Gradual implementation** provides the ability to monitor the effect of incremental changes and make adjustments before the organization is negatively impacted.

(b) **Weaknesses:** Some of the weaknesses identified by the experts include the following:

- **When utilizing** a series of mini-waterfalls, there is usually a lack of overall consideration of the business problem for the overall system.
- Each phase of an iteration is **rigid** and do not overlap each other.
- Since some modules will be completed much earlier than others, **well-defined interfaces** are required.
- It is difficult to demonstrate **early success** to management.

Spiral Model

The Spiral model is a software development process **combining elements of both design and prototyping-in-stages.** It tries to combine advantages of top-down and bottom-up concepts. It combines the features of the prototyping model and the waterfall model (given in Figure). The spiral model is intended for large, expensive and complicated projects. **Game development** is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects. A list of pertinent characterizing **features** includes the following:

- The **new system requirements** are defined in as much detail as possible. This usually involves interviewing a number of users.
- A **preliminary design** is created for the new system. This phase is the most important part of "Spiral Model" in which all possible alternatives are analyzed. This phase has been added specially in order to identify and resolve all the possible risks in the project development.
- A **first prototype** of the new system in constructed from the preliminary design. This is usually a scaled- down system.
- A **second prototype** is evolved by a fourfold procedure by evaluating the first prototype in terms of its strengths, weaknesses, and risks.

(a) **Strengths:** Some of its strengths identified by the experts and practitioners include the following:

- It enhances the **risk avoidance**.
- It is useful in helping for **optimal development** of a given software iteration based on project risk.
- It can **incorporate** Waterfall, Prototyping, and Incremental methodologies in the framework, and provide guidance as to which combination of these models best fits a given software iteration, based upon the type of project risk.

(b) **Weaknesses:** Some of the weaknesses identified by the experts include the following:

- It is challenging to determine the **exact composition** of development methodologies to use for each iteration around the Spiral.
- It may prove **highly customized** to each project, and thus is quite complex and

limits reusability.

- A **skilled and experienced project manager** is required to determine how to apply it to any given project.
- **No established controls** exist for moving from one cycle to another cycle.
- There are **no firm deadlines**, leading to inherent risk of not meeting budget or schedule.

Rapid Application Development (RAD) Model

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

- Key emphasis is on fulfilling the business need.
- Project control involves prioritizing development and defining delivery deadlines or "timeboxes."
- Generally includes Joint Application Development (JAD).
- Active user involvement is imperative.
- Produces documentation necessary to facilitate future development and maintenance.

(a) **Strengths:** Some of the strengths identified by the experts and practitioners include the following:

- The **operational version** of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks.
- RAD tends to produce systems at **lower cost**.
- Quick **initial reviews** are possible.
- It holds a **great level of commitment** from stakeholders than Waterfall, Incremental, or spiral frameworks.
- It **concentrates** on essential system elements from user viewpoint.
- It provides for the ability to **rapidly change system design** as demanded by users.
- It leads to a **tighter fit** between user requirements and system specifications.

(b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:

- Fast speed and lower cost may affect adversely the **system quality**.
- The project may end up with **more requirements** than needed (gold-plating).
- It may lead to **inconsistent designs** within and across systems.
- It may call for **violation of programming standards** related to inconsistent documentation.
- It may call for **lack of attention** to later system administration needs
- **Formal reviews** and audits are more difficult to implement than for a complete system.
- Since some modules will be completed much earlier than others, **well–defined interfaces** are required.

Agile Model

This is an **organized set** of software development methodologies **based on the iterative and incremental development**, where requirements and solutions evolve through collaboration between self- organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle. Agile Manifesto is based on following **12 features**:

- Customer satisfaction by rapid delivery of useful software;
- Welcome changing requirements, even late in development;
- Working software is delivered frequently (weeks rather than months);
- Working software is the principal measure of progress;
- Sustainable development, able to maintain a constant pace;
- Close, daily co-operation between business people and developers;
- Face-to-face conversation is the best form of communication (co-location);
- Projects are built around motivated individuals, who should be trusted;
- Continuous attention to technical excellence and good design;
- Simplicity;
- Self-organizing teams; and
- Regular adaptation to changing circumstances.

(a) **Strengths:** Some of the strengths identified by the experts and practitioners include the following:

- Agile methodology has the concept of an **adaptive team**, which enables to respond to the changing requirements.
- The **team does not have to invest time** and efforts and finally find that by the time.
- **Face to face communication** from customer representative leaves a little space for guesswork.
- The documentation is **crisp** and to the point to save time.
- The **end result** is generally the high quality software in least possible time duration and satisfied customer.

(b) **Weaknesses:** Some of the weaknesses identified by the experts and practitioners include the following:

- In case of some software deliverables, especially the large ones, it is **difficult to assess the efforts**
- required at the beginning of the software development life cycle.
- There is **lack of emphasis** on necessary designing and documentation.
- Agile **increases potential threats** to business continuity and knowledge transfer.
- Agile requires more **re-work** and due to the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects.
- The project can easily get **taken off track** if the customer representative is not clear about the final outcome.
- Agile **lacks the attention** to outside integration.

System Development Life Cycle (SDLC)

The System Development Life Cycle provides system designers and developers to follow a sequence of activities. **It consists of a generic sequence of steps or phases in which each phase of the SDLC uses the results of the previous one.** The SDLC is document driven, which means that at crucial stages, the processes documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. **A deliverable may be a substantial written document**, a software artifact, a system test plan or even a physical object such as a new piece of technology that has been ordered and delivered.

The advantages of this system are given as follows:

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

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

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

Some of the shortcomings and anticipated risks associated with the SDLC are as follows:

- The development team may find it **cumbersome.**
- The users may find that the end product is **not visible for a long time.**
- The rigidity of the approach may **prolong the duration of many projects.**
- It may **not be suitable for small and medium sized projects.**

Preliminary Investigation

A preliminary investigation is normally initiated by some sort of system request. **Thereby, it largely enables the requirements engineer to tackle the issues and Feasibility Study for the following:**

- Determine whether the **solution** is as per the business strategy;
- Determine whether the **existing system can rectify** the situation without a major modification;
- Define the **time frame** for which the solution is required;
- Determine the approximate **cost** to develop the system; and
- Determine whether the **vendor product** offers solution to the problem.

(i) **Identification of Problem:** The first step in an application development is to define the problem clearly and precisely, which is done only after the critical study of the existing system and several rounds of discussions with the user group.

(ii) **Identification of Objectives:** After the identification of the problem, it is easy to work out and precisely specify the objectives of the proposed solution.

(iii) **Delineation of Scope:** The scope of a solution defines its typical boundaries. It should be clear and comprehensible to the user management stating the extent 'what will be addressed by the solution and what will not'.

The typical scope determination may be performed on the following dimensions:

- **Functionality Requirements:** What functionalities will be delivered through solution?
- **Data to be Processed:** What data is required to achieve these functionalities?
- **Control Requirements:** What are the control requirements for this application?
- **Performance Requirements:** What level of response time and throughput is required?
- **Constraints:** What are the conditions the input data has to conform to?
- **Interfaces:** Is there any special hardware/software that the application has to interface with? For example-Payroll application.
- **Reliability requirements:** Reliability of an application is measured by its ability to remain uncorrupted and probability of failure-free operations.

Moreover, while eliciting information to delineate the scope; few aspects need to be kept in mind:

- **Different users may represent the problem and required solution in different ways**. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project.
- While the **initiator of the project may be a member of the senior management**, the actual users may be from the operating levels in an organization.
- While presenting the **proposed solution for a problem**, the development organization has to clearly quantify the economic benefits to the user organization. For example, when a system is proposed for Road tax collection.
- It is **also necessary to understand the impact of the solution** on the organization. Wide impact met with greater resistance. ERP implementation is a classic example.
- While **economic benefit** is a critical consideration when deciding on a solution, there are several other factors that have to be given weightage too.

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

- **Reviewing Internal Documents:** The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal. Analysts can usually learn these details by examining organization charts.

- **Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it.

  Usually, preliminary investigation interviews involve only management and supervisory personnel.

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

The Feasibility Study of a system is evaluated under following dimensions described briefly as follows:

- **Technical:** Is the technology needed available?
- **Financial:** Is the solution viable financially?
- **Economic:** Return on Investment?
- **Schedule/Time:** Can the system be delivered on time?
- **Resources:** Are human resources reluctant for the solution?
- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any adverse effect on quality of work life?
- **Legal:** Is the solution valid in legal terms?

System Requirements Analysis

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

The following objectives are performed in this phase in order to generate the deliverable, Systems Requirements Specification (SRS):

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

In order to accomplish the aforementioned objectives, a series of steps are taken. A generic set of process are described as follows:

(i) **Fact Finding:** Every system is built to meet some set of needs, for example, the need of the organization for lower operational costs, better information for managers, smooth operations for users or better levels of services to customers.

Various fact-finding techniques/tools are used by the system analyst for determining these needs/requirements are briefly discussed below:

- **Documents:** Document means manuals, input forms, output forms, diagrams, organization charts, job descriptions, procedure manuals etc. Documents are a very good source of information.
- **Questionnaires:** Users and managers are asked to complete questionnaire about the information systems. The main strength of questionnaires is that a large amount of data can be collected quickly.
- **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews provide picture of the problems and opportunities. Interviews also give analyst the opportunity to observe and record first-hand user reaction.
- **Observation:** In prototyping approaches, observation plays a central role in requirement analysis. Only by observing, the system can be successfully developed.

