Giridhar Dande

CA FINAL

INFORMATION SYSTEMS & CONTROL AUDIT

CHAPTER-1

Concepts of Governance and Management of Information Systems

Giridhar Dande
G's publiCAtions

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, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language."

It relates to "the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions.

A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives.

Enterprise Governance

‘The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization’s resources are used responsibly.’

Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit.

Examples include codes on corporate governance and financial reporting standards.

Enterprise Governance has two dimensions:

1.Corporate Governance or Conformance

2. Business Governance or Performance

Conformance means – another term for conformity

1.Corporate Governance or Conformance

the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance.

Corporate governance refers to the structures and processes for the direction and control of companies.

Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders.

The corporate governance provides a historic view and focuses on regulatory requirements.

Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital.

The Sarbanes Oxley Act of US and the Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

2.Business Governance or Performance

is pro-active in its approach.

It is business oriented and takes a forward looking view.

This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers.

This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them.

It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required.

Benefits of Governance

- Defining and encouraging desirable behavior in the use of IT and in the execution of IT outsourcing arrangements.

- Implementing and integrating the desired business processes into the enterprise.

- Providing stability and overcoming the limitations of organizational structure.

- Improving customer, business and internal relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework.

- Enabling effective and strategically aligned decision making for the IT Principles that define the

role of IT,
IT Architecture,
IT Infrastructure,
Application Portfolio and Frameworks,
Service Portfolio,
Information and Competency Portfolios and
IT Investment & Prioritization.

IT Governance and Governance of Enterprise IT (GEIT)

IT Governance

Key practices to determine status of IT Governance

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

Benefits of IT Governance

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

Increased	- value delivered through IT enterprise. - user satisfaction with IT services
Improved	- agility in supporting business needs - management and mitigation of IT-related business risk - transparency and understanding of IT's contribution to the business.

	- compliance with relevant laws, regulations and policies.
- Better cost performance of IT - IT becoming an enabler for change rather than an inhibitor. - More optimal utilization of IT resources	

Governance of Enterprise IT (GEIT)

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

The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Key Governance Practices of GEIT

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

Benefits of GEIT

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

Corporate Governance, Enterprise Risk Management and Internal Controls

Corporate Governance

The concept of Corporate Governance has succeeded in attracting a good deal of public interest because of its importance for the economic health of corporations, protect the interest of stakeholders including investors and the welfare of society, in general.

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

1. Clear assignment of responsibilities and decision-making authorities, incorporating a hierarchy of required approvals from individuals to the board of directors.

2.Establishment of a mechanism for the interaction and cooperation among the

board of directors,

senior management and
the auditors.

3. Implementing

strong internal control systems, including
internal and external audit functions,
risk management functions independent of business lines, and
other checks and balances.

4. 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.

5. 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.

Enterprise Risk Management (ERM)

Enterprise Risk Management deals with risks and opportunities affecting value creation or preservation, defined as follows:

"Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant.

IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

Internal Controls

Internal Controls as per COSO

In a computerized environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if an organization's management sets up a system of internal controls.

According to COSO, Internal Control is comprised of five interrelated components: **(I-C-RCM)**

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.

These are associated with control activities regarding information and communication systems of the entity that acts as one of the component of internal accounting system.

These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

Control Environment:

This includes the elements that establish the control context in which specific accounting systems and control procedures must operate.

The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.

For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.

Risk Assessment:

This includes the elements that identify and analyze the risks faced by an organization and the way the risk can be managed.

Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organization.

A control environment must include an assessment of the risks associated with each business process.

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, and independent checks on performance and valuation of records.

These are called accounting controls.

Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.

Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

Monitoring:

The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

This includes the elements that ensure internal controls operate reliably over time.

The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

Role of IT in Enterprises

Implementing IT has to consider not only implementation of IT controls from conformance perspective but also IT could be a key enabler for providing strategic and competitive advantage.

This requires that senior management considers IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services.

This makes it imperative to develop an IT strategy, which is aligned with business strategy and ensures value creation and facilitates benefit realization from the IT investments.

IT Steering Committee

As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee.

Depending on the size and needs of the enterprise, the senior management may appoint a high -level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives.

This committee called as the IT Steering Committee.

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

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 3 levels of managerial activity in an enterprise:

Level-1 Strategic Planning:

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

Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.

Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among those businesses.

Level-2 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.

Level-3 Operational Control:

Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Classification of Strategic Planning – 4 types

1. Enterprise Strategic Plan - ESP

Business Planning determines the overall plan of the enterprise.

The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate.

It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise.

It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives, a specification of constraints that apply, and a listing of priorities.

In an IT environment, it is important to ensure that the IT plan is aligned with the enterprise plan.

2. Information Systems Strategic Plan - ISSP

The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment.

This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long -term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals.

Some of the enablers of the IS Strategic plan are:

Enterprise business strategy,
Definition of how IT supports the business objectives,
Inventory of technological solutions and current infrastructure,
Monitoring the technology markets,
Timely feasibility studies and reality checks,
Existing systems assessments,
Enterprise position on risk,
time-to-market,
quality, and
Need for senior management buy-in,
support and critical review.

3.Information Systems Requirements Plan - ISRP

Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems.

This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information.

Based on the information architecture requirements of an enterprise, the Information Systems Requirements Plan has to be drawn up so as to meet the information requirements of the enterprise.

Some of the key enablers of the information architecture are as follows:

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

4.Information Systems Applications and Facilities Plan - ISAFP

On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan.

This plan includes:

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

Key Management Practices for Aligning IT Strategy with Enterprise Strategy

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

Understand enterprise direction:

Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives.

Consider also the external environment of the enterprise.

Conduct a gap analysis:

Identify the gaps between the current and target environments and consider the alignment of assets with business outcomes to optimize investment in and utilization of the internal and external asset base.

Consider the critical success factors to support strategy execution.

Assess the current environment, capabilities and performance:

Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT.

Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement.

Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.

Communicate the IT strategy and direction:

Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

Define the strategic plan and road map:

Create a strategic plan that defines, in co- operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals.

Include how IT will support

IT-enabled investment programs,
business processes,
IT services and IT assets.

IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high- level road map.

Business Value from Use of IT

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

Evaluate	Direct	Monitor
Value Optimization		
Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.	Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.	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. - enabled investments where claimed benefits met or exceeded.
	- services where expected benefits realized. -services with clearly defined and approved operational costs and expected benefits
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits.	

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

Risk Management

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.

Related Terms

Asset	Vulnerability	Threat
Exposure	Likelihood	Attack
Risk	Counter Measure	

Asset: can be defined as something of value to the organization.

Irrespective the nature of the assets themselves, they all have one or more of the **following characteristics:**

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

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.

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.

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 and cannot exist without a target asset.

Threats are typically prevented by applying some sort of protection to assets.

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

It is not just the immediate impact, but the real harm that occurs in the long run.

For example - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.

The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

Attack: An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability.

In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.

Simply, it is the act of trying to defeat Information Systems (IS) safeguards.

The type of attack and its degree of success determines the consequence of the attack.

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

Risk assessment includes the following:

-Identification of threats and vulnerabilities in the system;

-Potential impact of harm that a loss of CIA, would have on enterprise operations or assets.

-The identification and analysis of security controls for the information system.

Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by: (WIDE-UAE)

Widespread use of technology.
Interconnectivity of systems.
Devolution of management and control.
Elimination of distance, time and space as constraints.
Unevenness of technological changes.

Attractiveness of conducting unconventional electronic attacks against organizations.
External factors such as legislative, legal and regulatory requirements or technological developments.

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.	Passwords should not be stored in configuration files instead some secure mechanism should be used.

Risk Management Strategies – T[5]

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them.

Some risks may be minor, and it may not be cost effective to implement expensive control processes for them.

Risk management strategy is explained and illustrated below:

Tolerate/Accept the risk

One of the primary functions of management is managing risk.

Some risks may be considered minor because their impact and probability of occurrence is low.

In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.

Terminate/Eliminate the risk

It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor.

The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

Transfer/Share the risk

Risk mitigation approaches can be shared with trading partners and suppliers.

A good example is outsourcing infrastructure management.

In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization.

Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

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

Evaluate	Direct	Monitor
Risk Management		
Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;	Direct 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	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 –(CM-RADA)

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

Maintain a Risk Profile: Maintain an inventory of known risks and risk attributes, including

expected frequency,
potential impact,
responses,
related resources,
capabilities, and
current control activities.

Respond to Risk: Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

Analyze Risk: Develop useful information to support risk decisions that take into account the business relevance of risk factors.

Define a Risk Management Action Portfolio: Manage opportunities and reduce risk to an acceptable level as a portfolio.

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.

Metrics of Risk Management

Some of the key metrics are as follows:

1.Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment.

2.Number of significant IT related incidents that were not identified in risk Assessment.

3.Percentage of enterprise risk assessments including IT related risks.

4.Frequency of updating the risk profile based on status of assessment of risks.

COBIT 5 Business Framework – Governance and Management of Enterprise IT

COBIT 5 is the only business framework for the governance and management of enterprise Information Technology.

This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

As per COBIT 5, Information is the currency of the 21st century enterprise.

Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues.

It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help enterprises to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities.

Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions.

COBIT 5 provides good practices in governance and management to address these critical business issues.

It is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies.

It helps enterprises to create optimal value from their information and technology.

It provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use.

COBIT 5 is intended for enterprises of all types and sizes, including non - profit and public sector and is designed to deliver business benefits to enterprises, including:

- **User** satisfaction with IT engagement and services;
- **I**ncreased value creation from use of IT;
- **R**educed IT related risks and compliance with laws, regulations and contractual requirements;
- **D**evelopment of more business-focused IT solutions and services;
- **I**ncreased enterprise wide involvement in IT-related activities.

Integrating COBIT 5 with Other Frameworks

COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance.

COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as

Information Technology Infrastructure Library (**ITIL**),

The Open Group Architecture Framework (**TOGAF**) and

ISO 27001.

Thus, COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language.

Components in COBIT – (M-CMPF)

Management Guidelines

Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.

Control Objectives

Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

Maturity Models

Assess maturity and capability per process and helps to address gaps.

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.

Framework

Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;

Benefits of COBIT 5

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

Five Principles of COBIT 5

Principle 1: Meeting Stakeholder Needs

Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources.

It provides all of the required processes and other enablers to support business value creation through the use of IT.

Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

Stakeholder needs have to be transformed into an enterprise's actionable strategy.

The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals.

This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 integrates governance of enterprise IT into enterprise governance.

It covers all functions and processes within the enterprise.

COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone - internal and external that is relevant to governance and management of enterprise information and related IT.

Principle 3: Applying a Single Integrated Framework

There are many IT related standards and best practices, each providing guidance on a subset of IT activities.

COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.

It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components.

COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.

Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.

Principle 5: Separating Governance from Management

The COBIT 5 framework makes a clear distinction between governance and management.

These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

Seven Enablers of COBIT 5

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, but at the operational level, information is very often the key product of the enterprise itself.

Services, Infrastructure and Applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

People, Skills and Competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Using COBIT 5 Best Practices for GRC

GRC program implementation requires the following:

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

GRC program can be measured by using the following goals and metrics:

1.The reduction of redundant controls and related time to execute.

2.The reduction in control failures in all key areas.

3.The reduction of expenditure relating to legal, regulatory and review areas.

4.Reduction in overall time required for audit for key business areas.

5.Improvement through streamlining of processes and reduction in time through automation of control and compliance measures.

6.Improvement in timely reporting of regular compliance issues and remediation measures.

7.Dashboard of overall compliance status and key issues to senior management on a real - time basis as required.

IT Compliance Review

Key Management Practices of IT Compliance

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

Identify External Compliance Requirements

On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.

Optimize Response to External Requirements

Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.

Consider industry standards,
codes of good practice,
and best practice guidance for adoption and adaptation.

Confirm External Compliance

Confirm compliance of policies,
principles,
standards,
procedures and methodologies with legal,
regulatory and contractual requirements.

Obtain Assurance of External Compliance

Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies.

Confirm that corrective actions to address compliance gaps are closed in a timely manner.

Key Metrics for Assessing Compliance Process

Compliance with External Laws and Regulations	Compliance with Internal Policies
-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. -Coverage of compliance assessments.	-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. -Frequency of policies review and updates.

Information System Assurance

Using COBIT 5 for Information System Assurance

COBIT 5 has been engineered to meet expectations of multiple stakeholders.

It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc.

It is written in a non -technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers, regulators for understanding and addressing IT related issues as relevant to them.

Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, regulators and auditors (internal/external) for implementing or evaluating Governance and management practices from an end-to-end perspective.

COBIT has been used as an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001 etc. have been integrated into overall enterprise governance.

Evaluating IT Governance Structure and Practices by Internal Auditors

The following guidance is from internal audit perspective as issued by The Institute of Internal Auditors (IIA).

Leadership

- Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.

- Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.

- Determine how IT will be measured in helping the organization achieve these goals.

- Review how roles and responsibilities are assigned within the IT organization and how they are executed.

- Review the role of senior management and the board in helping establish and maintain strong IT governance.

Organizational Structure

- Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.

- This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization.

Processes

- Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems.

- What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?

Risks

- Review the processes used by the IT organization to identify, assess, and monitor risks within the IT environment.

- Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.

Controls

- Assess key controls that are defined by IT to manage its activities and the support of the overall organization.

- Ownership, documentation, and reporting of self-validation aspects should be reviewed as activity of internal audit.

- Additionally, the control set should be strong enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.

Performance Measurement

- Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

Sample Areas of GRC for Review by Internal Auditors – SEG-RIREEA

Scope: The internal audit activity must evaluate and contribute to the

improvement of governance,
risk management, and
control processes using a systematic and disciplined approach.

Evaluate Enterprise Ethics: The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.

The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

Governance: internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

1.Promoting appropriate ethics and values within the organization.

2.Ensuring effective organizational performance management and accountability.

3.Communicating risk and control information to appropriate areas of the organization.

4.Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

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.

Risk Management Process: The internal audit activity may gather the information to support this assessment during multiple engagements.

The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Evaluate Risk Exposures: The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems.

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.

Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

Sample Areas of Review of Assessing and Managing Risks (E-MRP, E-IPS)

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

Ensure that assurance providers are independent and qualified: Ensure that the entities performing assurance are independent from the function, groups or organizations in scope.

The entities performing assurance should demonstrate

an appropriate attitude and appearance,
competence in the skills and knowledge necessary to perform assurance, and
adherence to codes of ethics and professional standards.

Monitor Internal Controls: Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.

Review Business Process Controls Effectiveness: Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively.

It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as
periodic testing of controls,
continuous controls monitoring,
independent assessments,
command and control centers, and
network operations centers.

Perform Control Self-assessments: Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.

Execute assurance initiatives: Execute the planned assurance initiative.

Report on identified findings.

Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

Identify and Report Control Deficiencies: Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.

Plan Assurance Initiatives: Plan assurance initiatives based on

Enterprise, assurance and conformance objectives,
strategic priorities,
inherent risk resource constraints, and
sufficient knowledge of the enterprise.

Scope assurance initiatives: Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.

CH:2 - Information Systems Concepts

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

Classification of System

On the basis of Elements

Abstract System also known as Conceptual System or Model can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God.	**Physical System**, on the other hand, is a set of tangible elements, which operated together to accomplish an objective e.g. Computer system, University system etc.

On the basis of Interactive behavior

An **Open System** interacts with other systems in its environment. **For example;** Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.	**Closed System** does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task.

On the basis of Working/Output

A **Deterministic System** operates in a predictable manner. For **example** - software that performs on a set of instructions is a deterministic system.	A **Probabilistic System** can be defined in terms of probable behavior. For **example** - inventory system is a probabilistic system where the average demand, average time for replenishment, etc may be defined, but the exact value at any given time is not known.

On the basis of Degree of Human intervention

In a **Manual System**, the activities like data collection, maintenance and final reporting are done by human.	In an **Automated System**, the activities like data collection, maintenance and final reporting are carried out by computer system or say machine itself.

Information Systems and its Components

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

1. All systems work for predetermined objectives and the system is designed and developed accordingly.

2. In general, a system has a number of interrelated and interdependent subsystems or components.

3.No subsystem can function in **isolation**; it depends on other subsystems for its inputs.

4. If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are **interrelated**'.

5. The way a subsystem works with another subsystem is called **interaction.**

6.The different subsystems interact with each other to achieve the **goal** of the system.

7. The work done by individual subsystems is integrated to achieve the **central goal** of the system.

8.The goal of individual subsystem is of lower priority than the goal of the entire system.

Functions of Information Systems

Finance and Accounting – The main goal of this subsystem is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget.

It also helps in forecasting revenues, determining the best resources and uses of funds and managing other financial resources.

Typical **sub-application areas** in finance and accounting are – **(GFA-ACT-IFB)**

✓ General ledger ✓ Financial accounting ✓ Accounts receivable/payable	✓ Asset accounting ✓ Cash management ✓ Treasury management	✓ Investment management ✓ Fund management ✓ Balance sheet.

Marketing and Sales – Marketing and sales activities have a key role for running a business successfully in a competitive environment.

The objective of this subsystem is to maximize the sales and ensure customer satisfaction.

The marketing system facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products.

The sales department may use an order processing system to keep the status and track of orders, generate bills for the orders executed and delivered to the customer, strategies for rendering services during warranty period and beyond, analyzing the sales data by category such as by region, product, sales manor sales value.

Production or Manufacturing – The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service.

The system

generates production schedules and
schedules of material requirements,
monitors the product quality,

plans for replacement or overhauling the machinery and also helps in overhead cost control and waste control.

Inventory /Stores Management- The inventory management system is designed with a view to keeping the track of materials in the stores.

The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials with optimal re-order quantity and facilitate various queries about inventory like total inventory value at any time, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc.

Human Resource Management- Human resource is the most valuable asset for an organization.

Utilization of this resource in the most effective and efficient way is an important function for any enterprise.

Human Resource Management System (HRMS) aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc. helps management for allocating manpower to right activity at the time of need or starting a new project.

This system also keeps track of employees' output or efficiency.

An **HRM system** may have the following modules –

- Promotion management
- Recruitment management.
- Travel management.
- Benefit administration.
- Salary administration.
- Personnel administration. etc.

Types of Information Systems – OK-MS

1.Operational-Level Systems (OLS)	**2.Knowledge-Level Systems(KLS)**	**3.Management-Level Systems(MLS)**	**4.Strategic Level Systems (SLS)**
>TPS Activities **>TPS components – (IPSO)** -**I**nput -**P**rocessing -**S**torage -**O**utput **Features of TPS – (SLAB)** -**S**ource of input for other systems -**L**arge volume of data -**A**utomation of basic operations -**B**enefits are easily measurable	**(A) Office Automation Systems (OAS)** **>OAS operations** -Document Capture -Document Creation -Receipts and Distribution -Recording Utilization of Resources -Calculations -Filling, Search, Retrieval and Follow up **>4-Benefits of OAS** **>Computer Based OAS** -TPS -EDMS -EMCS +Electronic Mail +FAX +Voice Mail -Teleconferencing and Video-conferencing Systems	**(A) Management Information Systems (MIS)** **>Characteristics of an effective MIS** -Management Oriented -Management Directed -Integrated -Computerized -Common Data Flows -Common Database -Heavy Planning Element -Sub System Concept **>8-Misconceptions about MIS** **>Pre-requisites of an Effective MIS** -Database -Qualified System and Management Staff -Support of Top Management -Control and maintenance of MIS **>Evaluation of MIS** **>Constraints in operating a MIS**	**(A) Executive Information Systems (EIS)** >6-Characteristics of EIS. >5-types of information used in executive decision making **–(H-FILL)** -High degree of uncertainty -Future orientation -Informal Source -Lack of structure -Low level of detail **>6-Contents/Principles of EIS** **>7-Differences between EIS vs TIS.**

	(B) Knowledge Management System (KMS) -Explicit -Tacit	**>8-Limitations of MIS** **(B) Decision Support System (DSS)** >Planning languages -GPPL -SPPL **>10-Characteristics of DSS** **>3-Components of DSS** -The user -Databases **Implementation of Database – 3 levels** +Physical +Logical +External -Model base **>Examples of DSS in Accounting** -CAS -CBS -BVAS -GDSS **>6 -Difference between DSS and traditional MIS**	

Specialized Systems-ECC

(A) Expert System	**(B) Cross Functional Information Systems**	**(C) Core Banking System (CBS)**
Business applications of ES-(MP-AGM) - Marketing - Personnel - Account and Finance - General Business - Manufacturing >Need for ES – (3 Major Reasons) >5-Benefits of ES **Potential applications of ES –(CASE-D)** -Complexity -Availability -Structure -Expertise -Domain	**>ERP** **>Components of ERP – (S-PCC)** -Software Component -Process Flow -Customer Mindset -Change Management **>10-Benefits of ERP**	10-Elements of core banking

1. OPERATIONAL-LEVEL SYSTEMS (OLS)

A. Transaction Processing Systems (TPS)

- TPS is an information system that manipulates transaction data into usable information.
- Any business activity such as

- Sales,
- Purchase,
- Production,
- Delivery,
- Payments or Receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use.

➢ For **example**, selling of a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance.