(ii) **Analysis of the Present System:** Detailed **investigation of the present system** involves collecting, organizing and evaluating facts about the system and the environment in which it operates. The following areas should be studied in depth:

- **Reviewing Historical Aspects:** A brief history of the organization is a logical starting point for an analysis of the present system.
- **Analyzing Inputs:** A detailed analysis of present inputs is important since they are basic to the manipulation of data.
- **Reviewing Data Files:** The analyst should investigate the data files maintained by each department, noting their number and size.
- **Reviewing Methods, Procedures and Data Communications:** Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished.
- **Analyzing Outputs:** The outputs or reports should be scrutinized carefully by the system analysts to determine 'how well they will meet organization's needs.
- **Reviewing Internal Controls:** A detailed investigation of the present information system is not complete until internal control mechanism is reviewed..
- **Modeling the Existing System:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner.
- **Undertaking Overall Analysis of the Existing system:** The final phase of the detailed investigation includes the analysis of the present work volume.

(iii) **System Analysis of Proposed Systems:** After a thorough analysis of each functional area of the present information system, the proposed system specifications must be clearly defined. **The required systems specifications should be in conformity with the project's objectives articulated and in accordance with the following:**

- **Outputs are produced with great emphasis** on timely managerial reports that utilize the management by exception' principle.
- **Databases are maintained with great accent** on online processing capabilities.
- **Input data is prepared directly from original source documents** for processing by the computer system.
- **Methods and procedures that show the relationship of inputs and outputs** to the database, utilize data communications as, when and where **deemed appropriate**.
- **Work volumes and timings are carefully considered** for present and future periods including peak periods.

(iv) **System Development Tools:** Many tools and techniques have been developed to improve current information systems and to develop new ones.

A set of the prominent tools have been already mentioned categorically and some are being described in detail as follows:

(a) **Structured English:** Structured English, also known as Program Design Language (PDL), is the use of the English language with the syntax of structured programming. Thus, Structured English aims at getting the benefits of both the programming logic and natural language.

(b) **Flowcharts:** Flowcharting is a pictorial representation technique that can be used by analysts to represent the inputs, outputs and processes of a business process.

(c) **Data Flow Diagrams:** A Data Flow Diagram uses few simple symbols to illustrate the flow of data among external entities.

Data Flow Diagram Symbols

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

(d) **Decision Tree:** A Decision Tree or tree diagram is a support tool that uses a tree-like graph or model of decisions including chance event outcomes, resource costs, and utility. Decision tree is commonly used in operations research.

(e) **Decision Table:** A Decision Table is a table, which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency. The four parts of the decision table are given as follows:

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

(f) **CASE Tools:** CASE refers to the automation of anything that humans do to develop systems and support virtually all phases of traditional system development process. For example, these packages can be used to create complete and consistent requirements specifications with specifications languages.

(g) **System Components Matrix:** A System Component Matrix provides a matrix framework to document the resources used and the information produced by an information system. It can be used for both systems analysis and system design.

(h) **Data Dictionary:** A data dictionary contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system.

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help to establish an audit trail.

(i) **User Interface Layout and Forms:** Several type layout forms for both soft and hard copy are used to model components of an automated information system. Some of the prominent and inevitable ones are described briefly as follows:

- **Layout form and Screen Generator:** These are for printed report used to format or "paint" the desired layouts.
- **Menu Generator:** Menu generator outlines the functions, which the system is aimed to accomplish.
- **Report Generator:** Report generator has capacity of performing similar functions to screen generators.
- **Code Generator:** Code generator allows the analyst to generate modular units of source code and play significant role in systems development process.

(v) **Systems Specification:** At the end of the analysis phase, the systems analyst prepares a document called **Systems Requirement Specifications (SRS)**. **A well documented SRS may normally contains the following sections:**

- **Introduction:** Goals, Objectives, Scope and Environment of the computer-based system.
- **Information Description:** Problem description; Information content, Hardware, software, human interfaces for external system elements and internal software functions.
- **Functional Description:** Diagrammatic representation of functions; processing narrative for each function; Interplay among functions; Design constraints.
- **Behavioral Description:** Response to external events and internal controls.
- **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.

- **Appendices:** Data flow Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review:** The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.

(vi) **Roles Involved in SDLC:** A variety of tasks during the SDLC are performed by special teams/committees/individuals based on requisite expertise as well as skills. Some of the generic roles are described as follows:

(a) **Steering Committee:** It is a special high power committee of experts to accord approvals for go-ahead and implementations.

(b) **Project Manager:** A project manager is normally responsible for more than one project. He is responsible for delivery of the project deliverables within the time and periodically reviews the progress of the project with the project leader.

(c) **Project Leader:** The project leader is dedicated to a project, which has to ensure its completion and fulfillment of objectives. He reviews the project status more frequently than a Project Manager.

(d) **Systems Analyst / Business Analyst:** The systems analysts' main responsibility is to conduct interviews with users and understand their requirements. He is a link between the users and the designers and plays a pivotal role in the Requirements analysis and Design phase.

(e) **Module Leader/Team Leader:** A project is divided into several manageable modules, and the development responsibility for each module is assigned to Module Leaders. For example, while developing a **financial accounting** application. Module leaders are responsible for the delivery of tested modules within the stipulated time and cost.

(f) **Programmer/Developers:** Programmers is a mason of the software industry, who converts design into programs by using programming language. They also test the program to assure correctness and reliability.

(g) **Database Administrator:** The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team

(h) **Quality Assurance:** This team sets the standards for development, and checks compliance with these standards on a periodic basis.

(i) **Testers:** Testers are junior level quality assurance personnel who test programs and subprograms and prepare test reports.

(j) **Domain Specialist:** Whenever a project team has to develop an application in a field that's new to them, they take the help of a domain specialist. For example, if a team undertakes application development in **Insurance,** they may seek the assistance of an **Insurance expert.** A domain specialist need not have knowledge of software systems.

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

System Designing

The design phase activities includes Architectural Design; Design of the Data/Information Flow; Design of the Database; Design of the User-interface; Physical Design; and Design and acquisition of the hardware/system software platform', which are described briefly as follows:

(a) **Architectural Design:** Architectural design deals with the organization of applications in terms of hierarchy of modules and sub-modules. At this stage, we identify major modules; functions and scope of each module; interface features of each module. It has three elements – Module, Connection, and Couple.

(b) **Design of Data/Information flow:** The design of the data and information flow is a major step in the conceptual design of the new system. In designing the data / information flow for the proposed system, the inputs that are required are - existing data / information flows, problems with the present system, and

objective of the new system.

(c) **Design of Database:** Design of the database involves determining its scope ranging from local to global structure. The scope is decided on the basis of interdependence among organizational units**. The design of the database involves four major activities, which are shown in Table 5.5.5**

Table 5.5.5: Major Activities in Database Designing

Design Activity	**Explanation**
Conceptual Modeling	These describe the application domain via entities, attributes of these entities and dynamic constraints on these entities and their relationships.
Data Modeling	Conceptual Models need to be translated into data models so that they can be manipulated by both high-level and low-level programming languages.
Storage Structure Design	Decisions must be made on how to linearize and partition data structure so that it can be stored on some device.
Physical Layout Design	Decisions must be made on how to distribute the storage structure across specific storage media and locations.

System Acquisition

(a) **Acquisition Standards: Acquisition standards should focus on the following:**

- Ensuring **security, reliability, and functionality** into a product;
- **Ensuring managers complete appropriate reviews** and acquiring products compatible with existing systems;
- **Invitations-to-tender** soliciting bids from vendors when acquiring hardware and software;
- **Request-for-proposals** soliciting bids when acquiring off-the-shelf or third-party developed software; and
- **Establishing acquisition standards** to ensure security requirements to be accurately identified in request-for-proposals.

(b) **Acquiring Systems Components from Vendors:**

The following considerations are valid for both acquisition of hardware and software:

- **Vendor Selection:** This step is a critical step for success of acquisition of systems. Vendor selection is to

  be done prior to sending RFP. 'RFP are sent only to selected vendors'.

- **Geographical Location of Vendor:** The issue to look for whether the vendor has local support persons. Otherwise, the proposals submitted by vendor not as per RFP requirements need to rejected. This stage may be referred to as 'technical validation'.

- **Presentation by Selected Vendors:** All vendors, whose proposals are accepted after "technical validation", are allowed to make presentation to the System Acquisition Team.

- **Evaluation of Users Feedback:** The best way to understand the vendor systems is to analyze the feedback from present users. Present users can provide valuable feedback.

(i) **Validation of Vendors' proposals:** The contracts and software licensing process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming, but in any case it has to be gone through. **The following factors have to be considered towards rigorous evaluation**

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

(ii) **Methods of validating the proposal:** Some of the validation methods are given as follows:

- **Checklists:** It is the **most simple and a subjective method** for validation and evaluation. The various criteria are put in check list in the form of suitable **questions against which the responses are validated.** For example, Support Service Checklists.

- **Point-Scoring Analysis:** Point-scoring analysis **provides an objective means** of selecting a final system.

- **Public Evaluation Reports:** Several consultancy as well as independent agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports. This method is particularly useful where the buying staff has inadequate knowledge of facts.

- **Benchmarking Problems related Vendor's Solutions:** Benchmarking problems related to vendors' proposals are accomplished by sample programs that represent the buyer's primary work load.

- **Testing Problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system.

System Development: Programming Techniques and Languages

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 could result in the failure of a program after some time.
- **Robustness:** It refers to the **applications' strength** to uphold its operations in adverse situations by taking into account all possible inputs and outputs of a program in case of least likely situations.
- **Accuracy:** It refers not only to **'what program is supposed to do',** but should also take care of 'what it should not do'. The second part becomes more challenging for quality control personnel and auditors.
- **Efficiency:** It refers to the **performance per unit cost** with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a **user-friendly interface** and easy-to-understand internal/external documentation.
- **Readability:** It refers to the **ease of maintenance of program** even in the absence of the program developer.

Other related aspects of this phase are given as follows:

(a) **Programming Language:** Application programs are **coded in the form of statements or instructions** and the same is converted by the compiler to object code. The **programming languages commonly used are** given as follows :

- High level general purpose programming languages such as COBOL and C;
- Object oriented languages such as C++, JAVA etc.;
- Scripting language such as JavaScript, VBScript; and
- Decision Support languages such as LISP and PROLOG.

(b) **Program Debugging:** Debugging is the most **primitive form** of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program **compiles cleanly**. A clean compile means that the program can be successfully converted from the source code into machine language instructions. **Debugging can be a tedious task consisting of following four steps:**

- **Giving input** to the compiler,
- Letting the compiler to **find errors** in the program,
- **Correcting lines of code** that are erroneous, and
- **Resubmitting** the corrected source program as input to the compiler.

System Testing

Testing is a process used to identify the correctness, completeness and quality of developed computer software.

Different levels/facets of Testing are described as follows.

(i) **Unit Testing:** Unit testing is a software verification method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. or may belong to a super class, abstract or child class.

There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

- **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. Programmer checks whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization.
- **Stress Tests:** Stress testing is a form of testing that is used to determine the stability of a given system or entity.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

In terms of techniques, Unit Testing is classified as Static Analysis Testing and Dynamic Testing. Such typical testing techniques are elaborated as follows:

(a) **Static Testing:** Static Analysis Tests are conducted on source programs and do not normally require executions in operating conditions. Typical static analysis techniques include the following:

- **Desk Check:** This is done by the programmer him/herself. S/he checks for logical syntax errors, and deviation from coding standards.
- **Structured Walk Through:** The application developer leads other programmers to scan through the text of the program and explanation to uncover errors.
- **Code Inspection:** The program is reviewed by a formal committee. Review is done with formal checklists.

(b) **Dynamic Analysis Testing:** Such testing is normally conducted through execution of programs in operating conditions. Typical techniques for dynamic testing and analysis include the following**:**

- **Black Box Testing:** Black Box Testing takes an external perspective of the test object, to derive test cases.
- **White Box Testing:** It uses an internal perspective of the system to design test cases based on internal structure. It
- **Gray Box Testing:** It is a software testing technique that uses a combination of black box testing and white box testing.

(ii) **Integration Testing:** Integration testing is an activity of software testing in which individual software modules are combined and tested as a group. **This is carried out in the following two manners:**

- **Bottom-up Integration:** It is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub- system testing, and then testing of the entire system. Bottom-up testing is easy to implement.
- **Top-down Integration:** It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module.. A stub does not go into the details.

(iii) **Regression Testing:** In the context of the integration testing, the regression tests ensure that changes have not introduced new faults. The data used for the regression tests should be the same as the data used in the original test.

(iv) **System Testing:** It is a process in which software and other system elements are tested as a whole. **The types of testing that might be carried out are as follows:**

- **Recovery Testing:** This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'.
- **Security Testing:** This is the process to determine that an Information System protects data and maintains functionality as intended or not.
- **Stress or Volume Testing:** Stress testing is a form of testing that is used to determine the stability of a given system or entity.
- **Performance Testing:** Software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device.

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

- **Quality Assurance Testing:** It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance policy, methodology and prescriptions.
- **User Acceptance Testing:** It ensures that the functional aspects expected by the users have been well addressed in the new system. **There are two types of the user acceptance testing described as follows:**

o **Alpha Testing:** This is the first stage, often performed by the users within the organization by the developers, to improve and ensure the quality/functionalities as per user's satisfaction.

o **Beta Testing:** This is the second stage, generally performed after the deployment of the system. It is performed by the external users, during the real life execution of the project. It normally involves sending the product outside and receives feedback.

System Implementation

(i) **System Change-Over Strategies:** Conversion or changeover is the process of changing over or shifting over from the old system to the new system. **The Four types of popular implementation strategies are described as follows:**

o **Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. .

O **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and other files continue to be used on the old system i.e. the new is brought in stages (phases).

O **Pilot Changeover:** With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption.

O **Parallel Changeover:** This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online.

(ii) Such requisite **changeover or Conversion** includes all those activities, which must be completed to successfully convert from the previous system to the new information system. Fundamentally these technical **activities** can be classified as follows:

- **Procedure Conversion:** Operating procedures should be carefully completed with sufficient-enough documentation for the new system.
- **File Conversion:** Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed.
- **System conversion:** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one.
- **Scheduling Personnel and Equipment:** Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager.

Post Implementation Review and Systems Maintenance

(i) **Post Implementation Review:** A Post Implementation Review answers the question "Did we achieve what we set out to do in business terms. **Typical evaluations include the following:**

- **Development Evaluation:** Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained.
- **Operational Evaluation:** The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties. It tries to answer the questions related to functional aspects of the system.
- **Information Evaluation:** An information system should also be evaluated in terms of information it provides or generates. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner.

(ii) **System Maintenance:** Maintaining the system is an important aspect of SDLC. As key personnel change positions in the organization, new changes will be implemented, which will require system updates at regular intervals. **Maintenance can be categorized in the following ways:**

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the

code or defects found during the executions. A defect can result from design errors, logic errors coding errors and system performance errors. Examples of corrective maintenance include correcting a failure.

- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the System and activities to increase the system's performance or to enhance its user interface.
- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. This work is known as preventive change.

Operation Manuals

It is typical user's guide, also commonly known as Operations Manual. Moreover, it may be a technical communication document intended to give assistance to people using a particular system. It is usually written by technical writers. **The section of an operation manual will include the following:**

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

6
Auditing of Information Systems

Need for Audit of Information Systems

Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets.
- **Value of Computer Hardware, Software and Personnel***:* These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised environment, a data error during entry or process would cause great damage.
- **Maintenance of Privacy:** Data collected contains private information about an individual too. There is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

Information Systems Auditing: It is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both. **This enables organizations to better achieve four major objectives that are as follows:**

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective, competition and the market environment.
- **System Effectiveness Objectives**: Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment

Effect of Computers on Audit

Two basic functions carried out to examine these changes are:

- Changes to Evidence Collection; and
- Changes to Evidence Evaluation.

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

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor..
- **Absence of input documents:** Transaction data entered into the computer directly without supporting documentation e.g. input of telephone orders into a telesales system.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time.
- **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets.
- **Legal issues:** The use of computers to carry out trading activities is also increasing..

(ii) **Changes to Evidence Evaluation:** Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system.

- **System generated transactions:** Financial systems have the ability to initiate, approve and record financial transactions.
- **Automated transaction processing** systems can cause the auditor problems. Automated transaction generation systems are frequently used in 'just in time' (JIT) inventory and stock control systems.
- **Systemic Error:** Computers are designed to carry out processing on a consistent basis. Given the same inputs, they produce the same output. This consistency can be viewed in both a positive and a negative manner.

Responsibility for Controls

Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems.

Skill set of IS Auditor

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

- **Sound knowledge** of business operations, practices and compliance requirements;

- Should possess the **requisite professional** technical qualification and certifications
- A good understanding of **information Risks** and Controls;
- Knowledge of **IT strategies**, policy and procedural controls;
- Ability to understand **technical and manual controls** relating to business continuity; and
- Good knowledge of **Professional Standards** and Best Practices of IT controls and security.

Functions of IS Auditor

IS Auditor is the assessor of business risk. The auditor can check the technicalities to understand the risk and make a sound assessment and present risk-oriented advice to management**. IS Auditors review risks relating to IT systems and processes; some of them are:**

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

Categories of Information Systems Audits

Information Systems Audits has been categorized into **five types**:

(i) **Systems and Application:** An audit to verify that systems and applications are appropriate, efficient, and adequately controlled to ensure valid, reliable, timely, and secure **input, processing, and output** at all levels of a system's activity

(ii) **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient **processing of applications** under normal and potentially disruptive conditions.

(iii) **Systems Development:** An audit to verify that the **systems under development** meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** An audit to verify that IT management has **developed** an organizational structure and procedures to ensure a **controlled and efficient** environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** An audit to verify that **controls are in place** on the client, server, and on the network connecting the clients and servers.

Steps in Information System Audit

Different audit organizations go about IS auditing in different ways. However, **it can be categorized into six stages:**

(i) **Scoping and pre-audit survey:** Auditors determine the main areas of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management.

(ii) **Planning and preparation:** During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan.

(iii) **Fieldwork:** This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

(iv) **Analysis:** This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier.

(v) **Reporting:** Reporting to the management is done after analysis of evidence is gathered and analyzed.

(vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

Basic Plan

Planning is one of the primary and important phases in an Information System Audit, which ensures that the audit is performed in an effective manner.

Important points are given as follows:

- The **extent of planning** will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.
- **Obtaining knowledge** of the business is an important part of planning the work. The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- The auditor may **wish to discuss** overall audit plan and audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit. The overall audit plan and the audit program remains the auditor's responsibility.
- The auditor should **develop and document** an overall audit plan describing the expected scope and conduct of the audit.
- The audit should be **guided** by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a onetime activity to be taken and completed in the beginning of the audit. Planning is a continuous activity which goes on throughout the entire audit cycle.

Preliminary Review

The preliminary review of audit environment enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

The following are some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review.

(i) **Knowledge of the Business:** Related aspects are given as follows:

- General **economic factors** and industry conditions affecting the entity's business,
- **Nature** of Business, its products & services,
- General **exposure** to business,
- Its **clientele**, vendors and most importantly, strategic business partners to whom critical processes have been outsourced,

- **Level of competence** of the Top management and IT Management, and
- Finally, **Set up** and organization of IT department.

(ii) **Understanding the Technology:** An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- **Analysis** of business processes and level of automation,
- Assessing the **extent of dependence** of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business
- Understanding **technology architecture** which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying **network diagrams** to understand physical and logical network connectivity,
- Understanding **extended enterprise architecture** wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
- **Knowledge of various technologies** and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
- And finally, **Studying Information Technology** policies, standards, guidelines and procedures.

(iii) **Understanding Internal Control Systems:** For gaining understanding of Internal Controls emphasis to be placed on **compliance and substantive testing**.