➢ Typically, a TPS involves the **following activities**:

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

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

- **Inputs –** Source documents, such as customer orders, sales, slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs in to the TPS.
  They serve several purposes like
  - capturing data,
  - facilitating operations by communicating data and authorizing another operation in the process,
  - standardizing operations by indicating, which data require recording and what actions need to be taken and providing a permanent file for future analysis, if the documents are retained etc.
- **Processing –** This involves the use of journals and registers to provide a permanent and chronological record of inputs.
  Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting.
  Some of the common journals are sales journal, purchase journal, cash receipts journal etc.
- **Storage –** Ledgers and files provide storage of data on both manual and computerized systems.
  The general ledger, the accounts/vouchers payable ledgers, and the accounts receivable ledger are the records of final account that provide summaries of a firm's financial accounting transactions.
- **Outputs –** Any document generated in the system is output & Some documents may be an input.
  For **example,** a customer invoice is an output from the order-entry application system and also and input document to the customer.
  The trial balance lists the balances of all the accounts on the gametal ledger and tests the accuracy of the record keeping.
  Financial reports summarize the results of transaction processing and express these results in accordance with the principles of financial reporting.

(b) Features of TPS

- **Source of input for other systems –**
  TPS is the basic source of internal information for other information systems.
  Heavy reliance by other information systems makes TPS important for tactical and strategic decisions as well.
- **Large volume of data –**

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

- **Automation of basic operations –**
  Any TPS aims at automating the basic operations of a business enterprise and plays a critical role in the day-to-day functioning of the enterprise.
  Any failure in the TPS for a short period of time can play havoc with the functioning of the enterprise.
- **Benefits are easily measurable –**
  TPS reduces the workload of the people associated with the operations.
  It improves their efficiency by automating some of the operations.
  Most of the TPS benefits are tangible and easily measurable.
  Therefore, cost benefit analysis regarding the desirability of TPS is easy to conduct.

2. KNOWLEDGE-LEVEL SYSTEMS (KLS)

(A) Office Automation Systems (OAS): The application of computers to handle the office activities is also termed as office automation. Different office activities can be **broadly grouped** into the following types of operations:

- **Calculations –** These include the usual calculator functions like routine arithmetic, interest calculations, working out the percentages etc.
- **Document Capture –** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be Captured.
- **Document Creation –** This consists of preparation of documents, dictation, editing of texts etc.
- **Filling, Search, Retrieval and Follow up –** This is related to filling, indexing, searching of documents, which takes up significant time.
- **Receipts and Distribution –** This basically includes distribution of correspondence to designated recipients.
- **Recording Utilization of Resources –** This includes, where necessary, record keeping in respect to specific resources utilized by office personnel.

(a) Benefits of Office Automation Systems

OAS	-improve communication within an organization and between enterprises. -reduce the cycle time between preparation and receipt of messages at the recipients' end. -reduce the costs of office communication both in terms of time spent by executives and cost of communication links. -ensure accuracy of information and smooth flow of communication.

(b) Computer Based Office Automation Systems:

- **Text Processing Systems(TPS) –** The key points relating to TPS are given as follows:
  - TPS are the most commonly used components of the OAS.
    This is so because a large proportion of the office communication takes place in writing using words of a natural language.
  - TPS automate the process of development of documents such as letters, reports, memos etc. They permit use of standard stored information to produce personalized documents.
    Such automation reduces keying effort and minimizes the chances of errors in the document.

- The text processor may be simple word processing systems or desktop publishing systems. The desktop publishing systems help in quick production of multiple copies of the document with quality printing.
- The desktop publishing systems are often supported with laser printers, inkjet printers, scanners and other such devices for producing good quality documents.

- **Electronic Document Management System (EDMS) –** The key points relating to these systems are given as follows:
  - These Systems capture the information contained in documents, stored for future reference and make them available to the users as and when required.
    These systems are linked to the OAS such as text processors, electronic message communication systems etc.
  - These systems are very useful in remote access of documents that is almost impossible with manual document management systems, for **example**, a customer may have a complaint concerning delivery of goods not being in accordance with the delivery instructions in the order.
  - In the case of internal communication, document management systems can prove to be very useful. For **example**, the loan application form filed in a branch of a bank can be accessed by the sanctioning officer for scrutiny at the head office or any office for scrutiny of loan proposals.
  - With computer based document management systems, location of the executive becomes irrelevant for access to documents.
- **Electronic Message Communication Systems –** Business enterprises have been using a variety of communication systems for finding and receiving messages.
  These include telephone, mail and facsimile (Fax), etc.
  The computer based message communication systems offer a lot of economy not only in terms of reduced time in sending or receiving the message but also in terms of reliability of the message and cost of communication.
  Components of Message Communication Systems – 3 basic components based message communication systems are given as follows:
  - ✓ Electronic Mail
  - ✓ Facsimile (Fax)
  - ✓ Voice Mail

- **Electronic Mail-** Various features of electronic mail are stated below: **(EOB-IPE)**
  - **Electronic Transmission-** The transmission & confirmation of messages with email is electronic and message delivery is very quick, almost instantaneous.
  - **Online Development and Editing -** The email message can be developed and edited online before transmission.
    The online development and editing eliminates the need for use of paper in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
  - **Broadcasting and Rerouting -** Email permits sending a message to a large number of target recipients.
    Thus, it is easy to send a circular to all branches of a bank using Email resulting in a lot of saving of paper.
    The email could be rerouted to people having direct interest in the message.
  - **Integration with other Information Systems -** The E-mail has the advantage of being integrated with the other information systems.

Such integration helps in ensuring that the message if accurate and the information required for the message is accesses quickly.

- **Portability -** Email renders the physical location of the recipient and sender irrelevant.
  The email can be accessed from any Personal computer/tablet/smart phones equipped with the relevant communication hardware, software and link facilities.
- **Economical -** The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode for sending and receiving messages.
  Since the speed of transmission is increasing, the time cost on communication media per page is falling further, adding to the popularity of email.
  The email is proving to be very helpful not only for formal communication but also for informal communication within the enterprise.

- **Facsimile (Fax) –** It is electronic communication of images of documents over telephone lines.
  The computer based fax technology automates fax communication and permits sharing of fax facilities.
  It uses ***special software*** and fax servers to send and receive fax messages using common communication resources.
  These servers have the ability to receive fax messages and automatically reroute them to the intended recipient after viewing it at the central computer, similarly, the managers in an enterprise can leave the fax messages to the server which will send it to the intended recipient automatically.

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

- **Teleconferencing and Video-conferencing Systems -** Teleconferencing is conducted in a business meeting involving more than 2 persons located at 2 or more different places.
  The teleconferencing helps in reducing the time and cost of meeting as the participants do not have to travel to attend the meeting.
  It may be audio or video conferencing with or without use of computer systems.
  These systems are based on Personal computers featuring a digital camera and run on visual communication software.
  The communication links are still quite expensive making the desktop video conferencing useful only for selected applications.

(B) Knowledge Management System (KMS)

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

- There are 2 broad types of knowledge - Explicit and Tacit.
- KMS makes a direct connection between an organization's intellectual assets — both Explicit [**recorded**] and Tacit [**personal know-how**] — and positive results.

Explicit knowledge: Explicit knowledge is that which can be formalized easily and as a consequence is easily available across the organization.
Explicit knowledge is articulated, and represented as spoken words, written material and compiled data.
This type of knowledge is codified, easy to document, transfer and reproduce.
For example – Online tutorials, Policy and procedural manuals.

Tacit knowledge: Tacit knowledge, on the other hand, resides in a few often-in just one person and hasn't been captured by the organization or made available to others.
Tacit knowledge is unarticulated and represented as intuition, perspective, beliefs, and values that individuals form based on their experiences.
It is personal, experimental and context-specific. It is difficult to document and communicate the tacit knowledge.
For example – hand-on skills, special know-how, employee experiences.

3.MANAGEMENT-LEVEL SYSTEMS(MLS)

III. Management-Level Systems: These support the middle managers in monitoring, decision-making and administrative activities and are helpful in answering questions like - Are things working well and in order? These provide periodic reports rather than instant information on operations.
For example - a college control system gives report on the number of leaves availed by the staff,
salary paid to the staff,
funds generated by the fees, finance planning etc.

These types of systems mainly answer **"what if"** questions.
For example - What would be quality of teaching if college has to achieve top ranking in academics?
These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems.

(A) Management Information Systems (MIS) –

MIS has been defined by **Davis and Olson** as "An integrated user-machine system designed for providing information to support operational control, management control and decision making functions in a n organization".

Other notable definition of MIS is "MIS is a computer based system that provides flexible and speedy access to accurate data".

MIS supports the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals.
Nature of MIS at different levels has different flavors and they are available in the form of reports, tables, graphs and charts or in presentation format using some tools.

MIS at the top level is much more comprehensive but is condensed or summarized compared to the information provided to those at middle level management.

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

- **Management Oriented –** It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives.
  Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.
- **Management Directed–** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts.
  For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- **Integrated –** The best approach for developing information systems is the integrated approach as all the functional and operational information sub- systems are **tied** together into one entity.
  An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub- systems that operate within a company.
- **Common Data Flows –** It means the use of common input, processing and output procedures and media whenever required.
  Data is captured by the system analysts only once and as close to its original source as possible.
  Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system.
  This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- **Common Database** – Database is the mortar that holds the functional systems together.
  It is defined as a **"super-file",** which consolidates and integrates data records formerly stored in many separate data files.
  The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- **Computerized -** Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system.
  In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly.
  Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff.
- **Heavy Planning Element –** An MIS usually takes one to 3 years and sometimes even longer period to get established firmly within a company.
  Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- **Sub System Concept –** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan.

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

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

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

i. Database
ii. Qualified System and Management Staff
iii. Support of Top Management
iv. Control and maintenance of MIS

(i) Database - It is collection of files,
which is collection of records and
records are nothing but collection of data.

The data in database is organized in such a way that accessing to the data is improved and redundancy is reduced.

The ***main characteristics*** of database are given as follows:

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

(ii) Qualified System and Management Staff - The 2nd pre-requisite of effective MIS is that it should be manned by qualified officers.
These officers, who are experts in the field, should understand clearly the views of their fellow officers.
For this, the organizational management base should comprise of ***2 categories*** of officers:

- Systems and Computer experts and
- Management experts.

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

(iii) Support of Top Management – The support from top management is required for the effectiveness of MIS in an organization. The **reasons** for the same are as follows:

- Any implementation, which does not receive the support of top management will not be effectively controlled and tends to be get lesser priority and may be delayed or abandoned.
- The resources involved in computer-based information systems are large and are growing larger in view of importance gained by MIS.
- To gain the support of top management, the officers should place before top management all the supporting facts and state clearly the benefits, which will accrue from it to the concern.
- This step will certainly shed light on management, and will change their attitude towards MIS. Their wholehearted support and cooperation will help in making MIS an effective one.

(iv) Control and maintenance of MIS- Control of the MIS means the operation of the system as it was designed to operate.

Some time, users develop their own procedures or short cut methods to use the system, which reduce its effectiveness.

To check such habits of users, the management at each level in the organization should devise checks for the information system control.

Maintenance is closely related to control. Formal methods for changing and documenting changes must be provided.

(d) Evaluation of MIS – An effective MIS should be capable of meeting the information requirements of its executives in future as well.

This capability can be maintained by evaluating the MIS and taking appropriate timely action.

The evaluation of MIS should take into account the following **major points**:

- Examining whether enough flexibility exists in the system to cope with any expected or unexpected information requirement in future.
- Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.
- Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

(e) Constraints in operating a MIS – Major constraints, which come in the way of operating an information system, are given as follows:

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

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

- The quality of the outputs of MIS is basically governed by the **quality** of input and processes.

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

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

A properly-designed DSS is an ***interactive software-based system*** intended to help decision makers to compile useful information from

- raw data,
- documents,
- personal knowledge, and/or
- business models to identify and solve problems and make decisions.

In other words, a DSS can be defined as a system that provides ***tools*** to managers to assist them in solving semi-structured and unstructured problems in their own.

A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enable them to generate the information required by them in making decisions.

A DSS supports the human decision-making process, rather than a means to replace it.

Two types of planning languages that are commonly used in DSS are:

- General-purpose planning languages and
- Special-purpose planning languages.

- **General-purpose planning languages** that allow users to perform many routine tasks, for example; retrieving various data from a database or performing statistical analyses.
  The languages in most electronic spreadsheets are good examples of general-purpose planning languages.
  These languages enable user to tackle abroad range of budgeting, forecasting, and other worksheet-oriented problems.
- **Special-purpose planning languages** are more limited in what they can do, but they usually do certain jobs better than the general-purpose planning languages.
  Some statistical languages, such as SAS and SPSS, are examples of special purpose planning languages.

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

- This supports decision making and occurs at ***all levels*** of management.

- Instead of helping ***individuals*** working on independent tasks, it should be able to help ***group*** making decisions.
- It should be flexible and adaptable.
- It should be easy to use.
- A user should not have knowledge of computer programming to generate reports that helps in decision making.
- DSS focuses on decision rather than data and information.
- DSS can be used for structured problems.
- DSS should be user-friendly.
- DSS should be extensible and evolve overtime.
- DSSs are used mainly for decision making rather than communicating decisions and training purposes.
- DSS impact should be on decision where the manager's judgment is essential and there is sufficient structure for computers.

(b) Components of DSS – A DSS comprise of the following basic components, which are:

i. The user
ii. Databases
iii. Model base

(i) The user - The user of a DSS is usually a manager with an unstructured or semi-structured problem to solve.
Typically, users do not need a computer background to use a DSS for problem solving.
The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution.
Manager and staff specialist (analyst) are the **two broad classes** of users.
The **key points** relating to these users are given as follows:

- **Manager -** These are the users, who have basic computer knowledge and want the DSS to be very user friendly.
  The manager may be at any level of authority in the organization (e.g., either top management or operating management).
- **Staff Specialist (Analysts) -** These are the people, who are more details oriented and willing to use complex system in their day-to-day work.

(ii) Databases – A DSS includes one or more databases that contain both routine and non-routine data from both internal and external sources.
The data from external sources include data about the operating environment of an organization.
For **example;** data about economic conditions, market demand for the organization's goods or services, and industry competition.
DSS users **may** construct additional databases themselves.
Some of the data may come from internal sources in the normal course of operations.
For **example;** data from the financial and managerial accounting systems such as account, transaction, and planning data.
The database may also capture data from other subsystems such as

- marketing,
- production, and
- personnel.

External data include assumptions about such variables as

- interest rates,

- vacancy rates,
- market prices, and
- levels of competition.

Implementation of Database - Database is implemented at 3 levels as listed below:

- **Physical level –** It involves the implementation of the database on the hard disk i.e. storage of data in the hard disk.
  The management of storage and access is controlled by operating system.
- **Logical Level –** It is designed by professional programs, which have complete knowledge of DBMS.
  It deals with the nature of data stored, the scheme of the data.
  Storage which is logically divided into various tables having rows and columns and the techniques for defining relationships with indexes.
- **External level –** The logical level defines schema, which is divided into smaller units known as sub-schemas and
  given to the managers each sub-schema containing all relevant data needed by one manager.

(iii) Model base – The planning language in a DSS allows the user to maintain a dialogue with the model base, which is the ***"brain"*** of DSS because it performs data manipulations and computations with the data provided to it by the user and the database.
There are many types of model bases, but most of them are custom-developed models that do some types of mathematical functions.
for **example;** cross tabulation, regression analysis, time series analysis, linear programming and financial computations.
The analysis provided by the routines in the model base is the key to supporting the user's decision.

(c) Examples of Decision Support Systems in Accounting – Many DSS are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems.
Below are several illustrations of these systems:

- Cost Accounting System
- Capital Budgeting System
- Budget Variance Analysis System
- General Decision Support System

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

Using this DSS, accountants, managers, and engineers identify and prioritize these factors.
Then they can evaluate up to seven investment alternatives at once.

- **Budget Variance Analysis System -** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance.
  One institution uses a computerized DSS to generate monthly variance reports for division comptrollers.
  The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional 1 and 5-year budget projections using the forecasting tools provided in the system.
  The DSS thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
- **General Decision Support System -** As mentioned earlier, some planning languages used in DSS are general purpose and therefore have the ability to analyze many different types of problems.
  In a sense, these types of DSS are a decision-maker's tools.
  The user needs to input data and answer questions about a specific problem domain to make use of this type of DSS.
  An **example**, is a program called ***Expert Choice*** which supports a variety of problems requiring decisions.
  The user works interactively with the computer to develop a hierarchical model of the decision problem.
  The DSS then asks the user to compare decision variables with each other.
  Expert choice analyzes these judgments and presents the decision maker with the best alternative.

(d) Difference between DSS and traditional MIS:

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

4. STRATEGIC LEVEL SYSTEMS (SLS)

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

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

(a) Characteristics of EIS –

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

(b) The Executive Decision-Making Environment – The type of decisions that executives must make are very broad.
Often, executives make these decisions based on a vision they have regarding 'what it will take to make their enterprise successful.'
To a large extent, executives rely much more on their own intuition than on the sophisticated analytical skills. The intuitive character of executive decision- making is reflected strongly in the types of information found most useful to executives.

5 characteristics of the types of information used in executive decision making are given as follows:

Lack of structure – Many of the decisions made by executives are relatively unstructured.
These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance.
Also, it is not always obvious, 'which data are required' or 'how to weigh available data when reaching a decision.'

High degree of uncertainty – Executives work in a decision space that is often characterized by a lack of precedent.
For **example**, when the Arab oil embargo hit in mid 1970s, no such previous event could be referenced for advice.
Executives also work in a decision space where results are not scientifically predictable from actions.
If prices are lowered, for instance, product demand will not automatically increase.

Future orientation – Strategic-planning decisions are made in order to shape future events. As conditions change, enterprises must change also.
It is the executive's responsibility to make sure that the organization keeps pointed toward the future.

<u>Some key questions about the future include:</u>

1."How will future technologies affect what the company is currently doing?
2. What will the competition (or the government) do next?
3. What products will consumers demand five years from now?"
4. As one can see, the answers to all of these questions about the future external environment are vital.

Informal Source – Executives, more than other types of managers, rely heavily on informal source for key information.
For **example**, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company's database or in scheduled computer reports.

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

(c) Contents of EIS/Practical set of principles

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

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

(d) Difference between EIS and Traditional Information Systems –

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

SPECIALIZED SYSTEMS

Some of them are Expert Systems, Cross Functional Information Systems, and Core Banking System (CBS) etc.

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

Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems.

For **instance**, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like –

- how much can be invested.
- Does the client have any preferences regarding specific types of securities? And so on.

Some of the business applications of Expert Systems are as follows: (GM-MAP)

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

(a) Need for Expert Systems –

- Expert labor is expensive and scarce.
- Knowledge worker's employee, who routinely work with data and information to carry out their day-to-day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.
- Moreover, no matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.
- Both these limitations imposed by human information processing capability and the rushed pace at which business is conducted today put a practical limit on the quality of human decision making; thus, putting a need for expert systems.

(b) Benefits of Expert Systems –

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

Some of the properties that potential applications should possess to qualify for Expert System development are given as follows: (CASE-D)

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

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

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

(a) Components of ERP – (SPCC)

I. Software Component
II. Process Flow
III. Customer mindset
IV. Change Management

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

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

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

(iii) Customer mindset: By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance.

For **example**, some users may say that they have spent many years doing an excellence job without help from ERP system.
In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

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

(b) Benefits of ERP

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

(C) Core Banking System (CBS) - Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices.
Normal core banking functions will include transaction accounts, loans, mortgages and payments.
Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

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

Elements of core banking include:

- Making and servicing loans.
- Opening new accounts.
- Processing cash deposits and withdrawals.
- Processing payments and cheques.
- Calculating interest.
- Customer Relationship Management (CRM) activities.
- Managing customer accounts.

- Establishing criteria for minimum balances, interest rates, number of withdrawals allowed and so on.
- Establishing interest rates.
- Maintaining records for all the bank's transactions.

Application of Information Systems in Enterprise Processes

3-Vital roles in business firms -S^3

1.Support an organization's business processes and operations: This includes operations support systems such as Transaction Processing Systems, Process Control Systems.

2.Support business decision-making: This includes MIS, DSS, and EIS.

3.Support strategic competitive advantage: This includes ES, KMS, SIS, and Functional Business Systems.

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

Management Challenges – It includes

how the function and IT resources are maintained and
utilized to attain top performance and
build the business strategies.

Business Applications – It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.

Development Processes – It comprise how end users and IS specialists develop and execute business/IT solutions to problems.

Foundation Concepts – It includes fundamental business, and managerial concepts

e.g. 'what are components of a system and their functions', or
'what competitive strategies are required'.

Information Technologies (IT) – It includes

operation,
development and management of hardware,
software,
data management,
networks, and
other technologies.

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

Information system	- helps managers in efficient decision-making to achieve the organizational goals. - helps in making right decision at the right time i.e. just on time. - is viewed as a process; it can be integrated to formulate a strategy of action or operation. - may help in generating innovative ideas for solving critical problems.

-An organization will be able to survive and prosper in a highly competitive environment on the strength of a well-designed Information system.