(iv) **Legal Considerations and Audit Standards:** Related points are given as follows:

- The auditor should **carefully evaluate** the legal as well as statutory implications on his/her audit work.
- The Information Systems audit work could be required as **part of a statutory requirement** in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
- The statutes or regulatory framework may **impose stipulations** as regards minimum set of control

  objectives to be achieved by the subject organization. Sometimes, this may also include restrictions on the use of certain types of technologies. e.g. Freeware, shareware etc.
- The IS Auditor should also consider the **Audit Standards** applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

(v) **Risk Assessment and Materiality:** Risk Assessment is a critical and inherent part of the IS Auditor's planning and audit implementation.

The steps that can be followed for a risk-based approach to make an audit plan are given as follows:

- **Inventory** the information systems in use in the organization and categorize them.
- **Determine** which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- **Assess** what risks affect these systems and the severity of impact on the business.
- Based on the above assessment, **decide** the audit priority, resources, schedule and frequency.

Risks are categorized as follows:

- **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same.

  Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.
- **Control Risk:** Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.
- **Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

<u>Inherent Limitations of Audit</u>

Auditor shall form his/her opinion based on above processes. As per (SA 200) "Overall Objectives of An Independent Auditor and Conduct of An Audit in

Accordance With Standards of Auditing", **any opinion formed by the auditor is subject to inherent limitations of an audit, which include:**

- The **nature of financial reporting**;
- The **nature of audit procedures**
- The **need for the audit** to be conducted within a reasonable period of time and at a reasonable cost.
- The **matter of difficulty**, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.
- **Fraud**, particularly fraud involving senior management or collusion.
- The **existence and completeness of related party** relationships and transactions.
- The **occurrence of non-compliance** with laws and regulations.
- **Future events or conditions** that may cause an entity to cease to continue as a going concern.

<u>Concurrent or Continuous Audit</u>

Continuous auditing enables auditors to significantly reduce and eliminate the time between occurrence of the client's events and the auditor's assurance services thereon. Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

Types of Audit Tools: Different types of continuous audit techniques may be used. Many audit tools are also available; some of them are described below:

(i) **Snapshots:** Tracing a transaction is a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

(ii) **Integrated Test Facility (ITF):** The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

- **Methods of Entering Test Data:** The transactions to be tested have to be tagged. The application system recognize the tagged transactions and invoke two updates, one to the master file record and one to the ITF dummy entity. Auditors can also embed audit software modules to recognize transactions as ITF transactions. Tagging live transactions as ITF transactions has the advantages of ease of use. However, use of live data could mean that the limiting conditions are not tested. The auditors may also use test data that is specially prepared. In this approach the test data is likely to achieve more complete coverage than selected production data. However, preparation of the test data could be time consuming and costly.

- **Methods of Removing the Effects of ITF Transactions:** The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed. The application system may be programmed to recognize ITF transactions and to ignore them. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal. The effects of the transactions are not really removed.

(iii) **System Control Audit Review File (SCARF):** The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow- up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities. Auditors might use SCARF to collect the following types of information:

- **Application System Errors** - SCARF audit routines provide an **independent check** on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and Procedural Variances** - Organizations have to **adhere** to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception** - SCARF can be used to monitor different types of application system exceptions. For example, **salespersons** might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample** -Some embedded audit routines might be statistical sampling routines, SCARF provides a **convenient way** of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and Extended Records** - Snapshots and extended records can be written into the
SCARF file and printed when required.
- **Profiling Data** - Auditors can use embedded audit routines to collect data to build **profiles of system users**. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance Measurement** - Auditors can use embedded routines to collect data that is **useful for measuring or improving** the performance of an application system.

(iv) **Continuous and Intermittent Simulation (CIS):** This is a **variation of the SCARF** continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

- The **database management system reads** an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.

- **CIS replicates** or simulates the application system processing.
- **Every update** to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- **Exceptions** identified by CIS are written to an exception log file

Advantages and Disadvantages of Continuous Auditing: Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit.

Some of the advantages of <u>continuous audit techniques</u> are given as under:

- **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner. The **entire processing** can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability** – As evidences are collected from the system itself by using continuous audit techniques, auditors **can gather evidence** without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives** - Continuous audit techniques provides information to systems staff **regarding the test vehicle** to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users** – Using the ITFs, new users can **submit data** to the application system, and obtain feedback on any mistakes they make via the system's error reports.

The following are some of the disadvantages and limitations of the use of the continuous audit system:

- Auditors should be able to obtain **resources** required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the **development work** associated with a **new** application system.
- Auditors **need the knowledge** and experience of working with computer systems to be able to use

  continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the **audit trail** is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are **implemented in an application system** that is relatively stable.

(v) **Audit Hooks:** There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

Audit Trail

Audit trails are **logs that can be designed to record activity** at the system, application, and user level. Audit trails **provide an important detective control** to help accomplish security policy objectives.

Audit trail controls **attempt to ensure that a chronological record of all events is maintained**. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

(i) **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways:

- Detecting unauthorized access to the system,
- Facilitating the reconstruction of events, and
- Promoting personal accountability.

Each of these is described below:

- **Detecting Unauthorized Access*****:*** Detecting unauthorized access can occur in real time or after the fact. The **primary objective** of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to **report on changes** in system performance that may indicate infestation by a virus or worm. Real - time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- **Reconstructing Events*****:*** **Audit analysis** can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. **Knowledge** of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in **accounting control**. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability*****:*** Audit trails can be used to **monitor user activity** at the lowest level of detail. This capability is a **preventive control** that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

Role of IS Auditor in Physical Access Controls

Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

Audit of Environmental Controls

Related aspects are given as follows:

(a) **Role of Auditor in Environmental Controls:** Some of the critical audit considerations that an IS auditor should take into account while conducting his/her audit is given below:

(b) **Audit Planning and Assessment:** As part of risk assessment:

- The **risk profile** should include the different kinds of environmental risks. These comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risks.
- The **controls assessment** must ascertain that controls safeguard the organization against all acceptable risks are in place.
- The **security policy** of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
- **Building plans** and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
- The IS auditor should **interview** relevant personnel to satisfy himself about employees' awareness of environmental threats and controls.
- **Administrative procedures** such as preventive maintenance plans and their implementation, inspection and testing plan and procedures need to be reviewed

(c) **Audit of Environmental Controls:** Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. **The Auditor should verify that:**

- The **IPF** (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
- The **presence** of water and smoke detectors, power supply arrangements to such devices, and testing logs;
- The **location** of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- **Emergency procedures,** evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;
- **Documents** for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and

shortcomings pointed out by other auditors;

- **Power sources** and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power;
- **Environmental control equipment** such as air-conditioning, dehumidifiers, heaters, ionizers etc;
- **Compliant logs** and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair) are within acceptable levels; and
- **Identify undesired activities** such as smoking, consumption of eatables etc.

Managerial Controls and their Audit Trails

Types of Managerial Controls

Controls	***Scope***
Top Management and Information Systems Management Controls	Discusses the top management's role in planning, organizing, leading and controlling the information systems function. Also provides advice to top management in relation to long-run policy decision making and translates long- run policies into short-run goals and objectives.
System Development Management Controls	Provides a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation.
Programming Management Controls	Discusses the major phases in the program life cycle and the important controls that should be exercised in each phase.
Data Resource Management Controls	Discusses the role of database administrator and the controls that should be exercises in each phase.
Quality Assurance Management Controls	Discusses the major functions that quality assurance management should perform to ensure that the development, implementation, operation, and maintenance of information systems conform to quality standards.
Security Management Controls	Discusses the major functions performed by operations by security administrators to identify major threats to the IS functions and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.
Operations Management Controls	Discusses the major functions performed by operations management to ensure the day-to-day operations of the IS function are well controlled.

Application Controls and their Audit Trails

Types of Application Controls

Controls	**Scop e**

Boundry Controls	Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
Input Controls	Responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.
Communication Controls	Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
Processing Controls	Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
Output Controls	To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
Database Controls	Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.

Audit Trail Controls: Two types of audit trails that should exist in each subsystem are as follows:

- An **Accounting Audit Trail** to maintain a record of **events** within the subsystem; and
- An **Operations Audit Trail** to maintain a record of the **resource consumption** associated with each event in the subsystem.

Audit of Application Security Controls

Approach to Application Security Audit

Application security audit is looked from the usage perspective. A layered approach is used. **For this, auditors need to have a clear understanding of the following**

- **Business process** for which the application has been designed;
- The **source of data input** to and output from the application;
- The **various interfaces** of the application under audit with other applications;
- The **various methods** used to login to application, other than normal user-id and passwords;
- The **roles**, descriptions, user profiles and user groups that can be created in an application; and
- The **policy of the organization** for user access and supporting standards.

Understanding the Layers and Related Audit Issues

In this section, various aspects relating to each layer have been discussed.

(i) **Operational Layer:** The operational layer **audit issues** include:

- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities.

- **Password Controls:** In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum.
- **Segregation of Duties:** As frauds due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases. As defined earlier, Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals. Example to illustrate:
    - Record keeper of asset must not be asset keeper.
    - Cashier who creates a cash voucher in system, must not have right to authorize payments.
    - Maker must not be checker.

(ii) **Tactical Layer:** At the tactical layer, security administration is put in place. This includes:

- **Timely updates** to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
- **IT Risk Management:** This function is another important function performed, it includes the following activities:
    - **Assessing risk** over key application controls;
    - **Conducting** a regular security awareness programme on application user;
    - **Enabling application users** to perform a self-assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;
    - **Reviewing application patches** before deployment and regularly monitoring critical application logs;
    - **Monitoring peripheral security** in terms of updating antivirus software;
- **Interface Security:** This relates to application interfaced with another application in an organization. An auditor needs to understand that data flow to and from the application.
- **Audit Logging and Monitoring:** Regular monitoring the audit logs is required. The same is not possible for all transactions, so must be done on an exception reporting basis.