-Knowledge gathered though Information system may be utilized by managers in unusual situations.

Various types of Business Applications

1. E-business

This is also called electronic business and includes purchasing, selling, production management, logistics, communication, support services and inventory management through the use of internet technologies.

The primary components of E - business are infrastructure (computers, routers, communication media e.g. wire, satellite etc., software and programmers), electronic commerce and electronically linked devices and computer aided networks.

The advantage of E-business is 24-hour sale, lower cost of doing business, more efficient business relationship, eliminate middlemen, unlimited market place and access with broaden customer base, secure payment systems, easier business administration and online fast updating.

Only investment is needed in the purchase of space on internet, designing and maintenance of website.

Different types of business can be done e.g. it may be

B2B (Business to Business),
B2C (Business to Customer),
C2C (Customer to Customer) and
C2B (Customer to Business).

2. Financial Service Sector

The financial services sector (banks, building societies, life insurance companies and short term insurers) manages large amounts of data and processes enormous numbers of transactions every day.

Owing to application of IT, all the major financial institutions operate nationally and have wide networks of regional offices and associated electronic networks.

The associated substantial client databases are handled via large central mainframe systems that characterize the industry.

IT has changed the working style of financial services and makes them easier and simpler for customers also.

It also reduces their cost in terms of office staff and office building.

Through the use of internet and mobile phones financial service sectors are in direct touch with their customers and with adequate databases it will be easier for service sectors to manage customer relationships. For example, through emails or SMS.

3. Wholesaling and Retailing

A visit to any large store will show that IT has become a vital part of retailing.

Retail business uses IT to carry out basic functions including till systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information and accounting.

The laser scanners used in most grocery supermarkets and superstores to read product bar codes are among the most distinctive examples of modern computer technology.

By using internet or mobile phones retailers can collect and exchange data between stores, distribution centers, suppliers and head offices.

4.Public sectors

It includes services provided by the government mainly hospitals, police stations, universities etc.

IT/IS can be used here, to keep records of the cases, respective people involved it, other related documents and can consult the existing data warehouse or databases to take appropriate actions.

5.Others

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

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

Overview of Underlying IT Technologies

we discuss some of the IT tools crucial for business growth. **(SBI-CB)**

1.Business Website

By having a website, enterprise/business becomes reachable to large amount of customers.

In addition, it can also be used in an advertisement, which is cost effective and in customer relationship management.

These websites can be designed by using **HTML, XML, ASP.NET** etc.

2.Internet and Intranet

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

Intranet is system that permits the electronic exchange of business data within an organization, mostly between managers and senior staff.

E-commerce among partners (suppliers, wholesalers, retailers, distributors) using intranets, e-mail etc. provides new platform to the business world for conducting business in a faster and easier way.

3.Software and Packages

DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making that can boost the business in the competitive world.

e.g. by having information of buying habits of customer, sales of product; marketing strategy can be built quickly and effectively with the use of data mining tools and Knowledge Discovery in Database (KDD).

These can be used in Supply chain logistics, including planning, purchasing, replenishment, logistics, and space management.

4.Business Intelligence (BI)

refers to applications and technologies that are used to collect and provide access and analyze data and information about companies' operations.

BI software consists of range of tools.

Some BI applications are used to analyze performance or internal operations e.g. EIS (executive information system), business planning, finance and budgeting tools.

While others are used to store and analyze data e.g. Data mining, data warehouses, Decision support system etc.

Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools.

A complete Business Intelligence provides consistent and standard information essential in enterprise operations.

5. Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc.

Webcam, microphone etc. are used in conducting long distance meeting.

Use of computer systems, printer; scanner increases accuracy; reduce processing times; enable decisions to be made more quickly and speed up customer service.

For example, one can charge accurate prices and eliminates the need to apply price labels to individual items by the use of scanning system.

CH-3 Protection of Information Systems

Need for Protection of Information Systems

Q. Risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by: (WIDE-UAE)

-**W**idespread use of technology
-**I**nterconnectivity of systems
-**D**evolution of management and control
-**E**limination of distance, time, and space as constraints
-**U**nevenness of technological changes
-**A**ttractiveness of conducting unconventional electronic attacks **over** more conventional physical attacks against organizations.
-**E**xternal factors such as legislative, legal, and regulatory requirements or technological developments.

Q. common aspect in each case is the critical information that each organization generates

Strategic Plans: Most of the organizations readily acknowledge that strategic plans are crucial to the success of a company.

But many of them fail to really make an effort to protect these plans.

In today's global environment, the search for competitive advantage has never been greater.

The advantages of achieving insight into a competitor's intentions can be substantial. Industry studies bear witness to this fact.

Business Operations: Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary.

As such, they may provide a market advantage to the organization.

This is the case when one company can provide a service profitably at a lower price than the competitor.

A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor.

Finances: Financial information, such as salaries and wages, are very sensitive and should not be made public.

While general salary ranges are known within industry, precise salary information can provide a competitive edge.

This information if available can help competitive enterprises to understand and re-configure their salary structure accordingly.

When competitors' costs are lower, they can either underprice the market or increase prices. In either case, the damage to an organization may be significant.

Information Security Policy

Q. Issues to address

This policy does not need to be extremely extensive, **but clearly state**

senior management's
commitment to information security,
be under change,
version control and

be signed by the appropriate senior manager.

The policy should at least address the following issues:

-definition of information security & all relevant information security responsibilities
-reasons why information security is important to the organization, and its goals and principles
-brief explanation of the security policies, principles, standards and compliance requirements
-reference to security policy manual.

Q. Members of Security Policy

3 groups of management:

Management members **who** have budget and policy authority,
Technical group **who** know what can and cannot be supported, and
Legal experts **who** know the legal ramifications of various policy charges.

Q. Information Security Policies and their Hierarchy

Information Security Policy - USP+AUP	Organization Security Policies OISP+NSSP+ICP	Conditions of Connection
User Security Policy – This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners. **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.	**Organizational Information Security Policy:** This policy sets out the Group policy for the security of its information assets and the IT systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document. **Network & System Security Policy** – This policy sets out detailed policy for system and network security and applies to IT department users. **Information Classification Policy –** This policy sets out the policy for the classification of information.	This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

Q. Components of the Security Policy – IPS-TDP-IBM-SISIIL

- Incident response and reporting mechanism
- Purpose and Scope of the Document and the intended audience
- Security policy document maintenance and compliance requirements
- The Security Infrastructure
- Description of technologies and computing structure
- Physical and Environmental Security. (PES)
- Inventory and Classification of assets
- Business Continuity Planning(BCP)
- Monitoring and Auditing Requirements (MAR)
- System Development and Maintenance Controls (SDMC)
- IT Communications (IT-C)
- Security Organization Structure (SOS)
- IT Operations management
- Identity Management and access control
- Legal Compliances.

Q. Impact of Technology on Internal Controls (A-CS-PA-A-CD-I)

Authorization Procedures:

In **manual systems**, auditors evaluate the adequacy of procedures for authorization of examining the work of employees.	In **computer systems**, authorization procedures often are embedded within a computer program.

For example: In some on-line transaction systems, written evidence of individual data entry authorization, e.g. a supervisor's signature, may be replaced by computerized authorization controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).

Competent and Trustworthy Personnel:

Personnel should have proper skill and knowledge to discharge their duties.

Substantial power is often vested in the errors responsible for the CBIS
maintained
operated,
developed, and
implemented, within organizations.

Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.

Segregation of Duties:

Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions.

The main purpose is to prevent or detect errors or irregularities by applying suitable controls.

The irregularities are frauds due to various facts like

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

From a **functional perspective**, segregation of duties should be maintained between the

Information systems use;
Data entry;
Computer operation;
Network management;
System administration;
Systems development and maintenance;
Change management;
Security administration, and
Security audit.

Physical Control over Assets and Records:

Physical control over access and records is critical in both manual systems and computer systems.

In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets.

A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located.

This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.

The nature and types of control available have changed to address these new risks.

Adequate Documents and Records:

This includes written or typed explanations of actions taken on specific transactions;

it also refers to written or typed instructions, which explain the performance of tasks.

In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system.	In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions.

Thus, no visible audit or management trail would be available to trance the transactions in a computerized system.

Adequate Management Supervision:

This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.

This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location.	In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service.

The Management's supervision and review helps to deter and detect both errors and fraud.

Comparing Recorded Accountability with Assets:

Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred.

In a manual system, independent staff prepares the basic data used for comparison purposes.	In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.

Delegation of Authority and Responsibility:

A clear line of authority and responsibility is an essential control in both manual and computer systems.

In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

Independent Checks on Performance:

In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures.	If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

Classification of Information Systems Controls

Objective of Controls	Nature of IS Resource	Audit Functions
- Preventive Controls - Detective Controls - Corrective Controls - Compensatory Controls	**(A) Environmental** -Environmental Issues and Exposures -Controls for Environmental Exposures **(B) Physical Access** -Physical Access Issues and Exposures -Controls for Physical Access Exposures **(C) Logical Access** -Logical Access Paths -Logical Access Issues and Exposures -Issues and Revelations related to Logical Access -Logical Access Control across the System	**- Managerial** 1. Top Management and Information Systems Management Controls 2. Systems Development Management Controls 3. Programming Management Controls 4. Data Resource Management Controls 5. Quality Assurance Management Controls 6. Security Management Controls 7. Operations Management Controls **- Application** 1. Boundary Controls 2. Input Controls 3. Communication Controls 4. Processing Controls 5. Database Controls 6. Output Controls

Classification on the basis of Objective of Controls

Preventive Controls: Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring.

An example of a preventive control is the use of passwords to gain access to a financial system.

The broad **characteristics** of preventive controls are as follows:

A clear-cut understanding about the vulnerabilities of the asset	Understanding probable threats	Provision of necessary controls for probable threats from materializing.

Detective Controls: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence.

An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend.

The main **characteristics** of such controls are given as follows:

Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.	An established mechanism to refer the reported unlawful activities to the appropriate person or group.	Interaction with the preventive control to prevent such acts from occurring	Surprise checks by supervisor

Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date.

A Business Continuity Plan (BCP) is considered to be a corrective control.

The main **characteristics** of the corrective controls are:

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

Compensatory Controls: Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset.

While designing the appropriate control one thing should be kept in mind - "The cost of the lock should not be more than the cost of the assets it protects."

Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls.

In such a scenario, there should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets.

Classification on the basis of "Nature of Information System Resources"

(A) Environmental Controls: These are the controls relating to IT environment such as power, air-conditioning, Un-interrupted Power Supply (UPS), smoke detection, fire- extinguishers, dehumidifiers etc.

This section deals with the **external factors** in the Information System and **preventive measures** to overcome these conflicts.

(i) Environmental Issues and Exposures: Environmental exposures are primarily due to elements of nature. However, with proper controls, exposures can be reduced.

Common occurrences are Fire, Natural calamities, Power spike, Air conditioning failure, Electrical shock, Equipment failure, Water damage/flooding-even with facilities located on upper floors of high buildings.

Water damage is a risk, usually from broken water pipes, and Bomb threat/attack.

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

Hardware and Media: This includes Computing Equipment, Communication equipment, and Storage Media.

Information Systems Supporting Infrastructure or Facilities: This typically includes Physical Premises like

Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities;	Staging Room, and Storage Areas; Communication Closets; Cabling ducts; Power Source, and Heating, Ventilation and Air Conditioning (HVAC).

Documentation: Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.

Supplies: The 3rd party maintenance procedures viz. air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.

People: employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective Information Processing Facility (IPF).

(B) Physical Access Controls

controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc.

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outsiders.

Controls for Physical Access Exposures

Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. The authorization given by the management should be explicit.

Some of the more common access control techniques are discussed categorically as follows:

(a) Locks on Doors	(b) Physical Identification medium	(c) Logging on Facilities	(d) Others
-Cipher Locks -Bolting door locks -Electronic door locks -Biometric door locks	-PIN -Plastic Cards - Identification Badges	-manual -electronic	

Cipher locks (Combination Door Locks) - Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time.

To enter, a person presses a 4-digit number, and the door will unlock for a predetermined period of time, usually 10 to 30 seconds.

Bolting Door Locks – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry, the keys should be not being duplicated.

Electronic Door Locks – A magnetic or embedded chip-based plastics card key or token may be entered into a reader to gain access in these systems.

Advantages of electronic door locks

- Through the special internal code, cards can be made to identity the correct individual.

- Restrictions can be assigned to particular doors or to particular hours of the day.

- Degree of duplication is reduced.

- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen.

- An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also parts of security.

Biometric Door Locks: These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks.

This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

Personal Identification numbers (PIN): A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual.

The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication.

His entry will be matched with the PIN number available in the security database.

Plastic Cards: These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.

Identification Badges-Special identification badges can be issued to personnel as well as visitors. For easy identification purposes, their colour of the badge can be changed.

Sophisticated photo IDs can also be utilized as electronic card keys.

Manual Logging: All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see.

Logging may happen at both fronts - reception and entrance to the computer room.

A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

Electronic Logging: This feature is a combination of electronic and biometric security systems.

The users logging can be monitored and the unsuccessful attempts being highlighted.

Dead Man Doors: These systems encompass a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only one person permitted in the holding area.

Non–exposure of Sensitive Facilities: There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.

Controlled Single Entry Point: All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.

Control of out of hours of employee-employees: Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently.

(C) Logical Access Controls

controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc.

(i) Logical Access Paths

(a) Online Terminals	(b) Dial-up ports	(c) Telecommunication Networks

(a) Online Terminals: To access an online terminal, a user has to provide a valid login-ID and password.

If additional authentication mechanisms are added along with the password, it will strengthen the security.

Operator Console – The operator console is one of the crucial places where any intruders can play havoc. Hence, access to operator console must be restricted.

This can be done by:

Keeping the operator console at a place, which is visible, to all?

By keeping the operator console in a protected room accessible to selected personnel.

(b) Dial-up Ports: Using a dial up port, user at one location can connect remotely to another computer present at an unknown location via a telecommunication media.

A modem is a device, which can convert the digital data transmitted to analog data (the one that the telecommunication device uses).

Thus, the modem can act as an interface between remote terminal and the telephone line.

Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line ensures security by confirming the presence and exactness of the data sent.

(c) Telecommunication Network: In a Telecommunication network, a number of computer terminals, Personal Computers etc. are linked to the host computer through network or telecommunication lines.

Whether the telecommunication lines could be private (i.e., dedicated to one user) or public, security is provided in the same manner as it is applied to online terminals.

(iii) Issues and Revelations related to Logical Access

Intentional or accidental exposures of logical access control encourage technical exposures, computer crimes and Asynchronous attacks. These are given as follows:

(a) Technical Exposures (7 in number)	(b) Computer Crime Exposures (7 in number)	(c) Asynchronous Attacks (5 in number)
1. Data Diddling	1. Financial Loss	1. Data Leakage
2. Bomb	2. Legal Repercussions	2. Subversive Threats
3. Trojan Horse	3. Loss of Credibility or Competitive Edge	- Invasive tap
4. Worm	4. Blackmail/Industrial Espionage	- Inductive tap
5. Rounding Down	5. Disclosure of Confidential Information	3. Wire-tapping
6. Salami Techniques	6. Sabotage	4. Piggybacking
7. Trap Doors	7. Spoofing	5. Denial of Service

Data Diddling: Data diddling involves the change of data before or after they are entered into the system.

A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.

Bomb: Bomb is a piece of bad code deliberately planted by an insider or supplier of a program.

An event, which is logical, triggers a bomb or time based.

The bombs explode when the conditions of explosion get fulfilled causing the damage immediately.

Since, these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.

Trojan Horse: These are malicious programs that are hidden under any authorized program.

Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action.

The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it.

A Trojan may:

Change or steal the password	May modify records in protected files	May allow illicit users to use the systems

Christmas Card is a well-known example of Trojan.

It was detected on internal E-mail of IBM system.

On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network.

Because of this message on other terminals, other users cannot save their half finished work.

Worm: A worm does not require a host program like a Trojan to relocate itself.

Thus, a Worm program copies itself to another machine on the network.

Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses.

Examples of worms: Existential Worm, Alarm clock Worm etc.

The **Alarm Clock worm** places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive.	**Existential worm** does not cause damage to the system, but only copies itself to several places in a computer network.

Rounding Down: This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

Salami Techniques: This involves slicing of small amounts of money from a computerized transaction or account.

A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted.

For example, in the rounding off technique, Rs. 21,23,456.39 becomes Rs.21,23,456.40, while in the Salami technique the transaction amount Rs.21,23,456.39 is truncated to either Rs.21,23,456.30 or Rs.21,23,456.00, depending on the logic.

Trap Doors: Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

Financial Loss: Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

Legal Repercussions: An organization has to adhere to many laws while developing security policies and procedures.

These laws protect both the perpetrator and organization from trial.

The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.

The IS auditor should take legal counsel while reviewing the issues associated with computer security.

Loss of Credibility or Competitive Edge: In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust.

This credibility will be shattered resulting in loss of business and prestige if security violation occurs.

Blackmail/Industrial Espionage: By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

Disclosure of Confidential, Sensitive or Embarrassing Information: These events can spoil the reputation of the organization.

Legal or regulatory actions against the company may be also a result of disclosure.

Sabotage: People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities.

They do it because of their dislike towards the organization or for their intemperance.

Spoofing: A spoofing attack involves forging one's source address.

One machine is used to impersonate the other in spoofing technique.

Spoofing occurs only after a particular machine has been identified as vulnerable.

A penetrator makes the user think that he is interacting with the operating system.

For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.

Data Leakage: Data is a critical resource for an organization to function effectively.

Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

Subversive Threats: An intruder attempts to violate the integrity of some components in the sub-system.

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

An intruder attempts to violate the integrity of some components in the sub-system by:

Invasive tap: By installing it on communication line, he may read and modify data.	**Inductive tap:** It monitors electromagnetic transmissions and allows the data to be read only.

Wire-tapping: This involves spying on information being transmitted over telecommunication network

Piggybacking: This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions.

This involves intercepting communication between the operating system and he user and modifying them or substituting new messages.

A special terminal is tapped into the communication for this purpose.

Shutting Down of the Computer/Denial of Service: This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer.

When a user establishes a connection on the Internet through TCP/IP, a **three-way** handshake takes place between

Synchronize (SYN) packets,
SYN ACK (Acknowledgement) packets and
ACK packets.

Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACK to complete the connection.

As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate requests are prevented from access.

This is known as Connection Flooding.

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

- Remote access to computer and data files through the network should be implemented.

- Having a terminal lock can assure physical security to some extent.

- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.

- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.

- In order to prevent the unauthorized user's access to the system, there should be proper control mechanisms over system documentation and manuals.

- Data transmission over remote locations should be controlled.

- The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.

- When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

Note: Logical Access Violators &
(iv) Logical Access Control across the System – both study from study material if time permits not so important.

Classification on the basis of "Audit Functions"

(A) Managerial Controls: In this part, we shall examine controls over the managerial controls that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.

The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

1. Top Management and Information Systems Management Controls

The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization.

The controls flow from the top of an organization to down; the responsibility still lies with the senior management.

Top management is responsible for preparing a master plan for the information systems function.

The senior managers who take responsibility for IS function in an organization face many challenges.

The **major functions** that a senior manager must perform are as follows:

(a) Planning	(b) Organizing	(c) Leading	(d) Controlling
- Preparing the plan - Types of Plans - Role of a Steering Committee	- Resourcing the Information Systems Function - Staffing the Information Systems Function	- Motivating and Leading Information Systems Personnel - Communicating with IS Personnel	- Overall Control of IS function - Control of Information System Activities - Control over Information System Services

(a) Planning – This includes determining the goals of the information systems function and the means of achieving these goals.

Preparing the plan: This involves the following tasks:

1. Recognizing opportunities and problems that come face to face with the organization in which Information technology and Information systems can be applied cost effectively.

2. Identifying the resources needed to provide the required information technology and information systems. and

3. Formulating strategies and tactics for acquiring the needed resources.

Types of Plans:

Top management must prepare 2 types of information systems plans for the information systems function: A Strategic plan and an Operational plan.

Strategic Plan: The Strategic Plan is the long-run plan covering, say, the next 3 to 5 years of operations;	**Operation Plan:** It is the short-plan covering, say, next 1 to 3 years of operations.

Role of a Steering Committee: The steering committee shall comprise of representatives from all areas of the business, and IT personnel.

The committee would be responsible for the overall direction of IT.

The ultimate responsibility for information systems planning should be vested in an information systems steering committee.

The steering committee should assume overall responsibility for the activities of the information systems function.

Here the responsibility lies beyond just the accounting and financial systems.

(b) Organizing - There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.

This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.

Resourcing the Information Systems Function: A major responsibility of top management is to acquire the resources needed to accomplish the goals and objectives set out in the information systems plan.

These resources include hardware, software, personnel, finances and facilities.

Adequate funding should be provided to support the acquisition and development of resources when and where they are needed.

Further, Auditors should question whether top managers have a good understanding of the role the information systems function should play in their organization.

Staffing the Information Systems Function: Staffing the Information systems function involves 3 major activities –

Acquisition of information systems personnel,
Development of information systems personnel; and
Termination of information systems personnel.

(c) Leading – This includes motivating, guiding, and communicating with personnel.

The purpose of leading is to achieve the harmony of objectives; i.e. a person's or group's objectives must not conflict with the organization's objectives.

The process of leading requires managers to motivate subordinates, direct them and communicate with them.

Motivating and Leading Information Systems Personnel: Though many theories exist, however there is no one best way of motivating and guiding all people and thus the strategies for motivating/leading people need to change depending upon particular characteristics of an individual person and his/her environment.

Communicating with IS Personnel: Effective communications are also essential to promoting good relationships and a sense of trust among work colleagues.

For example - Due to failure in understanding the directions given by the top management, a serious error is made in the system design; the effect of which is for long-term.

(d) Controlling – This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

This involves determining when the actual activities of the information system's functions deviate from the planned activities.

Overall Control of IS function: When top managers seek to exercise overall control of the information systems function, 2 questions arise:

How much the organization should be spending on the information systems function?	Is the organization getting value for the money from its information systems function?

Control of Information System Activities: Top managers should seek to control the activities on the basis of Policies and Procedures; where Policies provide broad, general guidelines for behavior whereas Standards provide specific guidelines for behavior.

New and existing staff must be made aware of the policies and procedures that govern their work.

Control over Information System Services: For each service level, estimates must be made of the expected benefits and resource consumption and finally the review committee must establish priorities.

2. Systems Development Management Controls

System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process.

It includes controls at controlling new system development activities.

The **6 activities** discussed below deal with system development controls in IT setup. **(U-SIT-UP)**

User Specification Activities: Users must be actively involved in the systems development process.

User involvement should not be ignored because of a high degree of technical complexity in the system.

Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system.

The creation of a user specification document often involves the joint efforts of the user and systems professionals.

However, it is most important that this document remains a statement of user needs.

System Authorization Activities: All systems must be properly authorized to ensure their economic justification and feasibility.

As with any transaction, system's authorization should be formal.

This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve or reject the request.

Internal Auditor's Participation: The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise.

The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. A

uditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.

Technical Design Activities: The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs.

The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design.

The adequacy of these activities is measured by the quality of the documentation that emerges from each phase.

Documentation is both a control and evidence of control and is critical to the system's long term success.

User Test and Acceptance Procedures: Just before implementation, the individual modules of the system must be tested as a unified whole.

A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing.

Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

The formal test and acceptance of the system should consider being the most important control over the SDLC. It is imperative that user acceptance be documented.

Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability.

Although discovering a major flaw at this juncture is costly, discovering the flaw during the production operations may be devastating.

Program Testing: All program modules must be thoroughly tested before they are implemented.

The results of the tests are then compared against predetermined results to identify programming and logic errors.

Program testing is time-consuming, the principal task being the creation of meaningful test data.

To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use.

This will give the auditor a frame of reference for designing and evaluating future audit tests.

Having a basis for comparison, the auditor can thus quickly verify the integrity of the program code.

On the other hand, if changes have occurred, the original test data can provide evidence regarding these changes. The auditor can thus focus attention upon those areas.

3. Programming Management Controls

The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

The program development life cycle comprises **6 major phases** –

Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases. **(PC-TO-DC)**

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
Control	The Control phase has 2 major purposes: Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations. Control over software development, acquisition, and implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.
Testing	3 types of testing can be undertaken: **Unit Testing –** which focuses on individual program modules; **Integration Testing –** Which focuses in groups of program modules; and **Whole-of-Program Testing –** which focuses on whole program. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	3 types of maintenance can be used are as follows: **Repair Maintenance –** in which program errors are corrected; **Adaptive Maintenance –** in which the program is modified to meet changing user requirements; **Perfective Maintenance -** in which the program is tuned to decrease the resource consumption.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, Bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).

4. Data Resource Management Controls

Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented.

Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

The control activities involved in maintaining the integrity of the database is as under:

1. Definition Controls: These controls are placed to ensure that the database always corresponds and comply with its definition standards.

2. Existence/Backup Controls: These ensure the existence of the database by establishing backup and recovery procedures.

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss.

Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases.

Various backup strategies are given as follows

Dual recording of data	Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.

Periodic dumping of data	This strategy involves taking a periodic dump of all or part of the database onto some backup storage medium – magnetic tape, removable disk, Optical disk etc. The dump may be scheduled.
Logging input transactions	This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump.
Logging changes to the data	This involves copying a record each time it is changed by an update action.

3. Access Controls: Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:

-User Access Controls through passwords, tokens and biometric Controls; and

-Data Encryption: Keeping the data in database in encrypted form.

4. Update Controls: These controls restrict update of the database to authorized users in two ways:

-By permitting only addition of data to the database; and

-Allowing users to change or delete existing data.

5. Concurrency Controls: These controls provide solutions, agreed-upon schedules and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.

6. Quality Controls: These controls ensure the accuracy, completeness, and consistency of data maintained in the database.

This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.

5. Quality Assurance Management Controls

Quality Assurance management is concerned with ensuring that the –

- Information systems produced by the information systems function achieve certain quality goals; and

- Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.

The reasons for the emergence of Quality assurance in many organizations are as follows:

Organizations are	- increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work. - undertaking more ambitious projects when they build software. - becoming more concerned about their liabilities if they produce and sell defective software.
- Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work, - Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned. - Improving the quality of Information Systems is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.	

6. Security Management Controls

Information security administrators are responsible for ensuring that information systems assets categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software are secure.

Assets are secure when the expected losses that will occur over some time, are at an acceptable level.

Major Security threats and their control measures

Threat	Controls
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed and sited to mitigate losses from water damage
Energy Variations	Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities like BCP, DRP, Insurance etc. must be adapted to withstand structural damages that may occur due to earthquake, snow, wind, avalanche etc.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.
Misuse of software, data and services	Code of conduct to govern the actions of information systems employees.
Hackers	Code of conduct to govern the actions of information systems employees.

However, in spite of the controls on place, there could be a possibility that a control might fail. When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls –

A Disaster Recovery Plan (DRP) and Insurance.

DRP: A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel.

Insurance: Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.

7. Operations Management Controls (DND-MPC-FC-H)

1. Computer Operations: The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available. 3 types of controls fall under this category:

Operation controls: These controls prescribe the functions that either human operators or automated operations facilities must perform.

Scheduling controls: These controls prescribe how jobs are to be scheduled on a hardware/software platform.

Maintenance controls: These controls prescribe how hardware is to be maintained in good operating order.

2. Network Operations: This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files.

Data may be lost or corrupted through component failure.

The **primary components** in the communication sub-systems are given as follows:

- Communication lines viz. twisted pair, coaxial cables, fiber optics, microwave and satellite etc.

- Hardware – ports, modems, multiplexers, switches and concentrators etc.

- Software – Packet switching software, polling software, data compression software

- Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.

3. Data Preparation and Entry: Irrespective of whether the data is obtained indirectly from source documents or directly from, say, customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the wellbeing of keyboard operators.

4. Production Control: This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

5. File Library: This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.

6. Documentation and Program Library: This involves that documentation librarians **ensure**

that documentation is stored securely;
that only authorized personnel gain access to documentation;
that documentation is kept up-to-date and

that adequate backup exists for documentation.

The documentation may **include**

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

-Each IS function must be clearly defined and documented including system software, application software, database administration etc.

-Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish the instructions that individuals must follow to compete their daily assigned tasks.

-Documented policies should exist in IS for use of IS resource; Physical security; Data security; On-line security; Use of Information systems; Reviewing, evaluating, and purchasing hardware and software; system development methodology; and Application program changes

-Job descriptions communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee.

-Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions.

7. Help Desk/Technical support: This assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and also provides the technical support for production systems by assisting with problem resolution.

8. Capacity Planning and Performance Monitoring: Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

9. Management of Outsourced Operations: This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

Application Controls and their Categories

1.Boundary Controls

The major controls of the boundary system are the access control mechanism. (ACM)

ACM links the authentic users to the authorized resources, they are permitted to access.

The ACM has 3 steps of identification, authentication and authorization with respect to the access control policy implemented.

Major Boundary Control techniques are given as follows:

Cryptography: It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file.

A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst.

Three techniques of cryptography are

transposition (permute the order of characters within a set of data),
substitution (replace text with a key-text) and
product cipher (combination of transposition and substitution).

Passwords: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.

A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, hashing of passwords and number of entry attempts.

Personal Identification Numbers (PIN): PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number.

Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.

Identification Cards: Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

Biometric Devices: Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

2. Input Controls

Source Document Controls	Data Coding Controls	Batch controls	Validation Controls

1. Source Document Controls: In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments.

Source document fraud can be used to remove assets from the organization.

For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier.

If these documents were entered into the data processing stream along with a fictitious vendor's invoice, the system could process these documents as if a legitimate transaction had taken place.

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

Use pre-numbered source documents: Source documents should come pre-numbered from the printer with a unique sequential number on each document.

Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.

Use source documents in sequence: Source documents should be distributed to the users and used in sequence.

This requires the adequate physical security be maintained over the source document inventory at the user site.

When not in use, lock and key and access to source documents should be limited to authorized persons.

Periodically audit source documents: Missing source documents should be identified by reconciling document sequence numbers.

Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors.

Documents not accounted for should be reported to management.

2. Data Coding Controls: Two types of errors can corrupt a data code and cause processing errors.

Transcription Errors (3 Classes)	Transposition Errors (2 types)
-**Addition errors** occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766. -**Truncation errors** occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327. -**Substitution errors** are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.	-**Single transposition errors** occur when two adjacent digits are reversed. For instance, **12**345 are recorded as **21**345. -**Multiple transposition errors** occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

3. Batch Controls: Batching is the process of grouping together transactions that bear some type of relationship to each other.

Various controls can be exercises over the batch to prevent or detect errors or irregularities.

Two types of batches occur:

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

4. Validation Controls: Input validation controls are intended to detect errors in the transaction data before the data are processed.

There are three levels of input validation controls:

Level-1: Field Interrogation: It involves programmed procedures that examine the characters of the data in the field.

Various field checks used to ensure data integrity have been described below: **(AP-VLCC)**

Arithmetic Checks	Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.
Picture Checks	These check against entry into processing of incorrect/invalid characters.

Valid Code Checks	Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.
Limit Check	This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre-established limits has occurred.
Check Digit	One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle.
Cross Checks	may be employed to verify fields appearing in different files to see that the result tally.

Level-2: Record Interrogation:

1. **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.

2. **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?

3. **Sequence Check:** If physical records follow a required order matching with logical records.

Level-3: File Interrogation: (VIP-DB-F)

Version usage	Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
Internal and External Labeling	Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.
Parity Check	When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.
Data File Security	Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.
Before and after Image and Logging	The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.
File Updating and Maintenance Authorization	Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.

3. Communication Controls

Physical Component Controls	Line Error Control	Flow Controls	Link Controls
Topological Controls	Channel Access Controls	Internetworking Controls	

(a) Physical Component Controls: These controls incorporate features that mitigate the possible effects of exposures.

Physical Components affecting reliability of Communication subsystem – **(TMC-PM)**

<table>
<tr><td>Transmission Media</td><td>It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types:<table><tr><td>Guided/Bound Media in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber.</td><td>In Unguided Media, the signals transmit via free-space emission like – satellite microwave, radio frequency and infrared.</td></tr></table></td></tr>
<tr><td>Modem</td><td>-Increases the speed with which data can be transmitted over a communication line.
-Reduces the number of line errors that arise through distortion if they use a process called equalization & also through noise.</td></tr>
<tr><td>Communication Lines</td><td>The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.</td></tr>
<tr><td>Port Protection Devices</td><td>Used to mitigate exposures associated with dial-up access to a computer system. The port-protection device performs various security functions to authenticate users.</td></tr>
<tr><td>Multiplexers and Concentrators</td><td>- These allow the band width or capacity of a communication line to be used more effectively.
-These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.</td></tr>
</table>

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

These errors must be detected and corrected.

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

(c) Flow Controls: Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data.

For **example**, a main frame can transmit data to a microcomputer terminal.

The microcomputer cannot display data on its screen at the same rate the data arrives from the main frame.

Moreover, the microcomputer will have limited buffer space.

Thus, it cannot continue to receive data from the mainframe and to store the data in its buffer pending display of the data on its screen.

Flow controls will be used, therefore, to prevent the mainframe swamping the microcomputer and, as a result, data is lost.

(d) Link Controls: In WANs, line error control and flow control are important functions in the component that manages the link between two nodes in a network.

The link management components mainly use 2 common protocols

HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

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

Local Area Network Topologies: Local Area Networks tend to **have 3 characteristics**:	**Wide Area Network Topologies:** Wide Area Networks have the following characteristics:

(1) they are privately owned networks; (2) they provide high -speed communication among nodes; and (3) they are confined to limited geographic areas (for example, a single floor or building or locations within a few kilometers of each other). They are implemented using **4 basic types of topologies**: (1) bus topology, (2) Tree topology, (3) Ring topology, and (4) Star topology. Hybrid topologies like the star-ring topology and the star-bus topology are also used.	1. they often encompass components that are owned by other parties (e.g. a telephone company). 2. they provide relatively low-speed communication among nodes; and 3. they span large geographic areas With the exception of the bus topology, all other topologies that are used to implement LANs can also be used to implement WANs.

(f) Channel Access Controls: Two different nodes in a network can compete to use a communication channel.

Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used.

These techniques fall into two classes: Polling methods and Contention methods.

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

(g) Internetworking Controls: Internetworking is the process of connecting two or more communication networks together to allow the users of one network to communicate with the users of other networks.

The networks connected to each other might or might not employ the same underlying hardware-software platform.

3 types of devices are used to connect sub- networks in an internet.

Device	Functions
Bridge	A bridge connects similar local area networks (e.g. one token ring network to another token ring network).
Router	A router performs all the functions of a bridge. In addition, it can connect heterogeneous Local Area Networks (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine channel availability.)
Gateway	Gateway is the most complex of the three network connection devices. The primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.

4. Processing Controls

These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. **(REFER)**

1. Run-to-run Totals: These help in verifying data that is subject to process through different stages. A specific record probably the last record can be used to maintain the control total.

2. Edit Checks: Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

3. Field Initialization: Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e. setting all values to zero/blank before inserting the field or record.

4. Exception Reports: Exception reports are generated to identify errors in the data processed. Such exception reports give the transaction code and why a particular transaction was not processed or what is the error in processing the transaction.

5. Reasonableness Verification: Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.

5. Database Controls

Major update controls (M-EPS)	Major Report controls (P-EPS)

Major update controls are given as follows: (M-EPS)

1. Maintain a suspense account: When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account.

A non- zero balance of the suspense accounts reflects the errors to be corrected.

2. Ensure All Records on Files are processed: While processing, the transaction file records mapped to the respective master file, and

the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.

3. Process multiple transactions for a single record in the correct order: Multiple transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centers).

Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.

4. Sequence Check between Transaction and Master Files: Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records.

Major Report controls are given as follows: (P-EPS)

1. Print-Run-to Run Control Totals: Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.

2. Existence/Recovery Controls: The back-up and recovery strategies together encompass the controls required to restore failure in a database.

Backup strategies are implemented using prior version and logs of transactions or changes to the database.

3. Print Suspense Account Entries: Similar to the update controls, the suspense account entries are to be periodically monitors with the respective error file and action taken on time.

4. Standing Data: Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc.

Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Any changes or errors in these tables would have an adverse effect on the organizations basic functions.

6.Output Controls

These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner.

Output can be in any form, it can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer's hard disk.

Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent.

Various Output Controls are given as follows: **(SLR-CSR)**

1. Storage and logging of sensitive, critical forms:

Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage.

Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.

2. Logging of output program executions:

When programs used for output of data are executed, these should be logged and monitored;
otherwise confidentiality/integrity of the data may be compromised.

3. Report distribution and collection controls:

Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data.

It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced.

A log should be maintained for reports that were generated and to whom these were distributed.

Where users have to collect reports the user should be responsible for timely collection of the report, especially if it is printed in a public area.

Uncollected reports should be stored securely.

4. Controls over printing:

Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place.

Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.

5. Spooling:

"Spool" is an acronym for **"Simultaneous Peripherals Operations Online".**

This is a process used to ensure that the user is able to continue working, while the print operation is getting completed.

When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk.

This file is then **"spooled"** to the printer as soon as the printer is ready to accept the data.

6. Retention controls:

Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored.

Retention control requires that a date should be determined for each output item produced.

Controls over Data Integrity and Security

For many organizations, a simple 5 scale grade will suffice as follows: **(THP-IP)**

1.Top Secret:

Highly sensitive internal information

e.g. pending mergers or acquisitions;
investment strategies;
plans or designs; that could seriously damage the organization if such information were lost or made public.

Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.

2. Highly Confidential:

Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations.

Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc., patient's medical records and similar highly sensitive data.

Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.

3. Proprietary:

Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates.

Such information is normally for proprietary use to authorized personnel only. Security at this level should be high.

4. Internal Use only:

Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility.

Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should controlled but normal.

5.Public Documents:

Information in the public domain;
annual reports, press statements etc.; which has been approved for public use.

Security at this level should minimal.

Data Integrity Policies

Major data integrity policies are given as under:

Virus-Signature Updating	Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
Software Testing	All software must be tested in a suitable test environment before installation on production systems.
Division of Environments	The division of environments into Development, Test, and Production is required for critical systems.
Offsite Backup Storage	Backups older than one month must be sent offsite for permanent storage.
Quarter & Year-End Backups	Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
Disaster Recovery	A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

The financial control techniques are numerous. **(ABCD-SSI)**

Authorization: This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.

Budgets: These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control.

Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

Cancellation of documents: This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.

Dual control: This entails having two people simultaneously access an asset.

Safekeeping: This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

Sequentially numbered documents: These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

Input/ output verification: This entails comparing the information provided by a computer system to the input documents.

This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.

Cyber Attacks

Some of the major cyber attacks are as follows:

Phishing: It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Network Scanning: It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.

Virus/Malicious Code: As per Section 43 of the Information Technology Act, 2000, "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

Spam: E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as spam.

Website Compromise/Malware Propagation: It includes website defacements. Hosting malware on websites in an unauthorized manner.

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

Financial Loss: Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.

Legal Repercussions: Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers.

Loss of credibility or Competitive Edge: News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility.

Disclosure of Confidential, Sensitive or Embarrassing Information: Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.

Sabotage: The above situation may lead to misuse of such information by enemy country.

Following are the major techniques to commit cyber frauds:

Hacking: It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.

Cracking: Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.

Data Diddling: Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.

Data Leakage: It refers to the unauthorized copying of company data such as computer files.

Denial of Service (DoS) Attack: It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.

Internet Terrorism: It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.

Logic Time Bombs: These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

Masquerading or Impersonation: In this case, perpetrator gains access to the system by pretending to be an authorized user.

Password Cracking: Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.

Piggybacking: It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.

Round Down: Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.

Scavenging or Dumpster Diving: It refers to the gaining access to confidential information by searching corporate records.

Social Engineering Techniques: In this case, perpetrator tricks an employee into giving out the information needed to get into the system.

Super Zapping: It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.

Trap Door: In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

CHAPTER-4

Business Continuity Planning and Disaster Recovery Planning

Giridhar Dande
G's publiCAtions

key terms related to BCM -B^3

Business Contingency: A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions.

Such an event could be a

power outage,
hardware failure,
fire, or storm.

If the event is very destructive, it is often called a disaster.

BCP Process: BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations.

The purpose of BCP is to ensure that vital business functions (critical business operations) are recovered and operationalized within an acceptable timeframe.

The purpose is to ensure continuity of business and not necessarily the continuity of all systems, computers or networks.

The BCP identifies the critical functions of the enterprise and the resources required to support them.

The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and incident response so as to ensure that the proper procedures will be carried out to ensure the timely restoration of services.

Business Continuity Planning (BCP): It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

It is imperative that every enterprise whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the enterprise.

It is not enough that enterprise has a BCP but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the enterprise.

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.

BCP is expected to provide:

1. Reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.

2. Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services to clients.

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

1. Proactively improves an enterprise's resilience against the disruption of its ability to achieve its key objectives

2. Provides a detailed method of restoring an enterprise's ability to supply its key products and services to an agreed level within an agreed time after a disruption, and

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

Advantages of Business Continuity

1. Is able to proactively assess the threat scenario and potential risks

2. Has planned response to disruptions which can contain the damage and minimize the impact on the enterprise, and

3. Is able to demonstrate a response through a process of regular testing and trainings.

BCM policy

Objective of this policy is to provide a structure through which

1.Critical services and activities undertaken by the enterprise operation for the customer will be identified.

2. Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.

3. Invocation of incident management and business continuity plans can be managed.

4. Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updating as required.

5. Planning and management responsibility are assigned to a member of the relevant senior management team.

Objectives and Goals of Business Continuity Planning

The key objectives of the contingency plan should be to:

1. Minimize the duration of a serious disruption to operations and resources (both information processing and other resources). **(G-2)**

2. Continue critical business operations.

3. Provide the safety and well-being of people on the premises at the time of disaster.

4. Minimize immediate damage and losses.

5. Establish management succession and emergency powers.

6. Facilitate effective co-ordination of recovery tasks. **(G-3)**

7. Identify critical lines of business and supporting functions.

8. Reduce the complexity of the recovery effort. **(G-4)**

Goals

Identify weaknesses and implement a disaster prevention program **(G-1).**

Developing a Business Continuity Plan

The methodology gives importance on the following:

1. Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan.