(iii) **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting.

8

Emerging Technologies

8.1 Grid Computing

The computing resources in most of the organizations are underutilized. The idea of Grid computing is to make use of such non-utilized computing power thereby the Return on Investment (ROI) on computing investments can be increased.

Thus, Grid computing is a network of computing or processor machines managed with a kind of software such as middleware, in order to access and use the resources remotely. The managing activity of grid resources through the middleware is called Grid Services. Grid Services provide access control, security, access to data including digital libraries and databases, and access to large-scale interactive and long-term storage facilities.

Grid Computing is more popular due to the following reasons:

- It has the ability to make use of unused computing power, and thus, it is a cost- effective solution.
- This enables heterogeneous resources of computers to work cooperatively and collaboratively to solve a scientific problem.

Grid computing requires the use of software that can divide and carve out pieces of a programs one large system image to several thousand computers. One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail. This is alleviated if that component has a failover component on another node, but problems can still arise if components rely on other pieces of software to accomplish tasks.

8.2 Cloud Computing

Cloud computing, simply means the use of computing resources as a service through networks, typically the Internet. The Internet is commonly visualized as clouds; hence the term.

With Cloud Computing, users can access database resources via the Internet from anywhere. Databases in cloud may be highly dynamic and scalable. It is a very independent platform in terms of computing. The best example of cloud computing is *Google Apps* where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. This enables anytime access to a shared pool of applications and resources. These applications and resources can be accessed using a simple front-end interface such as a Web browser.

Cloud computing provides the facility to access shared resources. The locations are typically not known to the end user. It also provides facilities for users to manage their applications 'on the cloud'.

With cloud computing, companies can scale up to massive capacities without having to invest in new infrastructure, train new personnel or license new software. Cloud computing is of particular benefit to small and medium-sized business systems, or large companies. In both the instances, service consumers use '***what they need on the Internet***' and '*pay only for what they use'*.

8.3.1 Cloud vs. Grid Computing

Cloud computing evolved from grid computing and provides on-demand resource provisioning. Grid computing may or may not be in the cloud paradigm depending on what type of users are using it. If the users are systems administrators and integrators, they care 'how things are maintained in the cloud'. If the users are consumers, they do not care 'how things are run in the system'.

- Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application on a variety of operating systems. CPU and network bandwidth is allocated and de-allocated on demand. The system's storage capacity goes up and down depending on the number of users and the amount of data transferred at a given time.
- Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks. Sharing resources assists introducing infrastructure costs and peak load capacity. Cloud and grid computing provide Service- Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for receiving data not in stipulated time.

Some pertinent **differences** are highlighted as follows:

- While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

8.3.2 Goals of Cloud Computing

The core goals of utilizing a cloud-based IT ecosystem are to pool available resources together into a highly efficient infrastructure. To meet the requirements, **some of the pertinent objectives in order to achieve the goals are as follows:**

- To create a highly **efficient IT ecosystem**, where resources are pooled together and costs are aligned with what resources are actually used;
- To access **services and data** from anywhere at any time;
- To **scale the IT ecosystem** quickly, easily and cost-effectively based on the evolving business needs;
- To **consolidate IT infrastructure** into a more integrated and manageable environment;
- To **reduce costs** related to IT energy/power consumption;
- To enable or improve **"Anywhere Access" (AA)** for ever increasing users; and
- To enable **rapidly provision resources** as needed.

8.3.3 Cloud Computing Architecture

The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves into multiple cloud components communicating with each other over a loose coupling mechanism, such as a messaging queue.

In the context of cloud computing, protection depends on having the Right Architecture for the Right Application (RARA). A cloud computing architecture consists of a **Front End** and a **Back End**. They connect to each other through a network, usually the Internet. The front end is the side, the computer user sees and interacts through, and the back end is the “cloud” section of the system, truly facilitating the services.

The details are given as follow:

- **Front End Architecture:** The front end of the cloud computing system comprises of the client’s devices and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft’s internet explorer or Apple’s Safari. Other types of systems have some unique applications which provide network access to its clients.
- **Back End Architecture:** Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud

computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

8.3.4 Cloud Computing Environment

The Cloud Computing environment can consist of multiple types of clouds based on their deployment and usage. Such typical Cloud computing environments, catering to special requirements, are briefly described as follows

(a) **Private Cloud:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called Internal Clouds or Corporate Clouds. *Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).* They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

Characteristics of Private Cloud

- **Secure:** The private cloud is secure as it is deployed and managed by the organization itself, and hence there is least chance of data being leaked out of the cloud.
- **Central Control:** As usual, the private cloud is managed by the organization itself, there is no need for the organization to rely on anybody and it's controlled by the organization itself.
- **Weak Service Level Agreements (SLAs):** SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider in private cloud. In private cloud, either Formal SLAs do not exist or are weak as it is between the organization and user of the same organization. Thus, high availability and good service may or may not be available.

Advantages of Private Cloud

- It improves average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.
- It provides a high level of security and privacy to the user.
- It is small in size and controlled and maintained by the organization.

Moreover, one major **limitation** is that IT teams in the organization may have to invest in buying, building and managing the clouds independently. Budget is a constraint in private clouds and they also have loose SLAs.

Major differences between On-Premise Private Cloud and Outsourced Private Cloud

	On-Premise Private Cloud	*Outsourced Private Cloud*
Management	Managed by the organization itself.	Managed by the third party. Everything is same as usual private cloud except that here the cloud is outsourced.
Service Level Agreements (SLAs)	SLAs are defined between the organization and its users. Users have broader access rights than general public cloud users and service providers are able to efficiently provide the service because of small user base and mostly efficient network.	These are usually followed strictly as it is a third party organization.

Network	Network management and network issue resolving are easier. The networks usually have high bandwidth and low latency.	The cloud is fully deployed at the third party site and organizations connect to the third party by means of either a dedicated connection or through Internet.
Security and Data Privacy	Comparatively, it is more resistant to attacks than any other cloud and the security attacks are possible from an internal user only.	Cloud is relatively less secure and the security threat is from the third party and the internal employee.
Location	The data is usually stored in the same geographical location where the cloud users are present. In case of several physical locations, the cloud is distributed over several places and is accessed using the Internet.	The cloud is located off site and when there is a change of location the data need to be transmitted through long distances.
Performance	The performance depends on the network and resources and can be controlled by the network management team.	The performance of the cloud depends on the third party that is outsourcing the cloud.

(b) Public Cloud: The public cloud is the cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called Provider Clouds. Public cloud consists of users from all over the world wherein a user can simply purchase resources on an hourly basis and work with the resources which are available in the cloud provider's premises.

Characteristics of Public Cloud:

- *Highly Scalable:* The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are considered to be scalable.
- *Affordable:* The cloud is offered to the public on a pay-as-you-go basis; hence the user has to pay only for what he or she is using (using on a per-hour basis). And this does not involve any cost related to the deployment.
- *Less Secure:* Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.
- *Highly Available:* It is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.
- *Stringent SLAs:* As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.

Advantages of Public Cloud:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- There is no need for establishing infrastructure for setting up and maintaining the cloud.
- Strict SLAs are followed.
- There is no limit for the number of users.

Moreover, one of the **limitations** is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen. Further, privacy and organizational autonomy are not possible.

(c) Hybrid Cloud: This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used. The hybrid cloud can be regarded as a private cloud extended to the public cloud and aims at utilizing the power of the public cloud by retaining the properties of the private cloud. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership with a vendor that provides private cloud platforms.

Characteristics of Hybrid Cloud

- *Scalable:* The hybrid cloud has the property of public cloud with a private cloud environment and as the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable
- *Partially Secure:* The private cloud is considered as secured and public cloud has high risk of security breach. The hybrid cloud thus cannot be fully termed as secure but as partially secure.
- *Stringent SLAs:* Overall the SLAs are more stringent than the private cloud and might be as per the public cloud service providers.
- *Complex Cloud Management:* Cloud management is complex as it involves more than one type of deployment models and also the number of users is high.

Advantages of Hybrid Cloud

- It is highly scalable and gives the power of both private and public clouds.
- It provides better security than the public cloud.

The **limitation** of Hybrid Cloud is that the security features are not as good as the private cloud and complex to manage.

(d) *Community Cloud:* The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Characteristics of Community Clouds

- *Collaborative and Distributive Maintenance:* In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
- *Partially Secure:* This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.
- *Cost Effective:* As the complete cloud is being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

Advantages of Community Clouds:

- It allows establishing a low-cost private cloud.
- It allows collaborative work on the cloud.
- It allows sharing of responsibilities among the organizations.
- It has better security than the public cloud.

The **limitation** of the community cloud is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

8.3.5 Cloud Computing Service Models

Cloud computing is a model that enables the end users to access the shared pool of resources such as computer, network, storage, database and application as an on-demand service without the need to buy or own it. The National Institute of Standards and Technology (NIST) define three basic service models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

(a) Infrastructure as a Service (IaaS): IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand. This allows users to maximize the utilization of computing capacities.

IaaS changes the computing from a physical infrastructure to a virtual infrastructure by abstracting the physical resources. The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs). The IT architects need not maintain the physical servers as it is maintained by the service providers.

Examples of IaaS providers include Amazon Web Services (AWS), Google Compute Engine, Open Stack and Eucalyptus.

A typical IaaS provider may provide the following services:

(a) *Compute:* Computing as a Service includes virtual Central Processing Inputs (CPUs) and virtual main memory for the Virtual Machines (VMs) that are provisioned to the end users.

(b) *Storage:* STaaS provides back-end storage for the VM images. Some of the IaaS providers also provide the back end for storing files.

(c) *Network:* Network as a Service (NaaS) provides virtual networking components such as virtual router, switch, and bridge for the VMs.