2. Obtaining commitment from appropriate management to support and participate in the effort.

3. Defining recovery requirements from the perspective of business functions.

4. Documenting the impact of an extended loss to operations and key business functions.

5. Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery.

6. Selecting business continuity teams that ensure the proper balance required for plan development.

7. Developing a business continuity plan that is understandable, easy to use and maintain.

8. 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.

Eight Phases

Phase-1. Pre-Planning Activities (Project Initiation)

used to obtain an understanding of the existing and projected computing environment of the organization.

This enables the project team to:

i. Refine the scope of the project and the associated work program.

ii. Develop project schedules.

iii. Identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase, a Steering Committee should be established.

The committee should have the overall responsibility for providing direction and guidance to the Project Team.

The committee should also make all decisions related to the recovery planning effort.

The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules.

Phase 2 – Vulnerability Assessment and General Definition of Requirements

This phase addresses measures to reduce the probability of occurrence.

This phase will include the following key tasks:

1. A thorough Security Assessment of the computing and communications environment including

physical security;
database security;
data and voice communications security;
systems and access control software security;
security planning and administration;
systems development and maintenance;
application controls; and

operating procedures;
personnel practices;
personal computers;
backup and contingency planning;
insurance.

2. 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.

3. 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.

4. Define the scope of the planning effort.

5. 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.

6. Develop a Plan Framework.

7.Assemble Project Team and conduct awareness sessions.

Phase 3 – Business Impact Assessment (BIA)

Enables the project team to:

1. identify critical systems, processes and functions.

2. assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities.

3. assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee.

This report identifies critical service functions and the timeframes in which they must be recovered after interruption.

The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

Phase 4 – Detailed Definition of Requirements

A profile is developed by identifying resources required to support critical functions identified in Phase 3.

This profile should include hardware, software, documentation, outside support, facilities and personnel for each business unit.

Recovery Strategies will be based on short term, intermediate term and long term outages.

Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

Phase 5 – Plan Development

During this phase, recovery plans components are defined and plans are documented.

This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations and the definition of Recovery Teams, their roles and responsibilities.

Recovery standards are also being developed during this phase.

Phase 6 – Testing Program

The plan Testing Program is developed during this phase.

Testing goals are established and alternative testing strategies are evaluated.

Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

Phase 7 – Maintenance Program

Maintenance of the plans is critical to the success of an actual recovery.

The plans must reflect changes to the environments that are supported by the plans.

It is critical that existing change management processes are revised to take recovery plan maintenance into account.

In areas, where change management does not exist, change management procedures will be recommended and implemented.

Many recovery software products take this requirement into account.

Phase 8 – Initial Plan Testing and Implementation

Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results.

Specific activities of this phase include the following – **(DI-SCAM)**

o **D**efining the test purpose/approach;
o **I**dentifying test teams.
o **S**tructuring the test.
o **C**onducting the test.
o **A**nalyzing test results.
o **M**odifying the plans as appropriate.

Components of BCM Process – 5 STAGES

BCM – Information Collection Process
BCM – Strategy Process
BCM – Development and Implementation Process
BCM – Testing and Maintenance Process
BCM – Training Process

BCM Information Collection Process – STAGE-1

- Business Impact Analysis (BIA)
- Classification of Critical Activities
- Risk Assessment

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

It enables us to refine the scope of BCP and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan.

Two other key deliverables of that phase are:

the development of a policy to support the recovery programs; and

an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

The process used for the development of both Business Impact Analysis and the Risk Assessment

Both the BIA and Risk Assessment will be reviewed as part of the annual BCM management review or following a change to the operation, its processes or associate risks.

Business Impact Analysis (BIA)

BIA is essentially a means of systematically assessing the potential impacts resulting from various events or incidents.

The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services.

It enables the business continuity team to

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

For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

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

Classification of Critical Activities – if possible see Study Material

BCP leader and BCP team leaders in consultation with respective function owner shall carry out BIA for infrastructure and business transactions.

BIA will result in

business categorization (like Vital, Desirable and Essential)
disaster scenarios (Catastrophic, major, minor trivial)

for various disaster causes (fire, flood, system failure etc.),

Risk Assessment

The risk assessment is assessment of the disruption to critical activities, which are supported by resources such as

people,
process,
technology,
information,
infrastructure supplies and stakeholders.

The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality.

It is the decision of the enterprise to select a risk assessment approach, but it is important that it is suitable and appropriate to address all of the enterprise's requirements.

Specific threats may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.

Vulnerabilities might occur as weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience.

The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist.

This is similar to vulnerability assessment phase of developing a BCP.

As a result of the BIA and the risk assessment, the enterprise should identify measures that:

- reduce the likelihood of a disruption
- shorten the period of disruption
- limit the impact of a disruption on the enterprise's key products and services.

BCM Strategy Process – STAGE-2

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources.

For example, one common preparation is to establish procedures for backing up files and applications.

Another is to establish contracts and agreements, if the contingency strategy calls for them.

Existing service contracts may need to be renegotiated to add contingency services.

Another preparation may be to purchase equipment, especially to support a redundant capability.

The enterprise may adopt any strategy but it should take into account the implementation of appropriate measures to reduce the likelihood of incidents and/ or reduce the potential impact of those incidents and resilience and mitigation measures for both critical and non-critical activities.

BCM Development and Implementation Process – STAGE-3

The enterprise should have an exclusive organization structure,

Incident Management Team / Crisis management team

for an effective response and recovery from disruptions. In the event of any incident, there should be a structure to enable the enterprise to: **C^5**

- **c**onfirm Impact of incident
- **c**ontrol of the situation
- **c**ontain the incident
- **c**ommunicate with stakeholders
- **c**oordinate appropriate response.

The Incident Management Plan (IMP)

To manage the initial phase of an incident, the crisis is handled by IMP.

The IMP should have top management support with appropriate budget for development, maintenance and training.

They should be flexible, feasible and relevant; be easy to read and understand; and provide the basis for managing all possible issues, including the stakeholder and external issues, facing the enterprise during an incident.

The Business Continuity Plan (BCP)

To recover or maintain its activities in the event of a disruption to a normal business operation, the BCP are invoked to support the critical activities required to deliver the enterprise's objectives. They may be invoked in whole or part and at any stage of the response to incident.

The recovery strategies may be two-tiered:

1.Business: Logistics, accounting, human resources, etc.

2.Technical: Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).

The plan development phase also includes the implementation of changes to use procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of recovery teams, their roles and responsibilities.

Recovery standards are also developed during this phase.

The organization's recovery strategy needs to be developed for the recovery of the many business processes.

BCM Implementation

Repeat phase-8 – if you have doubt plz check the study material.

BCM Testing and Maintenance Process – STAGE- 4

BCM Testing

A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation.

Testing may be based on a predetermined outcome, e.g. plan and scope in advance; or allow the enterprise to develop innovative solutions.

BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.) and technology and telecommunications recovery, including the availability and relocation of staff.

The frequency of testing should depend upon both the enterprise's needs, the environment in which it operates, and stakeholder requirements.

However, the testing program should be flexible, taking into account the rate of change within the enterprise, and the outcome of previous one.

In addition, it might lead to the improvement of BCM capability by:

1. Practicing the enterprise's ability to recover from an incident.

2. Verifying that the BCP incorporates all enterprise critical activities and their dependencies and priorities.

3. Highlighting assumptions, which need to be questioned.

4. Injecting confidence amongst exercise participants.

5. Raising awareness of business continuity throughout the enterprise by publicizing the exercise.

6. Validating the effectiveness and timeliness of restoration of critical activities.

7. 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:

1. The recovery procedures are complete and workable.

2. The competence of personnel in their performance of recovery procedures can be evaluated.

3. There sources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.

4. The manual recovery procedures and IT backup system/s are current and can either be operational or restored.

5. The success or failure of the business continuity training program is monitored.

BCM Maintenance

BCM maintenance process demonstrate the documented evidence of the proactive management and governance of the enterprise's business continuity program.

the key people who are to implement the BCM strategy and plans are trained and competent.

the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise's structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise's business continuity and incident management plans.

Similarly, the maintenance tasks undertaken in Development of BCP are to:

Determine	- the ownership and responsibility for maintaining the various BCP strategies within the enterprise. - the maintenance regime to ensure the plan remains up-to-date. - the maintenance processes to update the plan.

Identify	-the BCP maintenance triggers to ensure that any organisational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date.
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.

enterprise's	-BCM policy, strategies, framework and plans accurately reflect its priorities and requirements. -BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident. -BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise. -BCM maintenance and exercising programs have been effectively implemented. -has an ongoing program for BCM training and awareness
BCM	-strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program. -procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities.

-Change control processes are in place and operate effectively.

BCM Training Process – STAGE- 5

An enterprise with BCM uses training as a tool to **initiate a BCM culture** in all the stakeholders by:

-Developing a BCM program more efficiently.

-Providing confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions.

-Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels.

-Minimizing the likelihood and impact of disruptions.

Development of a BCM culture is supported by: - **(LAASE)**

-**L**eadership from senior personnel in the enterprise
-**A**ssignment of responsibilities
-**A**wareness raising
-**S**kills training
-**E**xercising plans.

Training, Awareness and Competency

While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined.

These are consistent with the competencies required by the organization of the relevant role and are given as follows:

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

Types of Plans - EBRT

There are various kinds of plans that need to be designed.

Emergency Plan	Back-up Plan	Recovery Plan	Test Plan

Emergency Plan

The emergency plan specifies the actions to be undertaken immediately when a disaster occurs.

Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack.

The actions to be initiated can vary depending on the nature of the disaster that occurs.

If an enterprise undertakes a comprehensive security review program(CSRP), the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that evoke the plan have been identified, **four** aspects of the emergency plan must be articulated.

First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'.	**Second**, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.	**Third**, any evacuation procedures required must be specified.	**Fourth**, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated.

Back-up Plan

The backup plan specifies

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

For some resources, the procedures specified in the backup plan might be straightforward.

For example
microcomputer users might be advised to make backup copies of critical files and store them off site.

In other cases, the procedures specified in the backup plan could be complex and somewhat uncertain.

For example

it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire.

The backup plan needs continuous updating as changes occur.

For example
as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly.

Indeed, it is prudent to have more than one person knowledgeable in a backup task in case someone is injured when a disaster occurs.

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 and might also indicate which applications are to be recovered first.

Members of a recovery committee must understand their responsibilities.

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 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 – FIDM

Full Backup	Incremental Backup	Differential Backup	Mirror Backup

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 back up 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 back up 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	Dis-Advantages
1. Restores are fast and easy to manage as the entire list of files and folders are in one backup set. 2. Easy to maintain and restore different versions.	1.Backups can take very long as each file is backed up again every time the full backup is run. 2. Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

Incremental Backup

An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type.

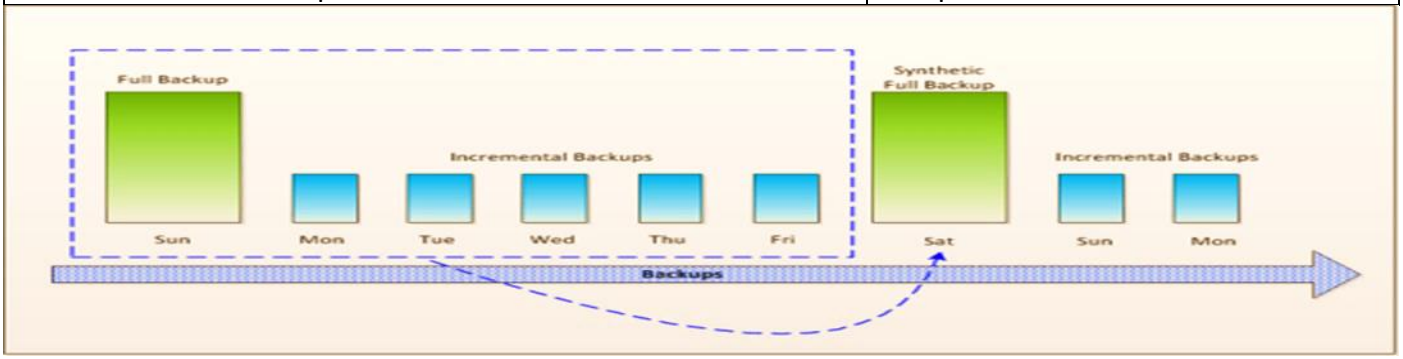
The last backup can be a full back up or simply the last incremental backup.

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 back up 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	Dis-Advantages
1. Much faster backups 2. Efficient use of storage space as files are not duplicated. Much less storage space used compared to running full backups and even differential backups.	1. Restores are slower than with a full back up and differential backups. 2. Restores are a little more complicated.



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 back up; 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 back up 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 back up, it still contains the files backed up on Tuesday.

Advantages	Dis-Advantages
1. Much faster backups then full backups. 2. 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. 3. Faster restores than incremental backups.	1. Backups are slower then incremental backups. 2. 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. 3. Restores are slower than with full backups and are a little more complicated than full backups but simpler than incremental backups.

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

Security administrators should consider the following backup options:

Cold Site

If an organisation can tolerate some downtime, cold-site backup might be appropriate.

A cold site has all the facilities needed to install a mainframe system -raised floors, air conditioning, power, communication lines, and so on.

An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

Hot Site

If fast recovery is critical, an organisation might need hot site backup.
All hardware and operations facilities will be available at the hot site.
In some cases, software, data and supplies might also be stored there.
A hot site is expensive to maintain.
They are usually shared with other organisations that have hot -site needs.

Warm Site

A warm site provides an intermediate level of backup.

It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install.

For example

a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

Reciprocal Agreement

Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster.

This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

If a 3rd-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

1. how soon the site will be made available subsequent to a disaster.

2. the number of organizations that will be allowed to use the site concurrently in the event of a disaster.

3. the priority to be given to concurrent users of the site in the event of a common disaster.

4.the period during which the site can be used.

5.the conditions under which the site can be used.

6.the facilities and services the site provider agrees to make available.

7.what controls will be in place and working at the off-site facility.

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.

- Operations managers and key employees participated in the development of the plan.

The plan	-is based upon a BIA that considers the impact of the loss of essential functions. -identifies the resources that will likely be needed for recovery and the location of their availability. -is simple and easily understood so that it will be effective when it is needed. -is realistic in its assumptions.

Information Technology

Determine	-if the plan reflects the current IT environment. -if the plan includes prioritization of critical applications and systems. -if the plan includes time requirements for recovery of each critical system, and that they are reasonable. -if a testing schedule exists and is adequate. -if weaknesses identified in the last tests were corrected.

Verify the date of the last test.

Is there a plan for alternate means of data transmission if the computer network is interrupted?

Has the security of alternate methods been considered?

Does the business resumption plan include arrangements for emergency telecommunications?

CH-5

Acquisition, Development and Implementation of Information Systems

This chapter is Divided in to 3 Divisions

Division-1 - SYSTEM DEVELOPMENT METHODOLOGY

Waterfall Model	Prototyping Model	Incremental Model	Spiral Model	RAD Model	Agile Model

Division -2 – SDLC – 8 Phases

Preliminary Investigation	Systems Requirements Analysis	Systems Design	Systems Acquisition	Systems Development	Systems Testing	Systems Implementation	Post Implementation Review and Maintenance

Division -3- Miscellaneous

Achieving System Development Objectives
Accountants' Involvement in Development Work

Division-1: SYSTEM DEVELOPMENT METHODOLOGY

SDM is a formalized, standardized, well-organized and documented set of activities used to manage a system development project.

Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations. The **methodology is characterized by the following:**

- The project is divided into a number of identifiable processes, and each process has a starting point and an ending point.

Each process comprises several activities, one or more deliverables, and several management control points.

The division of the project into these small, manageable steps facilitates both project planning and project control.

-Specific reports and other documentation, called Deliverables must be produced periodically during system development.

-Users, managers, and auditors are required to participate in the project, which generally provide approvals, often called signoffs, at pre-established management control points.

-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.

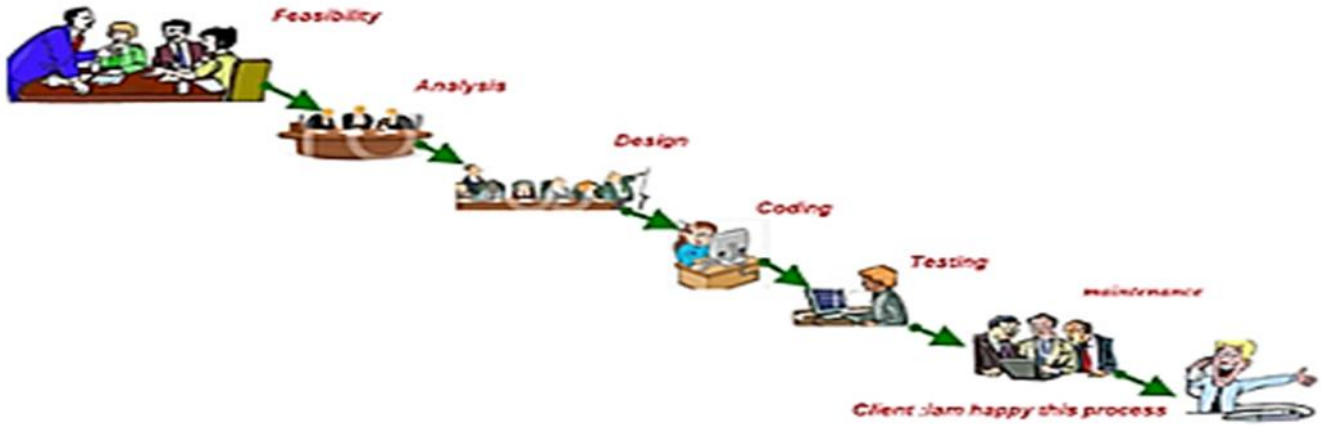
MODEL-1 Waterfall Model

The waterfall approach is a traditional development approach in which each phase is carried in sequence or linear fashion.

In this traditional approach of system development, activities are performed in sequence.

These phases include

requirements analysis,
specifications and design requirements,
coding,
final testing, and
release.



3-key characteristics are the following

1. Project is divided into sequential phases, with some overlap and splash back acceptable between phases.

2. Emphasis is on

planning,
time schedules,
target dates,
budgets and implementation of an entire system at one time.

3. Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval

by the user and IT management

occurring at the end of most phases before beginning the next phase.

4-Strengths

1.It is ideal for supporting less experienced project teams and project managers, whose composition fluctuates.

2.The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.

3.Progress of system development is measurable.

4.It enables to conserve resources.

10- Weaknesses

1. It promotes the gap between users and developers with clear vision of responsibility.

2.Written specifications are often difficult for users to read and thoroughly appreciate.

3. It leads to excessive documentation and often time-consuming.

4. It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.

5. System performance cannot be tested until the system is almost fully coded.

6. Problems are often not discovered until **system testing.**

7.Requirement inconsistencies, missing system components and unexpected development needs are often discovered during **design and coding.**

8. There is a little to iterate, which may be essential in situations.

9. Project progresses forward, with only slight movement backward.

10. It is criticized to be inflexible, slow, costly, and cumbersome due to significant structure and tight controls.

MODEL-2 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 component that is built quickly and at a lesser cost, and with the intention of modifying/replicating/expanding or even replacing it by a full-scale and fully operational system.

As users work with the prototype, they learn about the system criticalities and make suggestions about the ways to manage it.

These suggestions are then incorporated to improve the prototype, which is also used and evaluated.

Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped.

If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Prototyping can be viewed as a series of 4 steps:

The generic phases of this model are explained as follows: **(IDT-O)**

1. Identify Information System Requirements:

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

2. Develop the Initial Prototype:

The designers create an initial base model and give little or no consideration to internal controls, but instead emphasize system characteristics such as simplicity, flexibility, and ease of use.

These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents.

The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.

3.Test and Revise:

After finishing the initial prototype, the designers **first demonstrate** the model to users and then give it to them to experiment and ask users to record their likes and dislikes about the system and recommend changes.

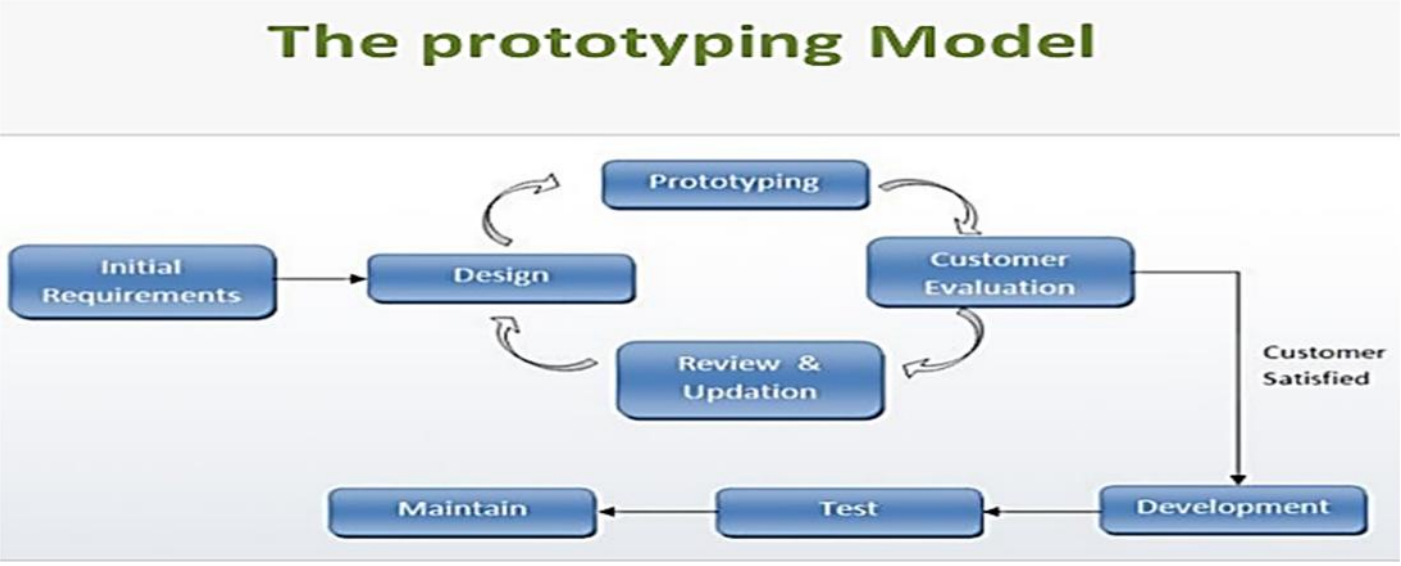
Using this feedback, the design **team modifies** the prototype as necessary and then resubmits the revised model to system users for reevaluation.

Thus iterative process of modification and reevaluation continues until the users are satisfied.

4.Obtain User Signoff of the Approved Prototype:

Users formally approve the final version of the prototype, which commits them to the current design and establishes a **contractual obligation** about what the system will, and will not, do or provide.

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



10-Strengths

1. It improves both user participation in system development and communication among project stakeholders.

2. It is especially useful for

resolving unclear objectives;
developing and validating user requirements;
experimenting with or comparing various design solutions, or
investigating both performance and the human computer interface.

3. Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.

4. It helps to easily identify, confusing or difficult functions and missing functionality.

5. It enables to generate specifications for a production application.

6. It encourages innovation and flexible designs.

7. It provides for quick implementation of an incomplete, but functional, application.

8. It typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.

9. A very short time period is normally required to develop and start experimenting with a prototype.

10. Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process.

9-Weaknesses

1. Prototyping may cause behavioral problems, if, system developers are unable to meet all user demands.

2. The interactive process of prototyping causes the prototype to be experimented with quite extensively.

3. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.

4. Prototyping can only be successful if the system users are willing to devote **significant time** in experimenting with the prototype and provide the system developers with change suggestions.

5. Prototype may not have sufficient checks and balances incorporated.

6. Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design with narrow focus that limits future system potential.

7.Requirements may frequently change significantly.

8.Identification of non-functional elements is difficult to document.

9.Approval process and control are not strict.

MODEL-3 Incremental Model

The Incremental model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished.

This model combines the elements of the waterfall model with the iterative philosophy of prototyping.

The product is decomposed into a number of components, each of which are designed and built separately (termed as builds as shown in diagram).

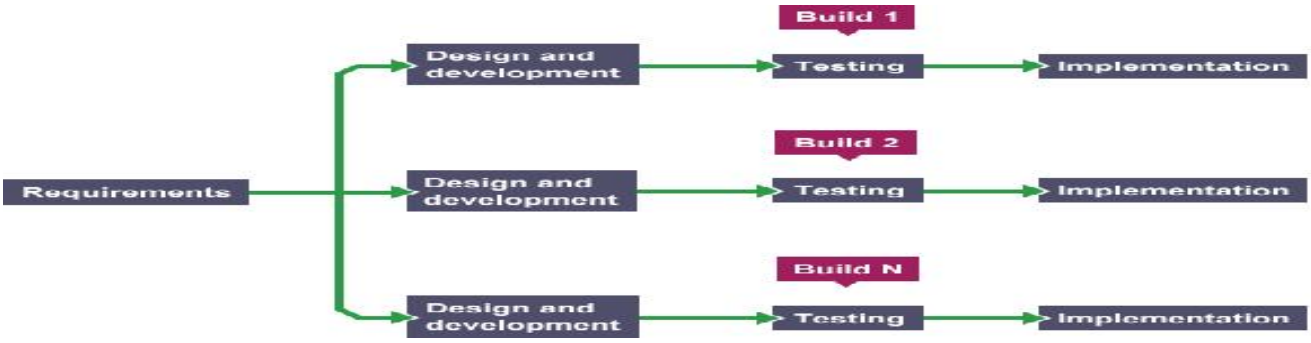
Each component is delivered to the client when it is complete.

3- few pertinent features are:

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

2. Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.

3. The initial software concept, requirement analysis, and design of architecture and system core are defined using the Waterfall approach, followed by iterative Prototyping, which comes to climax in installation of the final prototype.



7-Strengths

1. Potential exists for exploiting knowledge gained in an early increment as later increments are developed.

2. Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval by the

user and information technology management at designated major milestones.

3. Stakeholders can be given concrete evidence of project status throughout the life cycle.

4. It is more flexible and less costly to change scope and requirements.

5. It helps to mitigate integration and risks earlier in the project.

6. It allows the delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.

7. Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organization is negatively impacted.

5-Weaknesses

1. lack of overall consideration of the business problem and technical requirements for the overall system, before moving onto the next increment.

2. Each phase of an iteration is rigid and do not overlap each other.

3. Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.

4. Since some modules will be completed much earlier than others, well-defined interfaces are required.

5. It is difficult to demonstrate early success to management.

Model-4 Spiral Model

The Spiral model is a software development process combining elements of both design and prototyping-in-stages.
It tries to combine advantages of top-down and bottom-up concepts.
It combines the features of the prototyping model and the waterfall model.
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:

1. The new system requirements are defined in as much detail as possible.

This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

2. A preliminary design is created for the new system.

This phase is the most important part of "Spiral Model" in which all possible alternatives that can help in developing a cost effective project.

This phase has been added specially in order to identify and resolve all the possible risks in the project development.

If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.

3. A first prototype of the new system in constructed from the preliminary design.

This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

4. A second prototype is evolved by a 4 times procedure by evaluating the

first prototype in terms of its strengths, weaknesses, and risks;
defining the requirements of the second prototype;
planning and designing the second prototype; and
constructing and testing the second prototype.

3- Strengths

1. It enhances the risk avoidance.

2. It is useful in helping for optimal development of a given software iteration based on project risk.

3. It can incorporate Waterfall, Prototyping, and Incremental methodologies as special cases in the framework, and provide guidance as to which combination of these models best fits a given software iteration, based upon the type of project risk.

5- Weaknesses

1. There are no firm deadlines, cycles continue with no clear termination condition leading to, inherent risk of not meeting budget or schedule.

2. No established controls exist for moving from one cycle to another cycle.

Without controls, each cycle may generate more work for the next cycle.

3. A skilled and experienced project manager is required to determine how to apply it to any given project.

4. It may prove highly customized to each project, and thus is quite complex and limits reusability.

5. It is challenging to determine the exact composition of development methodologies to use for each iteration around the Spiral.

Model-5 Rapid Application Development (RAD) Model

Rapid Application Development (RAD) refers to a type of software development methodology;

which uses minimal planning in favor of rapid prototyping.

The planning of software developed using RAD is inserted pages 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.

10-Key features include the following:

1. Key objective is fast development and delivery of a high quality system at a relatively low investment cost.

2. Attempts to reduce inherent project risk by breaking a project into smaller segments and

providing more ease-of-change during the development process.

3. Aims to produce high quality systems quickly, primarily through the use of iterative Prototyping (at any stage of development), active user involvement, and computerized development tools.

4. Key emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.

5. Project control involves prioritizing development and defining delivery deadlines or “time boxes.”

6. Generally includes Joint Application Development (JAD), where users are intensely involved in system design, either through consensus building in structured workshops, or through electronically facilitated interaction.

7. Active user involvement is crucial.

8. Iteratively produces production software, as opposed to a throwaway prototype.

9. Produces documentation necessary to facilitate future development and maintenance.

10.Standard systems analysis and design techniques can be fitted into this framework.

8- Strengths

1. The operational version of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks.

2.Because RAD produces systems more quickly and to a business focus, this approach tends to produce systems at lower cost.

3. Quick initial reviews are possible.

4.Constant integration isolates problems and encourages customer feedback.

5.It holds a great level of commitment from stakeholders, both business and technical, than Waterfall, Incremental, or spiral frameworks.

6.It concentrates on essential system elements from user viewpoint.

7.It provides for the ability to rapidly change system design as demanded by users.

8.It leads to a tighter fit between user requirements and system specifications.

9- Weaknesses

1. Fast speed and lower cost may affect adversely the system quality.

2. The project may end up with more requirements than needed (gold-plating).

3. Potential for feature creep where more and more features are added to the system over the course of development.

4. It may lead to inconsistent designs within and across systems.

5. It may call for violation of programming standards related to inconsistent naming conventions and inconsistent documentation.

6. It may call for lack of attention to later system administration needs built into system.

7. Formal reviews and audits are more difficult to implement than for a complete system.

8. Tendency for difficult problems to be pushed to the future to demonstrate early success to management.

9. Since some modules will be completed much earlier than others, well–defined interfaces are required.

Model-6 Agile Model

It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Agile Manifesto is based on following 12 features:

1. Customer satisfaction by rapid delivery of useful software.
2. Welcome changing requirements, even late in development.
3. Working software is delivered frequently.
4. Working software is the principal measure of progress.
5. Sustainable development, able to maintain a constant pace.
6. Close, daily co-operation between business people and developers.
7. Face-to-face conversation is the best form of communication.
8. Projects are built around motivated individuals, who should be trusted.
9. Continuous attention to technical excellence and good design.
10. Simplicity.
11. Self-organizing teams.
12. Regular adaptation to changing circumstances.

5- Strengths

1. Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.

2. The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.

3. Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.

4. The documentation is crisp and to the point to save time.

5. The end result is generally the high quality software in least possible time duration and satisfied customer.

6- Weaknesses

1. it is difficult to assess the efforts required at the beginning of the SDLC.

2. There is lack of emphasis on necessary designing and documentation.

3. By nature, Agile projects are extremely light on documentation.

4. Agile requires more re-work and due to the lack of long-term planning and the lightweight approach to architecture.

5. The project can easily get taken off track if the customer representative is not clear about the final outcome.

6. Agile lacks the attention to outside integration.

DIVISION-2: SDLC

Perspective of the IS Audit, the following are the possible advantages

IS auditor	-can provide an evaluation of the methods and techniques used through the various development phases of the SDLC. -can have clear understanding of various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC. -if has a technical knowledge and ability of different areas of SDLC, can be a guide during the various phases of SDLC. -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.

PHASE-1 Preliminary Investigation

(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.

Managers and users may feel compelled to submit a request for a new system to the IS department, irrespective of the reason.

A system analyst is assigned to perform preliminary investigation who submits all proposals to the steering committee for evaluation to identify those projects that are most beneficial to the organization.

The analyst working on the preliminary investigation should accomplish the following objectives:**(CAR-DD)**

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

- Determine the technical and operational feasibility of alternative approaches.

(ii) Identification of objectives

After the identification of the problem, it is easy to work out and precisely specify the objectives of the proposed solution.

For instance, inability to provide a convenient reservation system, for a large number of intending passengers was the problem of the Railways.

(iii) Delineation(description) of Scope

The scope of a solution defines its typical boundaries.
It should be clear and comprehensible to the user management stating the extent and 'what will be addressed by the solution and what will not'.
Often, the scope becomes a controversial issue between development and user organizations.
Hence, drawing the scope in the beginning is essential and proves quite handy.

Moreover, while eliciting (evoking) information to delineate the scope, few aspects needs to be kept in mind:

1. Different users may represent the problem and required solution in different ways.

The system developer should evoke the need from the initiator of the project alternately called champion or executive sponsor of the project, addressing his concerns should be the basis of the scope.

2. While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization.

An understanding of their profile helps in designing appropriate user interface features.

3. While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization.

The information required has to be gathered at this stage.

4. It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities.

Solutions, which have a wide impact, are likely to be met with greater resistance.

5. While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weightage too.

These factors are to be considered from the perspective of the user management and resolved.

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

Reviewing Internal Documents: The **analysts** conducting the investigation first try to learn about the organization involved in, or affected by, the project. **For example,** to review an inventory system proposal, an analyst may try to know how does the inventory department operates and who are the managers and supervisors.	**Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about

Analysts can usually learn these details by examining organization charts and studying written operating procedures.	the nature of the project request and the reasons for submitting it.

(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**-(BROS-LEFT)**

Behavior Feasibility

It refers to the systems, which is to be designed to process data and produce the desired outputs.

However, if the data input for the system is not readily available or collectable, then the system may not be successful.

Resource Feasibility: This focuses on human resources.

Implementing sophisticated software solutions becomes difficult at specific locations because of the reluctance of skilled personnel to move to such locations.

Operational Feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility.

A system can be highly feasible in all respects except the operational and fails miserably because of human problems.

Some of the **questions, which help** in testing the operational feasibility of a project, may include the following:

Will	- the proposed system cause harm? - it produce poorer results in any respect or area? - loss of control result in any areas? - accessibility of information be lost? - individual performance be poorer after implementation than before?
-Is there sufficient support for the system from management and from users? -Are current business methods acceptable to users? -Have the users been involved in planning and development of the project?	

Schedule Feasibility:

Schedule feasibility involves the design team's estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee.

For example, if a design team projects that it will take 16 months for a particular system design to become fully functional, the steering committee **may reject** the proposal in favor of a simpler alternative that the company can implement in a shorter time frame.

Legal Feasibility:

Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations.

Any system, which is liable to violate the local legal requirements, should also be rejected.

Economic Feasibility:

It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented.

After problems or opportunities are identified, the analysts must determine the scale of response needed to meet the user's requests for a new system as well as the approximate amount of time and money that will be required in the effort.

The financial and economic **questions raised by analysts** during the preliminary investigation are for the purpose of estimating the following:

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

Financial Feasibility

The solution proposed may be prohibitively costly for the user organization.

For example, Monitoring the stock through VSAT network connecting multiple locations may be acceptable for an organization with high turnover. But this may not be a viable solution for smaller ones.

Technical Feasibility:

Essentially, an analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology.

The technical **issues usually raised** during the feasibility stage of investigation include the following:

Does	- the necessary technology exists to do what is suggested (and can it be acquired)? - the proposed equipment has the technical capacity to hold the data required to use the new system?
Can	- the proposed application be implemented with existing technology? - the system be expanded if developed?
- Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users? - Are there technical guarantees of accuracy, reliability, ease of access, and data security?	

PHASE-2 System Requirements Analysis -SRS

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

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

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

In order to accomplish the aforementioned objectives, a series of steps are taken. Such steps result in process, assuring appropriate systems requirements analysis.

A generic set of process are described as follows:**(FASS-SRI)**

1.Fact Finding

Every system is built to meet some set of needs,

for example, the need of the organization for lower operational costs, better information for managers, smooth operations for users or better levels of services to customers.

To assess these needs, the analysts often interact extensively with people, who will be benefited from the system in order to determine 'what are their actual requirements'.

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

Questionnaires: Users and managers are asked to complete questionnaire about the information systems when the traditional system development approach is chosen.

The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly.

Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.

Observation: In general, and particularly in prototyping approaches, observation plays a central role in requirement analysis.

Only by observing how users react to prototypes of a new system, the system can be successfully developed.

Documents: Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people, who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc.

Interviews: Users and managers may also be interviewed to extract information in depth.

The data gathered through interviews often provide system developers with a larger picture of the problems and opportunities.

Interviews also give analyst the opportunity to observe and record first-hand user reaction and to probe for further information.

2. Analysis of the Present System:

Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates.

Survey of existing methods, procedures, data flow, outputs, files, input and internal controls that should be intensive in order to fully understand the present system and its related problems.

The following areas should be studied in depth: **(RR-RAMU-RA)**

Reviewing Historical Aspects: A brief history of the organization is a logical starting point for an analysis of the present system.

The historical facts enable to identify the major turning points and milestones that have influenced its growth.

A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments.

Reviewing Data Files: The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval, these are used.

The system analyst should also review all on-line and off-line files, which are maintained in the organization as it will reveal information about data that are not contained in any outputs.

Reviewing Methods, Procedures and Data Communications: Methods and procedures transform input data into useful output.

A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished.

A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations.

S/he must review the types of data communication equipment including data interface, data links, modems, dial-up and leased lines and multiplexers.

The system analyst must understand how the data- communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

Analyzing Inputs: A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system.

The system analyst should be aware of various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area.

The system analyst must understand the nature of each form, 'what is contained in it', 'who prepared it', 'from where the form is initiated', 'where it is completed', the distribution of the form and other similar considerations.

Modeling the Existing System: As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the processes must be properly documented.

The flow charting and diagramming of present information not only organizes the facts, but also helps to disclose gaps and duplication in the data gathered.

It allows a thorough comprehension of the numerous details and related problems in the present operation.

Undertaking Overall Analysis of the Existing system: Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements;

the present costs-benefits of each of these must be investigated thoroughly.

Reviewing Internal Controls: A detailed investigation of the present information system is not complete until internal control mechanism is reviewed.

Locating the control points helps the analyst to visualize the essential parts and framework of a system.

An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system.

Analyzing Outputs: The outputs or reports should be scrutinized carefully by the system analysts in order to determine 'how well they will meet the organization's needs.

The analysts must understand what information is needed and why, who needs it and when and where it is needed.

Often, many reports are a carry-over from earlier days and have little relevance to current operations. Attempts should be made to eliminate all such reports in the new system.

3. System Analysis of Proposed Systems

The required systems specifications should be in conformity with the project's objectives articulated and in accordance with the following: **(MODI-W)**

-**M**ethods and procedures that show the relationship of inputs and outputs to the database, utilize data communications as, when and where deemed appropriate.

-**O**utputs are produced with great emphasis on timely managerial reports that utilize the management by exception' principle.

-**D**atabases are maintained with great accent on online processing capabilities.

-**I**nput data is prepared directly from original source documents for processing by the computer system.

-**W**ork volumes and timings are carefully considered for present and future periods including peak periods.

4. System Development Tools

Major tools	Prominent tools	
System Components and Flows User Interface Data Attributes and Relationships Detailed System Processes	-Structured English -Flowcharts -Data Flow Diagrams -Decision Tree -Decision Table	-CASE Tools - System Components Matrix -Data Dictionary - User Interface Layout and Forms

System Components and Flows: These tools help the system analysts to document the data flow among the major resources and activities of an information system.

System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities.

A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities (such as people or organizations etc.), processing activities and data storage elements.

User Interface: Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system.

Layout forms and screens are used to construct the formats and contents of input/output media and methods.

Dialogue flow diagrams analyze the flow of dialogue between computers and people.

Data Attributes and Relationships: The data resources in information system are defined, catalogued and designed by this category of tools.

A Data Dictionary catalogs the description of the attributes (characteristics) of all data elements and their relationships to each other as well as to external systems.

Entity-relationship diagrams are used to document the number and type of relationship among the entities in a system.

Detailed System Processes: These tools are used to help the programmer to develop detailed procedures and processes required in the design of a computer program.

Decision trees and decision tables use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system.

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.

A better structured, universal and precise tool is referred to as pseudo code.

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

It is a common type of chart that represents an algorithm or process showing the steps as boxes of various kinds, and their order by connecting these with arrows.

Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

Data Flow Diagrams: A Data Flow Diagram uses few simple symbols to illustrate the flow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements.

A DFD is composed of four basic elements: Data Sources and Destinations, Data Flows, Transformation processes, and Data stores.

Decision Tree: A Decision Tree is a support tool that uses a tree-like model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

Decision tree is commonly used in operations research, specifically in decision analysis, to help identify a strategy most likely to reach a goal and to calculate conditional probabilities.

5. Systems Specification

A well-documented SRS may normally contain the following sections:

Introduction: Goals, Objectives, software context, Scope and Environment of the computer-based system.

Information Description: Problem description;
Information content, flow and structure;
Hardware, software, human interfaces for external system elements and internal software functions.

Functional Description: Diagrammatic representation of functions;
Processing narrative for each function;
Interplay among functions; Design constraints.

Behavioral Description: Response to external events and internal controls.

Validation Criteria: Classes of tests to be performed to validate functions, performance and constraints.

Appendices: Data flow/Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.

SRS Review: The development team makes a presentation and then hands over the SRS document to be reviewed by the user.

The review reflects the development team's understanding of the existing processes. Only, after ensuring that the document represents existing processes accurately, the user should sign the document.

6. Roles Involved in SDLC

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

Some of the functions of Steering Committee are given as follows:

To **provide** overall directions and ensures appropriate	To be **responsible** for all cost	To **conduct** a regular review of progress of the project in the meetings of steering committee,	To **undertake** corrective actions like rescheduling, re-staffing, change in the

representation of affected parties	and timetables.	which may involve co-ordination and advisory functions	project objectives and need for redesigning.