(d) *Load Balancers:* Load balancing as a Service may provide load balancing capability at the infrastructure layer.

Characteristics of IaaS are as follows:

- *Web access to the resources:* The IaaS model enables the IT users to access infrastructure resources over the Internet. IT user need not get physical access to the servers.
- *Centralized management:* The resources distributed are controlled from any management console that ensures effective resource management and effective resource utilization.
- *Elasticity and Dynamic Scaling:* IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.
- *Shared infrastructure:* IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.
- *Metered Services:* IaaS allows the IT users to rent the computing resources instead of buying it. The users will be charged based on the amount of usage.

The different instances of IaaS are as follows:

- *Network as a Service (NaaS):* NaaS, an instance of IaaS, 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. 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 pay-per-use basis. NaaS allows network architects to create virtual networks; virtual network interface cards (NICs), virtual routers, virtual switches, and other networking components. It further 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):* STaaS, an instance of IaaS, 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. It is an ability given to the end users to store the data on the storage services provided by the service provider. 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.

STaaS is also a cloud business model that is delivered as a utility.

- *Database as a Service (DBaaS):* This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on demand. 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. 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):* It is a type of IaaS, that 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 an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. DTaaSis 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. The end-users are responsible for securing and 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.

(b) *Platform as a Service (PaaS*): PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider. In traditional application development, the application will be developed locally and will be hosted in the central location. In stand-alone application development, the application will be developed by traditional development platforms. PaaS changes the application development from local machine to online. For example- Google App Engine, Windows Azure Compute etc.

Typical PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases.

- *Programming Languages:* PaaS providers provide a wide variety of programming languages like Java, PHP, Python, and Ruby etc. for the developers to develop applications.
- *Application Frameworks:* PaaS vendors provide application development framework like Joomla, Word Press, and Sinatra etc. for application development.
- *Database:* PaaS providers provide some of the popular databases like ClearDB, Cloudant, Redis etc. so that application can communicate with the databases.
- *Other Tools:* PaaS providers provide all the tools that are required to develop, test, and deploy an application.

Characteristics of PaaS are as follows:

- *All in One:* Most of the PaaS providers offer services like programming languages to develop test and deploy applications in the same Integrated Development Environment (IDE).
- *Web access to the development platform:* PaaS provides web access to the development platform that helps the developers to create, modify, test, and deploy applications on the same platform.
- *Offline Access:* to enable offline development, some of the PaaS providers allows the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.
- *Built-in Scalability:* PaaS services provide built-in scalability to an application. This ensures that the application is capable of handling varying loads efficiently.
- *Collaborative Platform:* To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.
- *Diverse Client Tools:* PaaS providers offer a wide variety of client tools like Web User Interface (UI), Application Programming Interface (API) etc. to help the developers to choose the tool of their choice.

(c) *Software as a Service (SaaS):* SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider. Thus, the end users are exempted from

managing or controlling an application the development platform. SaaS changes the way the software is delivered to the customers.

In the traditional software model, the software is delivered as a license-based product that needs to be installed in the end user device. Since SaaS is delivered as an on-demand service over the Internet, there is no need to install the software to the end-user's devices. SaaS services can be accessed or disconnected at any time based on the end user's needs.

SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.

The services provided by SaaS as depicted in Fig. 8.3.10 are as follows:

(a) *Business Services:* SaaS providers provide a variety of business services to startup companies that include ERP, CRM, billing, sales, and human resources.

(b) *Social Networks:* Since the number of users of the social networking sites is increasing exponentially, cloud computing is the perfect match for handling the variable load.

(c) *Document Management:* Most of the SaaS providers provide services to create, manage, and track electronic documents.

(d) *Mail Services:* To handle the unpredictable number of users and the load on e- mail services, most of the email providers offer their services as SaaS services.

Characteristics of SaaS are as follows:

- *One to Many:* SaaS services are delivered as one-to-many models whereas single instance of the application can be shared by multiple customers.
- *Web Access:* SaaS services allow the end users to access the application from any location of the device is connected to the Internet.
- *Centralized Management:* Since SaaS services are hosted and managed from the central location, the SaaS providers perform automatic updates without any user-side updates.
- *Multi-device Support:* SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smart phones, and thin clients.
- *Better Scalability*: Most of the SaaS services leverage PaaS and IaaS for its development and deployment and ensure a better scalability than traditional software
- *High Availability:* SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented.
- *API Integration:* SaaS services have the capability of integrating with other software or service through standard APIs.

The different instances of SaaS are as follows:

- *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 and integration services with archiving, spam blocking, malware protection, and compliance features.

(d) *Other Cloud Service Models*

- Communication as a Service (CaaS): CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as- needed basis. This approach eliminates the large capital investments. Examples are: Voice over IP (VolP), Instant Messaging (IM), and Collaboration and

Videoconferencing application using fixed and mobile devices.

- *Data as a Service (DaaS):* DaaS provides data on demand to a 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. Four mechanisms of Cloud security that are currently provided are Email filtering, Web content filtering, Vulnerability management and Identity management.
- *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.

8.3.6 Characteristics of Cloud Computing

Cloud Computing, typically entails few very important characteristics apart from the popular essentials of the computing paradigms. Few of them are given as follows:

- High Scalability: Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
- Agility: The cloud works in the 'distributed mode 'environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).
- High Availability and Reliability: Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
- Multi-sharing: Multiple users can work more efficiently with cost reductions by sharing common infrastructure.
- Services in Pay-Per-Use Mode: SLAs between the provider and the user must be defined when offering services in pay per use mode. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
- Virtualization: This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- Performance: It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- Maintenance: The cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places.

8.3.7 Advantages of Cloud Computing

If cloud computing is used properly and to the extent necessary, working with data in the cloud can vastly benefit all types of businesses. Major advantages of Cloud Computing are given as follows:

- Cost Efficiency: Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot, licensing fees very expensive. The cloud is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go make it very reasonable for the company.
- Almost Unlimited Storage: Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no needs to worry about running out of storage space or increasing the current storage space availability.
- Backup and Recovery: Since all the data is stored in the cloud, backup and recovery is relatively much easier. Cloud service providers are competent enough to handle recovery of information. Hence, this makes the entire process much simpler than other traditional methods of data storage.
- Automatic Software Integration: In the cloud, software integration occurs automatically. We do not

need to take additional efforts. Cloud computing allows us to customize the options with great ease. Hence, one can handpick just those services and software applications that he thinks will best suit his particular enterprise.

- Easy Access to Information: One can access the information from anywhere, where there is an Internet connection. One move beyond time zone and geographic location issues.
- Quick Deployment: Cloud computing gives us the advantage of quick deployment. The entire system can be fully functional in a matter of a few minutes.

8.3.8 Issues relating to Cloud Computing

In spite of its many benefits, as mentioned above; Cloud Computing has certain issues in terms of Security and Implementation.

(A) Security Issues: Security is a major issue relating to cloud computing. Some of the major security issues related to Cloud Computing are shown in Fig. 8.3.11 and discussed below:

- Confidentiality: Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture &Control).
- Integrity: Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service.

  (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) are some ways to preserve integrity. The most direct way to is to employ cryptographic hash function.
- Availability: Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Temporary breakdowns, Denial of Service (DoS), and natural calamities are all threats to availability.
- Governance: There is a need of governance model, which controls the standards, procedures and policies of the organization. These actions should be looked under governance. Auditing and risk management programs verify the policy.
- Trust: Deployment model provided a trust to the Cloud environment. An organization has direct control as well as the federal agencies even have responsibility to protect the information system from the risk. Trust is an important issue in Cloud. Trust ensures that service arrangements allow visibility into the security.
- Legal Issues and Compliance: There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. Laws vary from place to place. There is a need to understand various types of laws and regulations that impose security and privacy duties and potentially impact Cloud computing initiatives. CSPs need to implement an internal control monitoring function. It is the responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way.
- Privacy: Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity. The Cloud should be designed in such a way that it decreases the privacy risk.
- Audit: Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer hosted on the virtual machine to watch 'what is happening in the system'. Time consuming audits seriously detains a key gain of Cloud agility.

- Data Stealing: In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing. Some of the Cloud providers use server/s from other service providers. In that case, there is a probability that the data is less secure and is more prone to the loss. If the external server is shut down, it creates loss for the user. Back up policies such as Continuous Data Protection (CDP) should be implemented.
- Architecture: In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model.
- Identity Management and Access control: The key critical success factor is to have robust federated identity management architecture. Cloud-based "Identity as a Service" may be a useful tool. Identity Management and Access control provides a secure authentication and authorization to an organization. The identity management provides a trust and shares the digital attributes between the Cloud provider and organization.
- Incident Response: It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place to share information during and after an incident. Exposed intrusion vector helps to understand an incident response.
- Software Isolation: Software isolation is to understand virtualization and other logical isolation techniques and evaluate the risks required for the organization.
- Application Security: Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the complete access to the server. Infected applications need to be monitored.

(B) Implementation/Adaptation Issues: Some of the well-identified implementation issues are as follows:

- Threshold Policy: A threshold policy is of immense importance in a pilot study before moving the program to the production environment. This involves checking how policy detects sudden increases in the demand. Working out thresholds is really a matter of concern higher demand would be detected. As we moved out of the buying crunch, the need diminished and the instances of those resources would be de-allocated and put to other use.
- Interoperability: If a company outsources with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has Application Programming Interfaces (APIs). This creates problems of achieving interoperability of applications between two cloud computing vendors.
- Hidden Costs: Cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges for storage terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. Companies could experience latency when there is heavy traffic.
- Unexpected Behavior: Let's suppose that credit card validation application works well at our company's internal data centre. It is important to test the application with a pilot study to check for unexpected behavior. If tests show unexpected results, we will need to fix the problem before obtaining cloud services from the cloud.

  Consumers should do security testing on their own checking, ask for old stored data and check how long it takes for the vendor to recover.

  Another area of security testing is to test a trusted algorithm and then try to access data in the cloud using the decryption keys. To protect the data, one may want to manage his/her own private keys. Checking on the private key management is no longer a simple.
- Software Development in Cloud: To develop software, use cloud server pools. This allows controlling costs for a project. The project managers can also assign individual hardware resources to different cloud types. To optimize assets, the managers can get cost-accounting data.
- Environment Friendly Cloud Computing: One incentive for cloud computing is that it may be more environment friendly. First, reducing hardware components and replacing them with cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems, they can be handled more efficiently as a group.

8.4 Mobile Computing

Mobile Computing refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of the biggest problem of business people on the move i.e. mobility.

8.4.1 Components of Mobile Computing

The key components of Mobile Computing are as follows:

- *Mobile Communication:* This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties and concrete technologies.
- *Mobile Hardware:* This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA). At the back end, there are various servers like Application Servers, Database Servers, MCSS (Mobile Communications Server Switch) or a wireless gateway. The characteristics of mobile computing hardware are defined by the size, weight, primary storage, secondary storage, and means of input, means of output, battery life, expandability and durability of the device.
- *Mobile Software:* Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks of malware and access to personal information of mobile owner.

8.4.2 How Mobile Computing Works?

Here is how Mobile Computing works:

- The user enters or access data using the application on handheld computing device.
- Using one of several connecting technologies, the new data are transmitted from handheld to site's information system where files are updated and the new data are accessible to other system user.
- Now both systems (handheld and site's computer) have the same information and are in sync.
- The process work the same way starting from the other direction.

The process is similar to the way a worker's desktop PC except device is not physically connected to the organization's system. The communication between the user device and site's information systems uses different methods for transferring and synchronizing data, some involving the use of Radio Frequency (RF) technology.

8.4.3 Mobile Computing Services

8.4.4 Benefits of Mobile Computing

It leads to a range of tangible benefits, including the following:

- It provides mobile workforce with **remote access to work order details**, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to **update work order status** in real-time, facilitating excellent communication.
- It **facilitates access to corporate services** and information at any time, from anywhere.
- It provides **remote access to the corporate Knowledgebase** at the job location.
- It enables to **improve management effectiveness** by enhancing information quality, information flow, and ability to control a mobile workforce.

8.4.5 Limitations of Mobile Computing

- Insufficient Bandwidth: Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G networks. Higher speed wireless LANs are inexpensive but have very limited range.
- Security Standards: When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern. One can easily attack the VPN.
- Power consumption: When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Expensive batteries must be used to obtain the necessary battery life. Greener IT saves the power or increases the battery life.
- Transmission interferences: Weather, terrain interferes with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.
- Potential health hazards: People who use mobile devices while driving are often distracted from driving, involved in traffic accidents. Cell phones may interfere with sensitive medical devices. Cell phone signals may cause health problems.
- Human interface with device: Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

8.4.6 Issues in Mobile Computing

- *Security Issues:* Wireless networks have relatively more security requirements than wired network. A number of approaches have been suggested.
  - o *Confidentiality:* Preventing unauthorized users from gaining access to critical information of any particular user.
  - o *Integrity:* Ensures unauthorized modification, destruction or creation of information cannot take place.
  - o *Availability:* Ensuring authorized users getting the access they require.
  - o *Legitimate:* Ensuring that only authorized users have access to services.
  - o *Accountability*: Ensuring that the users are held responsible for their security related activities by arranging the user and activities are linked if and when necessary.
- *Bandwidth:* Bandwidth utilization can be improved by logging and compression. Technique of caching plays an important role. Cached data can improve query response time. Cached data can support disconnected operations.
- *Location Intelligence:* As the mobile computers move, they encounter networks. A mobile computer must be able to switch from infrared mode to radio mode as it moves from indoors to outdoors. Additionally it should be capable of switching from cellular mode to satellite mode. The physical distance may not reflect the true network distance. A small movement may result in a much longer path. This can increase the network latency as well as risk of disconnection.
- *Power Consumption:* Mobile Computers will rely on their batteries as the primary power source. Power consumption should be minimized to increase battery life.
- *Revising the technical architecture:* To provide complete connectivity among users; the current communication technology must be revised. Additionally, application and data architectures must also be revised.
- *Reliability, coverage, capacity, and cost:* Wireless network is less reliable, have less geographic coverage and reduced bandwidth, are slower, and cost more than the wired-line network.
- *Integration with legacy mainframe and emerging client/server applications:* Application development paradigms are changing. As a result huge inventory of applications have been accumulated.
- *End-to-end design and performance:* Since mobile computing involves multiple networks and multiple server platforms; end-to-end design and network response time estimates are difficult to achieve.
- *Business challenges:* Mobile computing also faces business challenges. This is due to the lack of trained professionals.

8.5 Green Computing

Green computing or Green IT refers to the study and practice of environmentally sustainable computing or IT. In other words, it is the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way. Computers consume a lot of natural resources, from manufacture to run and disposing at the end. This can include "designing, manufacturing, using, and disposing of computers, servers, And associated subsystems - such as monitors, printers, storage devices, and networking and communications systems - efficiently and effectively with minimal or no impact on the environment".

The objective of Green computing is to reduce the use of hazardous materials, maximize energy efficiency, and promote the recyclability or biodegradability of defunct products and factory waste. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

8.5.1 Relevant Facts

All businesses are increasingly dependent on technology, and small business is no exception. We work on our PCs, notebooks and smart phones all day, connected to server's running24x7. Since the technology refresh cycle is fast, these devices quickly become obsolete, and at some point - more often sooner than later - we dispose of old devices and replace them with new ones. We use massive quantities of paper and ink to print documents, many of which we promptly send to the circular file.

8.5.2 Green Computing Best Practices

Government regulation, however well-intentioned, is only part of an overall green computing philosophy. The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment. Some of such steps for Green IT include the following:

Develop a sustainable Green computing plan

- Involve stakeholders to include checklists, policies for disposal of used equipment, and recommendations for purchasing green computer equipment in organizational policies and plans;
- Encourage the IT community to consider green computing practices and guidelines.
- On-going communication about and campus commitment produce notable results.
- Include power usage recommendations in organizational policies and plans; and
- Use cloud computing so that multiple organizations share the same computing resources.

Recycle

- Dispose e-waste according to central, state and local regulations;
- Discard used electronic equipment in a convenient and environmentally responsible manner;
- Manufacturers must offer safe recycling options when products become unusable; and
- Recycle computers through manufacturer's recycling services.

Make environmentally sound purchase decisions

- Purchase of desktop computers, notebooks and monitors based on environmental attributes;
- Provide a clear, consistent set of performance criteria for the design of products;
- Recognize manufacturer efforts to reduce environmental impact by eliminating environmentally sensitive materials, designing for longevity; and
- Use Server and storage virtualization that simplify maintenance.

Reduce Paper Consumption

- Reduce paper consumption by use of e-mail and electronic archiving;
- Use of "track changes" feature in electronic documents;
- Use online marketing rather than paper based marketing that help cut down on paper wasteland

- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

Conserve Energy

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler;
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources; and
- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

8.5.3 Green IT Security Services and Challenges

IT solution providers are offering green security services in many ways. If administered properly, green security can be a cost-efficient and lucrative green IT service for solution providers. The basic aim is to increase the customer's energy savings and assess ‘how sustainable computing technology can immediately help the environment’. Green IT services present many benefits for clients as well as providers.

Apart from the common security issues, the green security emphasizes the role of security tools, methods and practices that reduce a company's environmental impact. *But to estimate the scope, to cope with the lack of green security services in the market and get advice on conserving power and purchasing switches is very important and needs a high level of sensitivity. Learning about the challenges of implementing green security and the best practices is a major hope, as the artifacts are still evolving.*

8.6 Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) To connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, Challenging the long-standing policy of working on company-owned devices. Though it has led to an increase in employees’ satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

8.6.1 Advantages of BYOD

- *Happy Employees:* Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as organization provided devices.
- *Lower IT budgets:* The employees could involve financial savings to the organization by using the devices they already possess, thus reducing the outlay of the organization.
- *IT reduces support requirement:* IT department does not have to provide support and maintenance resulting in cost savings.
- *Early adoption of new Technologies:* Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.
- *Increased employee efficiency:* The efficiency of employees is more when the employee works on his own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.

8.6.2 Emerging BYOD Threats

These risks can be classified into four areas as outlined below:

- Network Risks: It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices, the IT practice team is unaware about the number of devices being connected to the network. This lack of visibility can be hazardous.
- Device Risks: It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance.
- Application Risks: It is normally exemplified and hidden in 'Application Viruses and Malware'. Majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.
- Implementation Risks: It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy.

8.6.3 Mobile Computing and BYOD

Mobile computing, including BYOD is the single most radical shift in business since the PC revolution of the 1980s. Over the next decade, it will have a huge impact on how people work and live, how companies operate, and on the IT infrastructure. These services will focus on the issues and opportunities surrounding the new way to communicate and consume computing services. Mobile computing is not just PCs on the move. Mobile devices such as smart phones, tablets, and the iPod Touch, the last PDA standing are a radically different kind of devices, designed from the ground up as end points of data networks internal corporate networks and the Internet rather than primarily as stand-alone devices. They are optimized for mobility, which means that they have to be light, easy to handle, and maximize battery life. Where laptops has a three hour battery life, the tablet and Smartphone regularly run 12 hours or more between charging and serve as windows into the Cloud.