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/programmers, who convert the users' requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.

Programmer/Developers: Programmers is a mason of the software industry, who converts design into programs by coding using programming language.

Apart from developing the application in a programming language, they also test the program for debugging activity to assure correctness and reliability

project manager: A project manager is normally responsible for more than one project and liaisonsing with the client or the affected functions.

he is responsible for delivery of the project deliverables within the time/budget and periodically reviews the progress of the project with the project leader and his team.

Phase-3 System Designing

The design phase activities includes
Architectural Design;
Physical Design;
Design of the Data Flow;
Design of the Database;
Design of the User-interface;
system software platform',

which are described briefly as follows:

Architectural design: deals with the organization of applications in terms of hierarchy of modules and sub-modules.

At this stage, we identify
major modules;
functions and scope of each module;
interface features of each module;
modules that each module can call directly or indirectly and Data received from / sent to / modified in other modules.

The architectural design is made with the help of a tool called Functional Decomposition, which can be used to represent hierarchies.

It has three elements – Module, Connection, and Couple.

The module is represented by a box and connection between them by arrows. Couple is data element that moves from one module to another and is shown by an arrow with circular tail.

physical design: the logical design is transformed into units, which in turn can be decomposed further into implementation units such as programs and modules.

During physical design, the primary concern of the auditor is effectiveness and efficiency issues.

The auditor should seek evidence that designers follow some type of structured approach like CASE tools to access their relative performance via simulations when they undertake physical design.

Some of the issues addressed here are

type of hardware for client application and server application,
Operating systems to be used,
type of networking,
processing – batch – online, real – time;
frequency of input, output; and
month-end cycles / periodical processing.

Some of the **generic design principles** being applied to develop the design of typical information systems include the following:

The design should	- be based on the analysis. - should follow standards laid down. - be modular, with high cohesion and low coupling.
- There is a tendency to develop merely one design and consider it the final product. -the recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria. - The software functions designed should be directly relevant to business activities.	

Modularity is measured by two parameters. Cohesion and Coupling.

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

Coupling is a measure of the interconnection between modules.

Design of Data flow: The design of the data flow is a major step in the conceptual design of the new system.

In designing the data flow for the proposed system, the inputs that are required are - existing data flows, problems with the present system, and objective of the new system.

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

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

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

User Interface Design: It involves determining the ways in which users will interact with a system.

The points that need to be considered while designing the user interface are - source documents to capture raw data, hard-copy output reports, screen layouts for dedicated source-document input, inquiry screens for database interrogation, graphic and color displays, and requirements for special input/output device.

System's Operating Platform: In some cases, the new system requires an operating platform including hardware, network and system software not currently available in an organization.

Auditors should be concerned about the extent to which modularity and generality are preserved in the design of the hardware/system software platform.

Phase-4 System Acquisition

Acquisition Standards: Management should establish acquisition standards that address the security and reliability issues as per current state-of-the art development standards.

Acquisition standards should focus on the following:

-Ensuring security, reliability, and functionality already built into a product;

-Ensuring manager's complete appropriate vendor, contract, and
licensing reviews and acquiring products compatible with existing systems;

-Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request -for-proposals.

-Invitations-to-tender soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software;

-Request-for-proposals soliciting bids when acquiring off-the-shelf or third-party developed software;

Other Acquisition Aspects and Practices

(i) Hardware Acquisition: In case of procuring such machinery as machine tools, transportation equipment, air conditioning equipment, etc.,

the management can normally rely on the time tested selection techniques and the objective selection criteria can be delegated to the technical specialist.

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

(ii) Software Acquisition: Once user output and input designs are finalized, the nature of the application software requirements must be assessed by the systems analyst.

This determination helps the systems development team to decide 'what type of application software products is needed' and consequently, the degree of processing that the system needs to handle.

This helps the system developers in deciding about the nature of the systems software and computer hardware that will be most suitable for generating the desired outputs, and also the functions and capabilities that the application software must possess.

At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor.

Phase-5 System Development

A good coded application and programs should have the following characteristics: (U-R-REAR)

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.

Reliability: It refers to the consistency with which a program operates over a period of time.

However, poor setting of parameters and hard coding of some data, subsequently could result in the failure of a program after some time.

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.

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.

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.

Phase-6 System Testing

Different levels/facets of Testing are described as follows.

1.Unit Testing	2.Integration Testing	3.Regression Testing	4.System Testing	5.Final Acceptance Testing

1.Unit Testing

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

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

Functional Tests: It check

'whether programs do, what they are supposed to do or not'.

The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.

Stress Tests: Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

These tests are designed to overload a program in various ways.

The purpose of a stress test is to determine the limitations of the program.

Performance Tests: Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.

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.

Unit Testing is classified as Static Testing and Dynamic Analysis Testing.

i.Static Testing: Static Analysis Tests are conducted on source programs and do not normally require executions in operating conditions. It Includes	**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.

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

Black Box Testing: Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though usually functional.

The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to uncover errors.

There is no knowledge of the test object's internal structure.

This method of test design is applicable to all levels of software testing i.e. unit, integration, functional testing, system and acceptance.

The higher the level, hence the bigger and more complex the box, the more one is forced to use black box testing to simplify.

If a module performs a function, which is not supposed to, the black box test does not identify it.

White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software.

The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs.

Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too.

It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit.

While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test.

After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

Gray Box Testing: It is a software testing technique that uses a combination of black box testing and white box testing.

In gray box testing, the tester applies a limited number of test cases to the internal workings of the software under test.

In the remaining part of the gray box testing, one takes a black box approach in applying inputs to the software under test and observing the outputs.

2. Integration Testing:

It occurs after unit testing and before system testing with an objective to evaluate the validity of connection of two or more components that pass information from one area to another.

Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

This is carried out in the following two manners:

Bottom-up Integration: It is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub - system testing, and then testing of the entire system.	**Top-down Integration:** It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module. An incomplete portion of a program code that is put under a function in order to allow the function and the program to be compiled and tested, is referred to as a stub.

Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available. The disadvantage, however is that testing of major decision / control points is deferred to a later period.	A stub does not go into the details of implementing details of the function or the program being executed. Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached. The difficulty arises in the top-down method, because the high-level modules are tested, not with real outputs from subordinate modules, but from stubs.

3. Regression Testing:

Each time a new module is added or any modification made in the software, it changes.

New data flow paths are established, new I/O may occur and new control logic is invoked.

These changes may cause problems with functions that previously worked flawlessly.

the regression tests ensure that changes or corrections have not introduced new faults.

The data used for the regression tests should be the same as the data used in the original test.

4.System Testing:

It is a process in which software and other system elements are tested as a whole.

System testing begins either when the software as a whole is operational or when the well-defined subsets of the software's functionality have been implemented.

The purpose of system testing is to ensure that the new or modified system functions properly.

These test procedures are often performed in a non-production test environment.

The types of testing that might be carried out are as follows:

Security Testing: This is the process to determine that an Information System protects data and maintains functionality as intended or not.

The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, availability authentication, authorization, and non-repudiation.

This testing technique also ensures the existence and proper execution of access controls in the new system.

Stress Testing: It is a form of testing that is used to determine the stability of a given system or entity.

It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

It may be performed by testing the application with large quantity of data during peak hours to test its performance.

Recovery Testing: This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'.

It is the forced failure of the software in a variety of ways to verify that recovery is liable to be properly performed, in actual failures.

Performance Testing: In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device.

This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

5.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:

i. 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.

ii. User Acceptance Testing: It ensures that the functional aspects expected by the users have been well addressed in the new system.

There are two types of the user acceptance testing described as follows:

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

Beta Testing: This is the second stage, generally performed after the deployment of the system.

It is performed by the external users, during the real life execution of the project.

It normally involves sending the product outside the development environment for real world exposure and receives feedback for analysis and modifications, if any.

Phase-7 System Implementation

Some of the generic activities involved in system implementation stage are described briefly as follows:

(i)Equipment Installation	**(ii) Training Personnel**	**(iii) System Change-Over Strategies (SCOS)**	**(iv) technical activities**
-Site Preparation -Installation of New Hardware / Software -Equipment Checkout		-Direct Implementation/Abrupt Change-Over -Phased Changeover -Pilot Changeover -Parallel Changeover	-Procedure Conversion -File Conversion -System conversion -Scheduling Personnel and Equipment

(i) Equipment Installation:

The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase.

An installation checklist should be developed at this time with operating advice from the vendor and system development team.

In those installations, where people are experienced in the installation of the same or similar equipment, adequate time should be scheduled to allow completion of the following activities:

Site Preparation: An appropriate location as prescribed and the typical equipment must be availed to provide an operating environment for the equipment that will meet the

vendor's temperature, humidity and dust control specifications etc.

Installation of New Hardware / Software: The equipment must be physically installed by the manufacturer, connected-to the power source and wired to communication lines, if required.

If the new system interfaces with the other systems or is distributed across multiple software platforms, some final commissioning tests of the operating environment may be desirable to prove end to end connectivity.

Equipment Checkout: The equipment must be turned on for testing under normal operating conditions.

Though the routine 'diagnostic tests' should be run by the vendor, the implementation in-house team should devise and run extensive tests of its own to ensure that equipment functionalities in actual working conditions.

(ii) Training Personnel: A system can succeed or fail depending on the way it is operated and used.

Therefore, the quality of training received by the personnel involved with the system in various capacities helps the successful implementation of information system.

Thus, training is a major component of systems implementation.

When a new system is acquired, which often involves new hardware and software, both users and computer professionals generally need some type of training.

Often, this is imparted through classes, which are organized by vendor, and through hands-on learning techniques.

(iii) System Change-Over Strategies: The Four types of popular implementation strategies are described as follows:

Direct Implementation / Abrupt Change-Over: This is achieved through an abrupt takeover – an all or no approach.

With this strategy, the changeover is done in one operation, completely replacing the old system in one go.

Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

Phased Changeover: With this strategy, implementation can be staged with conversion to the new system taking place gradually.

For example, some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases).

If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one.

Pilot Changeover: With this strategy, the new system replaces the old one in one operation but only on a small scale.

Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption.

For example - it might be tried out in one branch of the company or in one location.

If successful, then the pilot is extended until it eventually replaces the old system completely.

Parallel Changeover: This is considered the most secure method with both systems running in parallel over an introductory period.

The old system remains fully operational while the new systems come online.

With this strategy, the old and the new system are both used alongside each other, both being able to operate independently.

If all goes well, the old system is stopped and new system carries on as the only system.

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

Procedure Conversion: Operating procedures should be carefully completed with sufficient-enough documentation for the new system.

It applies to both computer- operations and functional area operations.

Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes.

Information on input, data files, methods, procedures, output, and internal control must be presented in clear, concise and understandable terms for the average reader.

File Conversion: Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed.

The cost and related problems of file conversion are significant whether they involve on-line files (common database) or off-line files.

In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested.

Adequate control, such as record counts and control totals, should be required output of the conversion program.

The existing computer files should be kept for a period of time until sufficient files are accumulated for back up.

System conversion: After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one.

All transactions initiated after this time are processed on the new system.

System development team members should be present to assist and to answer any questions that might develop.

Consideration should be given to operating the old system for some more time to permit checking, matching and balancing the total results of both systems.

Scheduling Personnel and Equipment: Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager.

As users become more familiar with the new system, the job becomes more routine. Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.

Phase-8 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?"

Some of the purposes served a Post Implementation Review ascertains the degree of success from the project, in particular, the extent to which it met its objectives, delivered planned levels of benefit, and addressed the specific requirements as originally defined.

A Post-Implementation Review should be scheduled some time after the solution has been deployed.

Typical periods range from **6 weeks to 6 months**, depending on the type of solution and its environment.

There are two basic dimensions of Information system that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly.

The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

Typical evaluations include the following:

Development Evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget.

It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained.

However, it may be noted that very few information systems have been developed on schedule and within budget.

In fact, many information systems are developed without clearly defined schedules or budgets.

Operational Evaluation: The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties.

It tries to answer the questions related to functional aspects of the system.

Such an evaluation is relatively straightforward if evaluation criteria are established in advance.

Information Evaluation: This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operational evaluations.

The objective of an information system is to provide information to a considerable extent to support the organizational decision system.

Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.

(ii) System Maintenance:

Maintenance can be categorized in the following ways:

Preventive Maintenance: Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

The long-term effect of corrective, adaptive and perfective changes increases the system's complexity.

As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it.

Corrective Maintenance: Corrective maintenance deals with fixing bugs in the code or defects found during the executions.

A defect can result from design errors, logic errors coding errors, data processing and system performance errors.

The need for corrective maintenance is usually initiated by bug reports drawn up by the end users

Scheduled Maintenance: Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks.

Rescue Maintenance: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution.

A system that is properly developed and tested should have few occasions of rescue maintenance.

Adaptive Maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system.

The term environment in this context refers to the totality of all conditions and influences, which act from outside upon the system.

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.

Division-3: Miscellaneous

Achieving System Development Objectives

An analysis on 'why organizations fail to achieve their systems development objectives' reveals bottlenecks. Some of the most notable ones are described briefly as follows:

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

Shifting User Needs: User requirements for IT are constantly changing.

As these changes accelerate, there will be more requests for Information systems development and more development projects.

When these changes occur during a development process, the development team faces the challenge of developing systems whose very purpose might change since the development process began.

Resistance to Change: People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace.

When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.

Inadequate Testing and User Training: New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.

Lack of Users' Participation: Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems.

User participation also helps to reduce user resistance to change.

(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:

Overworked or Under-Trained Development Staff: In many cases, system developers often lack sufficient educational background and requisite state of the art skills.

Furthermore, many companies do a little to help their development personnel stay technically sound, and more so a training plan and training budget do not exist.

Lack of Standard Project Management and System Development Methodologies: Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.

(iii) Management Related Issues: It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals.

Some of such bottlenecks are mentioned as follows:

Lack of Senior Management Support and Involvement: Developers and users of information systems watch senior management to determine 'which systems development projects are important' and act accordingly by shifting their efforts away from any project, which is not receiving management attention.

Development of Strategic Systems: Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.

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

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.

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

Development Costs: Development Costs for a computer based information system include costs of the system development process, like salaries of developers.

Operating Costs: Operating Costs of a computer based information system including hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.

Intangible Costs: Intangible Cost that cannot be easily measured.

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

A post implementation analysis is also done to see how the system development effort has benefitted an organization.

(ii) Computing Cost of IT Implementation and Cost Benefit Analysis: For analysis of ROI, accountants need the costs and returns from the system development efforts. For correct generation of data, proper accounting needs to be done. Accountants shall be the person to whom management shall look for the purpose.

(iii) Skills expected from an Accountant: An accountant, being an expert in accounting field must possess skills to understand the system development efforts and nuances of the same. S/he is expected to have various key skills, including understanding of the business objectives, expert book keeper, and understanding of system development efforts etc.

Ch: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: **(VMCC-HOC)**

- **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organization, which has a credible impact on its infrastructure and business competitiveness.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too.
  These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **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:**
  Unauthorized access to computer systems, malwares,
  unauthorized physical access to computer facilities and
  unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **High Costs of Computer Error:** In a computerized enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Organizational Costs of Data Loss:** Data is a critical resource of an organization for its present and future process and its ability to adapt and survive in a changing environment.
- **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 ***4 major objectives*** that are as follows: (**DASS**)

- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing.
  The importance to maintain integrity of data of an organization requires all the time.
  It is also important from the business perspective of the decision maker, competition and the market environment.
- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.
- **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- **(LAL-DNA)**

- **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record.
  In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer.
  This is normally achieved by having the client provide a computer terminal and being granted "**read**" access to the required data files.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system.
  For **example**, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month.
  The depreciation charge may be automatically transferred (journalized) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing.
  More organizations in both the public and private sector intend to make use of EDI and electronic trading over the Internet.
  This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.
- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "**on-line**" and readily accessible to the auditor.
  If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system.
  For **example**, the client's computer system may save data on detachable storage device by summarizing transactions into monthly, weekly or period end balances.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time.
  The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a tele sales system.
  The increasing use of Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.

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

- **System generated transactions:** Financial systems may have the ability to initiate, approve and record financial transactions.
- **Automated transaction processing systems** can cause the auditor problems.

For **example,** when gaining assurance that a transaction was properly authorized or in accordance with delegated authorities.
Automated transaction generation systems are frequently used in 'just in time' (JIT) inventory and stock control systems: When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier (perhaps using EDI technology).

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

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

Functions of IS Auditor

IS Auditors review risks relating to IT systems and processes; some of them are:

- Inadequate information security controls
- Inefficient use of resources, or poor governance
- Ineffective IT strategies, policies and practices
- IT-related frauds

Categories of Information Systems Audits – 5 types (TS-SIM)

- **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (end point device),
  server, and
  on the network connecting the clients and servers.
- **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.
- **Systems and Application:** An audit to verify that systems and applications
  are appropriate,
  are efficient, and
  are adequately controlled to ensure valid, reliable, timely, and
  secure input, processing, and
  output at all levels of a system's activity.

- **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.
- **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.

Steps in Information System Audit

Different audit organizations go about IS auditing in different ways and individual auditors have their own favorite ways of working. However, it can be categorized into **6 stages: - (SPF-ARC)**

- Scoping and pre-audit survey
- Planning and preparation
- Fieldwork
- Analysis
- Reporting
- Closure

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

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

(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.
SWOT (Strengths, Weaknesses, Opportunities, Threats) or
PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) Reporting: Reporting to the management is done after analysis of evidence 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.

Audit Standards and Best Practices

ISO 27001: ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS).
An ISMS is a systematic approach to manage Information security in an IS environment It encompasses people and, processes.

ISO 27001 defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large.
It is safe to say that this standard is the foundation of information security management.
It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organization as defined policies and procedures.

Many Indian IT companies have taken this certification, including INFOSYS, TCS, WIPRO.
Companies getting themselves certified by as ISO 27001, are better competitors to those not certified. Companies certified generate a greater client assurance.
It removes the dependency from individuals and put reliance on processes.

Internal Audit Standards: IIA (The Institute of Internal Auditors) is an international professional association.
This association provides dynamic leadership for the global profession of internal auditing.
IIA issued Global Technology Audit Guide (GTAG). GTAG provides management of organization about information technology management,
control, and security and
IS auditors with guidance on various information technology associated risks and recommended practices.

Basic Plan

Planning is one of the primary and important phases in an Information System Audit, which ensures that the audit is performed in an effective manner.
Planning takes more significance in case of Information Systems Audit since the audit risks are significantly impacted by ***inherent risk***.
Hence, for the audit efforts to be successful, a good audit plan is a critical success factor.
Planning develops the annual audit schedule to perform the individual audits.
It includes budgets of time and costs, and state priorities according to organizational goals and policies.
The objective of audit planning is to optimize the use of audit resources.

Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work is completed expeditiously.

Planning also assists in proper assignment of work to assistants and in coordination of the work done by other auditors and experts. Important points are given as follows:

- The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.
- Obtaining knowledge of the business is an important part of planning the work.
- The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel.
- The overall audit plan and the audit program; however, remains the auditor's responsibility.
- The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit.

- While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the auditor.

Preliminary Review

The following are some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review. – **(U-R-KLU)**

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

(ii) Risk Assessment and Materiality: Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation.
Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk (the risk of errors occurring in the area being audited).
Additionally, risk assessment will aid in planning decisions such as:

- The nature, extent, and timing of audit procedures.
- The areas or business functions to be audited.
- The amount of time and resources to be allocated to an audit.

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

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

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

- General economic factors and industry conditions affecting the entity's business,
- Nature of Business, its products & services,
- General exposure to business,
- Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
- Level of competence of the Top management and IT Management, and
- Finally, Set up and organization of IT department.

(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 audit work.
- 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.
- 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) 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.
- 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.
- finally, Studying Information Technology policies, standards, guidelines and procedures.

Risk

Risks are categorized as follows:

- Inherent Risk
- Control Risk
- Detection Risk

(i) 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.

(ii) 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.

(iii) 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.

Types of Audit Tools/continuous audit techniques

- Snapshots
- Integrated Test Facility (ITF)
- System Control Audit Review File (SCARF)
- Continuous and Intermittent Simulation (CIS)
- Audit Hooks

(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 processing authenticity, accuracy, and completeness.
This test data would be included with the normal production data used as input to the application system.
In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

Methods of Entering Test Data:

- The transactions to be tested have to be tagged.
- The application system has to be programmed to recognize the tagged transactions and have them invoke two updates, one to the application system master file record and one to the ITF dummy entity.
- Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions.
- Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing.
- However, use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing.
- The auditors may also use test data that is specially prepared.
- Test transactions would be entered along with the production input into the application system.

- In this approach the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way.
- However, preparation of the test data could be time consuming and costly.

Methods of Removing the Effects of ITF Transactions:

- The presence of ITF transactions within an application system affects the output results obtained.
- The effects of these transactions have to be removed.
- The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users.
- Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions.
- Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal.
- The effects of the transactions are not really removed.