8.7 Social Media, Web 2.0 and Web 3.0

Related aspects of Social Media, Web 2.0 and Web 3.0 are as given:

8.7.1 Social Media

While considering a network, we imagine a set of entities connected with each other on a logical or a physical basis. Physical networks like computer networks are those that can be planned, implemented and managed very optimally and efficiently. However, when we move from physical to logical networks, the visualization becomes much more difficult. Social Networks are comprised of the most intelligent components- human beings. Being so, any activity involved with the social networks, be it participation, management, or optimization becomes extremely complicated and context based. Due to the various facets of the human species, we can have multiple types of social networks in all the fields and areas. This can range from a network of researchers, to a network of doctors to a network of academics. Each type of network has its own focus area, member size, geographical spread, societal impact and objective. Managing such networks is not only complicated but requires lot of collective efforts and collaboration. There have been uncountable social networks formed but only a few has finally achieved their true goal/s, which emphasizes the complexity of such a matter.

A social network is usually created by a group of individuals, who have a set of common interests and objectives. There are usually a set of network formulators followed by a broadcast to achieve the network membership. This happens both in public and private groups depending upon the confidentiality of the network. After the minimum numbers are met, the network starts its basic operations and goes out to achieve its goal. Success of a social network mainly depends on contribution, interest and motivation of its members along with technology backbone or platform support that makes the life easier to communicate and exchange information to fulfill a particular communication need.

8.7.2 Web2.0

Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. The two major contributors of Web 2.0 are the technological advances enabled by Ajax (Asynchronous JavaScript and XML) and other applications such as RSS (Really Simple Syndication) and Eclipse that support the user interaction and their empowerment in dealing with the web. This refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication and more open sharing of information. One of the most significant differences between Web 2.0 and the traditional World Wide Web (referred as Web 1.0) is that Web 2.0 facilitates greater collaboration and information sharing among Internet users, content providers and enterprises. Thus it can be said that the migration is from the "read-only web" to "read-write web".

The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mash-ups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

8.7.3 Components of Web 2.0 for Social Networks

Major components that have been considered in Web 2.0 include the following:

- Communities: These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online to create communities, which are very cost efficient as well as easy to use.
- *RSS-generated Syndication:* RSS is a format for syndicating web content that allows feed the freshly published web content to the users through the RSS reader.
- Blogging: A blog is a journal, diary, or a personal website that is maintained on the internet, and it is updated frequently by the user. Blogging allows a user to make a post to a web log or a blog. Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.
- Wiki: A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.
- *Usage of Ajax and other new technologies:* Ajax is a way of developing web applications that combines XHTML and CSS (Cascading Style Sheets) standards- based presentation that allows the interaction with the web page and data interchange with XML (eXtensible Markup Language) and XSLT (eXtensible Stylesheet Language Transformations).
- Folksonomy: This allows the free classification of information available on the web, which helps the users to classify and find information, using approaches such as tagging. Also known as Social Bookmarking, the bookmarks in a folder are not stored on the user's computer rather tagged pages are stored on the web increasing the accessibility from any computer connected to the Internet.
- File Sharing/Podcasting: This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.
- Mash-ups: This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

8.7.4 Types and Behavior of Social Networks

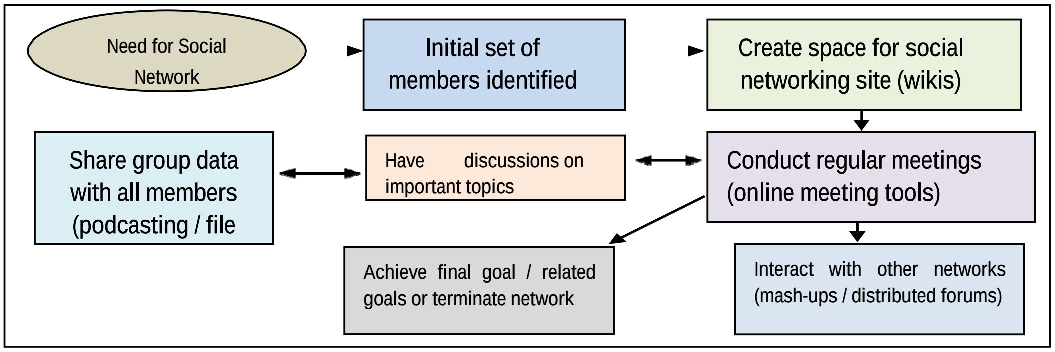
The nature of social networks makes its variety. We have various types of social networks based on needs and goals. Compartmentalizing social networks is quite a challenging activity. Social networks exist in various domains-within and outside organizations, within and outside geographical boundaries, within and outside social boundaries and many other areas. Such huge variations make the reach of social networks grow to all sectors of the society. Keeping these in mind, the main categories identified are given below:

- Social Contact Networks: These types of networks are formed to keep contact with friends and family. These have become the most popular sites on the network today. They have all components of Web 2.0 like blogging, tagging, wikis, and forums. Examples of these include Orkut, Facebook and Twitter.

- Study Circles: These are social networks dedicated for students, where they can have areas dedicated to student study topics, placement related queries and advanced research opportunity gathering. These have components like blogging and file sharing. Examples of these include, Fledge Wing and College Tonight.
- Social Networks for Specialist Groups: These types of social networks are specifically designed for core field workers like doctors, scientists, engineers, members of the corporate industries. A very good example for this type of network is LinkedIn.
- Networks for Fine Arts: These types of social networks are dedicated to people linked with music, painting and related arts and have lots of useful networking information for all aspiring people of the same line.
- Police and Military Networks: These types of networks, though not on a public domain, operate much like social networks on a private domain due to the confidentiality of information.
- Sporting Networks: These types of social networks are dedicated to people of the sporting fraternity and have a gamut of information related to this field. Examples of these include Athlinks.
- Mixed Networks: There are a number of social networks that have a subscription of people from all the above groups and is a heterogeneous social network serving multiple types of social collaboration.
- Social Networks for the 'inventors': These are the social networks for the people who have invented the concept of social networks, the very developers and architects that have developed the social networks. Examples include Technical Forums and Mash-up centers.
- Shopping and Utility Service Networks: The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behavior and send related information for the same to respective marts and stores.
- Others: Apart from the networks outlined above, there are multiple other social networks, which serve huge number of the internet population in multiple ways. Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to a more specialist network as shown in the Fig. 8.7.2.

8.7.5 Life Cycle of Social Networks

The concept of social networks and the components of Web 2.0, which are significant for social networks, have been outlined above. Next, we will see how Web 2.0 gets linked with the entire life cycle of a social network. For any social network, there are a number of steps in its life cycle. In each of the life cycle step of an online social network, Web 2.0 concepts have a great influence, as depicted in the Fig. 8.7.3. For all the steps in the life cycle, Web 2.0 provides tools and concepts, which are not only cost effective but very easy to implement. Often, online networks have a tendency to die out very fast due to lack of proper tools to communicate. Web 2.0 provides excellent communication mechanism concepts like Blogging and individual email filtering to keep everyone in the network involved in the day to day activities of the network.


Need for Social Network
Initial set of members identified
Create space for social networking site (wikis)
Share group data with all members (podcasting / file
Have discussions on important topics
Conduct regular meetings (online meeting tools)
Achieve final goal / related goals or terminate network
Interact with other networks (mash-ups / distributed forums)

8.7.6 *Applications of Web2.0*

Web 2.0 finds applications in different fields, some of which are as follows:

- *Social Media:* Social Media/Social Network is an important application of web 2.0 as it provides a fundamental shift in the way people communicate and share information. The social web offers a number of online tools and platforms that could be used by the users to share their data, perspectives, and opinions among other user communities.

- ***Marketing:*** Web 2.0 offers excellent opportunities for marketing by engaging customers in various stages of the product development cycle. It allows the marketers to collaborate with consumers on various aspects. Collaboration with the business partners and consumers can be improved by utilizing the tools provided by Web 2.0 paradigm. Consumer-oriented companies use networks such as Twitter and Facebook as common elements of multichannel promotion of their products.
- ***Education:*** Web 2.0 technologies can help the education scenario by providing students and faculty with more opportunities to interact and collaborate with their peers. By utilizing the tools of Web 2.0, the students get the opportunity to share what they learn with other peers by collaborating with them.

8.7.7 Benefits and Challenges for Social Networks using Web 2.0

Web 2.0 has provided a number of benefits to social networks. It provides a platform where users of the network need not to worry about the implementation or underlying technology at a very affordable cost and a very easy pickup time. Concepts of Web 2.0 like blogging are some things that people do on a day-to-day basis and no new knowledge skills are required. Web
2.0 techniques are very people centric activities and thus, adaptation is very fast. People are coming much closer to another and all social and geographical boundaries are being reduced at lightning speed, which is one of the biggest sustenance factors for any social network. Using Web 2.0 also increases the social collaboration to a very high degree and this in turn helps in achieving the goals for a social network.

Web 2.0 has introduced a number of powerful features that social networks are utilizing. These have provided significant advances, which can be seen by the worldwide acceptance of networking sites with these technologies. In spite of all challenges, the worldwide acceptance of social networks and its implementation using Web 2.0 is here to stay and flourish. It is up to us to participate in this movement and continue to contribute towards the betterment of the technology and concept for more contribution to the society as a whole.

8.7.8 Web 3.0

The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 are considered as the next logical step in the evolution of the Internet and Web technologies. For Web 1.0 and Web 2.0; the Internet is confined within the physical walls of the computer, but as more and more devices such as smart phones, cars and other household appliances become connected to the web, the Internet will be omnipresent and could be utilized in the most efficient manner.

Web 2.0 technologies allows the use of read/write web, blogs, interactive web applications, rich media, tagging or folksonomy while sharing content, and also social networking sites focusing on communities. At the same time, Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the “Data Web” Technology, which features the data records that are publishable and reusable on the web through query- able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence. These systems are capable of answering the questions posed by the users, because the application is able to think on its own and find the most probable answer, depending on the context, to the query submitted by the user. In this way, Web 3.0 can also be described as a “machine to user” standard in the internet.

The two major components of Web 3.0 are as follows:

- ***Semantic Web:*** This provides the web user common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines are able to take contextual Decisions on their own by finding, combining and acting upon relevant information on the web.
- ***Web Services:*** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.