(iii) System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions.
The information collected is written onto a special audit file- the SCARF master files.
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: **(PASS-PSP)**

- **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.
- **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.
- **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.
- **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.
- **Snapshots and Extended Records -** Snapshots and extended records can be written into the SCARF file and printed when required.
- **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*** tool.
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 simulates the application system processing.
- Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written to an exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

Advantages of continuous audit techniques are given as under:

- **Timely, Comprehensive and Detailed Auditing –** Evidence would be available more timely and in a comprehensive manner.
  The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability –** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment.
  This brings in the surprise test advantages.
- **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.

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. - need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
Continuous audit techniques	- are more likely to be used if auditors are involved in the development work associated with a new application system. - are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high. - 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 Objectives: Audit trails can be used to support security objectives in three ways: (**PDF)**

- **D**etecting unauthorized access to the system,
- **F**acilitating the reconstruction of events, and
- **P**romoting personal accountability.

Detecting Unauthorized Access:

- Detecting unauthorized access can occur in real time or after the fact.
- The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls.
- A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm.
- Depending upon how much activity is being logged and reviewed; real - time detection can impose a significant overhead on the operating system, which can degrade operational performance.
- After-the-fact detection logs can be stored electronically and reviewed periodically or as needed.
- When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

Facilitating the reconstruction of 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.

Implementing an Audit Trail: The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders.

Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls.

Audit logs, however, can generate data in overwhelming detail.

Important information can easily get lost among the superfluous detail of daily operation.
Thus, poorly designed logs can actually be dysfunctional.

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: **(CRR)**

- **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.
- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets,
  physical access threats,
  vulnerabilities of safeguards and exposures there from.
- **Review of Documents:** 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: 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 inspectors/auditors.
- Power sources and conduct tests to **assure** the quality of power, effectiveness of the power conditioning equipment, and generators.
  Also, the power supply interruptions must be checked to test the effectiveness of the back-up power.
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time to Repair) are within acceptable levels.
- Identify undesired activities such as smoking, consumption of eatables etc.

Top Management and Information Systems Management Controls

The Role of auditor at each activity is:

Planning: Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.

A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.

Organizing: Auditors should be concerned about how well top management acquires and manages staff resources for 3 reasons:

- The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.
- Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.
- Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.

Leading: Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership.

For **example** - staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function.
Auditors may use both formal and informal sources of evidence to evaluate how well top managers communicate with their staff.
The formal sources include IS plans, documents standards and policies whereas the informal sources of evidence include interviews with IS staff about their level of satisfaction with the top management.

Auditors must try to assess both the short- run and long-run consequences of poor communications within the information systems function and to assess the implications for
asset safeguarding,
data integrity,
system effectiveness, and
system efficiency.

Controlling: Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level.
Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

Audit Trails under Programming Management Controls – (CPT-COD)

Phase	Audit Trails
Planning	o They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. o They must evaluate how well the planning work is being undertaken.
Control	o They must evaluate whether the nature of and extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. o They must gather evidence on whether the control procedures are operating reliably. For **example** - they might first choose a sample of past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	o Auditors should find out whether programmers use some type of systematic approach to design. o Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.

Coding	• Auditors should seek evidence – o On the level of care exercised by programming management in choosing a module implementation and integration strategy. o To determine whether programming management ensures that programmers follow structured programming conventions. o To check whether programmers employ automated facilities to assist them with their coding work.
Testing	o Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. o Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. o Auditor's primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	o Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. o Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

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.

Boundary Controls

Accounting Audit Trail	Operations Audit Trail
1. Action privileges allowed/denied.	1. Resource usage from log-on to log-out time. 2. Log of Resource consumption.

Input Controls

Accounting Audit Trail	Operations Audit Trail
1. The identity of the person(organization) who was the source of the data. 2. The identity of the person(organization) who entered the data into the system. 3. The time and date when the data was captured. 4. The identifier of the physical device used to enter the data into the system. 5. The account or record to be updated by the transaction. 6. The standing data to be updated by the transaction; 7. The details of the transaction. 8. The number of the physical or logical batch to which the transaction belongs.	1. Time to key in a source document or an instrument at a terminal. 2. Number of read errors made by an optical scanning device. 3. Number of keying errors identified during verification. 4. Frequency with which an instruction in a command language is used. 5. Time taken to invoke an instruction using a light pen versus a mouse.

Communication Controls

Accounting Audit Trail	Operations Audit Trail
1. Unique identifier of the source/sink node. 2. Unique identifier of each node in the network that traverses the message.	1. Number of messages that have traversed each link and each node.

3. Unique identifier of the person or process authorizing dispatch of the message. 4. Time and date at which the message was dispatched. 5. Time and date at which the message was received by the sink node. 6. Time and date at which node in the network was traversed by the message. 7. Message sequence number; and the image of the message received at each node traversed in the network.	2. Queue lengths at each node; Number of errors occurring on each link or at each node. 3. Log of system restarts. 4. Message transit times between nodes and at nodes.

Processing Controls

Accounting Audit Trail	Operations Audit Trail
1. To trace and replicate the processing performed on a data item. 2. Triggered transactions to monitor input data entry, intermediate results and output data values.	1. A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used. 2. A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

Database Controls

Accounting Audit Trail	Operations Audit Trail
1. To attach a unique time stamp to all transactions, 2. To attach before-images and after-images of the data item on which a transaction is applied to the audit trail. 3. Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.	1. To maintain a chronology of resource consumption events that affects the database definition or the database.

Output Controls

Accounting Audit Trail	Operations Audit Trail
1. What output was presented to users; 2. Who received the output; 3. When the output was received; and 4. What actions were taken with the output?	1. To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

Understanding the Layers and Related Audit Issues

- Operational Layer
- Tactical Layer
- Strategic Layer

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

- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities.
  Auditor needs to always ensure the use of unique user IDs, and these needs to be traceable to individual for whom created.
  In case, guest IDs are used then test of same should also be there.
  Likewise, vendor accounts and third-party accounts should be reviewed.

In essence, users and applications should be uniquely identifiable.

- **Password Controls:** In general,
  password strength,
  password minimum length,
  password age,
  password non-repetition and
  automated lockout after 3 attempts should be set as a minimum.
  Auditor needs to check whether there are applications where password controls are weak.
  In case such instances are found, then auditor may look for compensating controls against such issues.
- **Segregation of Duties:** As frauds, due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases.
  As defined earlier, Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals.
  Example to illustrate:
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher in system, must not have right to authorize payments.
  - Maker must not be checker.

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

- **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.
- **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.
- **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.
- **Interface Security:** This relates to application interfaced with another application in an organization.
  An auditor needs to understand that data flow to and from the application.
  Security of the interfaced data is also important, especially when unencrypted methods of transmission are used for data transmission.

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

A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security.

The security policy should be supported and supplemented by detailed standards and guidelines.

These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

CH-7

Information Technology Regulatory Issues

The IT Act and its Objectives

Objectives of the Act

To give legal recognition	-to Digital signatures for authentication of any information or matter, which requires authentication under any law. -for keeping of books of accounts by banker's in electronic form. -for transactions carried out by means of EDI and other means of electronic communication.
To facilitate	-electronic filing of documents with Government departments -electronic storage of data -and give legal sanction to electronic fund transfers between banks and financial institutions.

-To amend the IPC, the IEA, 1872, the BBEA, 1891, and the RBI Act, 1934.

Section-3. Authentication of Electronic Records

-any subscriber may authenticate an electronic record by affixing his Digital Signature.

-authentication of the electronic record shall be effected by the use of ACS and HF which envelop and transform the initial electronic record into another electronic record.

"Hash function (HF)" means an algorithm translation of one sequence of bits into another, generally smaller, set known as "Hash Sum" such that an electronic record yields the same hash Sum every time the algorithm is executed with the same electronic record as its input making it computationally infeasible.

-person by the use of a public key of the **subscriber(receiver)** can verify the electronic record.

-private key and the public key are unique to the **subscriber(receiver)** and constitute a functioning key pair.

Section 3A - Electronic Signature

a subscriber(receiver) may authenticate any electronic record by such electronic signature or electronic authentication technique which-

- is considered reliable & specified in the 2nd Schedule.

any electronic signature or electronic authentication technique shall be considered reliable if-

the signature creation data	- are, within the context in which they are used, linked to the signatory or the authenticator and of no other person. - were, at the time of signing, under the control of the signatory or the authenticator and of no other person.
any alteration to the	- electronic signature made after affixing such signature is detectable. -information made after its authentication by electronic signature is detectable.

Legal Recognition of	
Electronic Records -Sec.4	**Electronic Signatures – Sec.5**
Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, such requirement shall be deemed to have been satisfied if such information or matter is - **a.** rendered or made available in an electronic form. **b.** accessible so as to be usable for a subsequent reference.	Where any law requires that any information or matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of electronic signature affixed. **Explanation: "signed",** with its grammatical variations and related expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be interpreted accordingly.

Section 6 - Use of Electronic Records and Electronic Signatures in Government and its agencies

1. Where any law provides for -

(a) the **filing** of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner.

(b) the **issue or grant** of any license, permit, sanction or approval by whatever name called in a particular manner.

(c) the **receipt** or **payment** of money in a particular manner, then, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-

(a) the **manner and format** in which such electronic records shall be filed, created or issued.	(b) the **method of payment** of any fee for filing, creation or issue any electronic record under clause (a).

Section.6A - Delivery of services by Service Provider

The Appropriate Government (AG) may, for the purposes of efficient delivery of services to the public through electronic means authorize, by order, any service provider to setup, maintain and upgrade the computerized facilities and perform such other services as it may specify by notification.

Explanation –

For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the AG to offer services through electronic means in accordance with the policy governing such service sector.

(2) The AG may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate such service charges, for the purpose of providing such services, from the person availing such service.

(3) the AG may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e- service charges by the service providers.

Section.7- Retention of Electronic Records

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if -

(a) the information contained therein remains accessible so as to be usable for a subsequent reference.

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received.

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

Section 7A. Audit of Documents, etc. maintained in Electronic form

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

Section 10. Power to make rules by Central Government in respect of Electronic Signature (ES)

The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of ES.

(b) the manner and format in which the ES shall be affixed.

(c) the manner or procedure which facilitates identification of the person affixing the ES.

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments

(e) any other matter which is necessary to give legal effect to ES.

Section 10A. Validity of contracts formed through electronic means

Where in a contract formation,
the communication of proposals,
the acceptance of proposals,
the revocation of proposals and acceptances,

as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Section 15. Secure Electronic Signature (ES)

An ES shall be deemed to be a secure electronic signature if-

(i) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person.

(ii) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Penalties, Compensation and Adjudication

Section 43. Penalty and Compensation for damage to computer, computer system, etc.

Section 43A. Compensation for failure to protect data

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Section 44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to –

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding 1 lakh and 50000 rupees for each such failure.	(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish, he shall be liable to a penalty not exceeding 5000 rupees for every day during which such failure continues;	(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding 10000 rupees for every day during which the failure continues.

Section 45. Residuary Penalty – Compensation 25000/- Penalty 25000/-

Offences

Section 65. Tampering with Computer Source Documents	Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for	Imp-3 Yrs or Fine- 2Lks or both

	a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with	
Section 66 Computer Related Offences	If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with	Imp-3 Yrs or Fine- 5 Lks or both
Section 66A Punishment for sending offensive messages through communication service, etc.	Note: A Division bench of Supreme Court decided on 24th March, 2015 in **Shreya Singhal v. Union of India** to struck down section 66A of Information Technology Act, 2000 as unconstitutional, as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Penal Code, 1860.	
Section 66B Punishment for dishonestly receiving stolen computer resource or communication device	Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with	Imp-3 Yrs or Fine- 1 Lk or both
Section 66C Punishment for identity theft	Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with	Imp-3 Yrs and Fine- 1 Lk
Section 66D Punishment for cheating by personation by using computer resource	Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with	Imp-3 Yrs or Fine- 1 Lk or both
Section 66E Punishment for violation of privacy	Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with	Imp-3 Yrs or Fine- 2 Lk or both
Section 66F Punishment for cyber terrorism	intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people or Whoever commits or conspires to commit cyber terrorism	Life
Section 67 Punishment for publishing or transmitting obscene material in electronic form	Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with	Imp-3 Yrs and Fine- 5 Lk 2nd &…. Imp-5 Yrs and Fine- 10 Lk
Section 67A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall	Imp-5 Yrs and Fine- 10 Lk 2nd &…. Imp-7 Yrs and Fine- 10 Lk

Section 67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form		Imp-5 Yrs and Fine- 10 Lk 2nd &…. Imp-7 Yrs and Fine- 10 Lk
Section 67C Preservation and Retention of information by intermediaries		Imp-3 Yrs and Fine
Section 68 Power of the Controller to give directions		Imp-2 Yrs or Fine- 1 Lk or both
Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource		Imp-7 Yrs and Fine
Section 69A Power to issue directions for blocking for public access of any information through any computer resource		Imp-7 Yrs and Fine
Section 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Any intermediary who intentionally or knowingly contravenes the provisions of sub - section (2) shall be punished with	Imp- 3 Yrs and Fine.
Section 71 Penalty for misrepresentation	Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with	Imp- 2 yrs or Fine- 1 lakh or Both
Section 72 Penalty for breach of confidentiality and privacy	has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person	Imp- 2 yrs or Fine- 1 lakh or Both
Section 72A Punishment for Disclosure of information in breach of lawful contract	has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person	Imp- 3 yrs or Fine- 5 lakh or Both

	concerned, or in breach of a lawful contract, such material to any other person	
Section 73 Penalty for publishing Electronic Signature Certificate false in certain particulars	Not issued/not accepted/revoked or suspended	Imp- 2 yrs or Fine- 1 lakh or Both
Section 74 Publication for fraudulent purpose	Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose	Imp- 2 yrs or Fine- 1 lakh or Both

Section 80. Power of police officer and other officers to enter, search, etc.

(1) any police officer, not below the rank of an Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest **without warrant** any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

"public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

Requirements of Various Authorities for System Controls & Audit

Requirements of IRDA for System Controls & Audit

It focuses on compliance with laws and regulations, which are given as follows:

(i) System Audit

All insurers shall have their systems and process audited at least once in 3 years by a CA firm.

CA firm must be having a minimum of 3-4 years' experience of IT systems of banks or mutual funds or insurance companies.

Who are not eligible: current internal or concurrent or statutory auditor.

(ii) Preliminaries.

Auditor is expected to obtain the following information at the audit location:

-Location(s) from where Investment activity is conducted.
-IT Applications used to manage the Insurer's Investment Portfolio.
-Obtain the system layout of the IT and network infrastructure including:
-Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe). -Are systems and applications hosted at a central location or hosted at different office?

-Internal circulars and guidelines of the Insurer.
-Standard Operating Procedures (SOP).
-List of new Products/funds introduced during the period under review along with IRDA approvals for the same.
-Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.

(iii) System Controls

1.There should be Electronic transfer of Data without manual intervention.
All Systems should be seamlessly integrated.
Audit Trail required at every Data entry point.
Procedures for reviewing and maintaining audit trail should be implemented.

2.The auditor should comment on the audit trail maintained in the system for various activities.

The auditor should review the Front Office Systems (FOS), MOS (Mid Office Systems) and BOS (Back Office Systems) and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.

3. Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.

Requirements of SEBI for System Controls & Audit

(i) Systems Audit:

- SEBI had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.
- The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.
- Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.
- The Auditors can perform a maximum of 3 successive audits.
- The proposal from Auditor must be submitted to SEBI for records.
- Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.
- The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report Audit has to be conducted and the Audit report be submitted to the Auditee.
- The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement.
- The report should also take previous audit reports in consideration and cover any open items therein.
- The Auditee management provides their comment about the Non-Conformities (NCs) and observations.
- For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI.
- The auditor should indicate if a follow-on audit is required to review the status of NCs.
- The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

(ii) Auditor Selection Norms:

Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc.

The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).

The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR.

It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as $(ISC)^2$.

The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.

The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository.

It should not have been engaged over the last 3 years in any consulting engagement with any departments/units of the entity being audited.

The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

Benefits of ISO 27001

- It can act as the extension of the current quality system to include security.
- It provides an opportunity to identify and manage risks to key information and systems assets.
- Provides confidence and assurance to trading partners and clients; acts as a marketing tool.
- Allows an independent review and assurance to you on information security practices.

Information Technology Infrastructure Library (ITIL)

This release of ITIL V3 brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set.

1.Service Strategy:

- The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service - provider investments in services.
- The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset.
- It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

- **IT Service Generation:** ITSM refers to the implementation and management of quality information technology services and is performed by IT service providers -
    - -through People, Process and Information Technology.
- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.
- **Financial Management:** FM aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.
- **Demand Management:** DM is a planning methodology used to manage and forecast the demand of products and services.
- **Business Relationship Management:** BRM is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.

II. Service Design:

- Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations.
- It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings.
- It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.

Service Catalogue Management: It maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers.

Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.

Service Level Management: It provides for continual identification, monitoring and review of the levels of IT services specified in the SLAs.

It is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be;

liaising with availability management,
capacity management,
incident management and problem management.

Supplier Management: The SM purpose is to obtain value for money from suppliers and contracts.

It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements.

SM oversees process of identification of

- business needs,
- evaluation of suppliers,
- establishing contracts,

- their categorization,
- management and termination.

Availability Management: Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost.

The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations.

Availability management addresses many IT component abilities like reliability, maintainability, serviceability, resilience and security to perform at an agreed level over a period of time.

Capacity Management: Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands.

The high-level activities include

- application sizing;
- workload management;
- demand management;
- modelling;
- capacity planning;
- resource management and performance management.

IT Service Continuity Management: It covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.

Information Security Management: It's basic goal is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization.

This is commonly expressed in terms of ensuring their
confidentiality, integrity and availability,

along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.

III. Service Transition:

Service Transition provides guidance on the service design and implementation ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively.

Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation.

The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations.

Knowledge Management: KM is the process of capturing, developing, sharing, and effectively using organizational knowledge.

It refers to a multi- disciplined approach to achieving organisational objectives by making the best use of knowledge.

Change management and Evaluation: This aims to ensure that standardized methods and procedures are used for efficient handling of all changes.

A change is an event that results in a new status of one or more configuration items (CIs), and which is approved by management, is cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.

Release and Deployment Management: Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure.

Service Transition Planning and Support: This process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes.

Service Asset and Configuration Management: It is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships.

Service Validation and Testing: The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.

IV. Service Operation:

Service Operation provides guidance on the management of a service through its day-to-day production life.

It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

1.Functions:

The major functions are as follows:

(i) Service Desk: service desk is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage.

Tasks include handling incidents and requests, and providing an interface for other ITSM processes.

Features include Single Point of Contact (SPOC);
Single Point of Entry and Exit; (SPEE)
easier for customers and streamlined communication channel.

(ii) Application management: ITIL application management encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

(iii) IT Operations: IT Operations primarily work from documented processes and procedures and should be concerned with a number of specific sub-processes, such as:

output management,
job scheduling,
backup and restore,
network monitoring/management,
system monitoring/management,
database monitoring/management storage monitoring/management.

(iv) IT Technical Support: IT technical support provides a number of specialist functions:
research and evaluation,
market intelligence,
proof of concept and pilot engineering,
specialist technical expertise, and
creation of documentation.

2. Request fulfillment: It focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.

3. Incident Management: It aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

4.Access Management: It is a process that focuses on granting authorized users the right to use a service, while preventing access to non-authorized users.

5.Event Management: It generates and detects notifications, while monitoring checks the status of components even when no events are occurring.

6.Problem Management: It aims to resolve the root causes of incidents and thus to minimize the adverse impact of incidents caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

V. Continual Service Improvement:(CSI)

CSI provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit.

This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services.

It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.

It provides guidance on linking improvement efforts and outcomes with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT Service Management processes.

IMPORTANT DEFINITIONS

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

"Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

"Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

CH-8: Emerging Technologies

Some pertinent similarities are highlighted as follows:

CLOUD COMPUTING	GRID COMPUTING
scalable	scalable
multi-tenancy and multitasking	multi-tenancy and multitasking
provide Service- Level Agreements (SLAs)	provide Service- Level Agreements (SLAs)

Some pertinent differences are highlighted as follows:

CLOUD COMPUTING	GRID COMPUTING
store objects as small or even several terabytes.	suited for data-intensive storage (only large)
focuses on computationally intensive operations	two types of instances: standard and high-CPU.

Goals of Cloud Computing

To meet the requirements, some of the pertinent objectives in order to achieve the goals are as follows:

1. To create a highly efficient IT ecosystem,
where resources are pooled together and

costs are aligned with what resources are actually used.

2. To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs.

3. To reduce costs related to IT energy/power consumption.

4. To consolidate IT infrastructure into a more integrated and manageable environment.

5. To access services and data from anywhere at any time.

6. To enable or improve "Anywhere Access" (AA) for ever increasing users and rapidly provision resources as needed.

Cloud Computing Architecture

A cloud computing architecture consists of a Front End and a Back End.

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

They connect to each other through a network, usually the Internet.

Front End Architecture:

The front end of the cloud computing system comprises of the client’s devices (or computer network) and some applications needed for accessing the cloud computing system.

All the cloud computing systems do not give the same interface to users.

Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft’s internet explorer or Apple’s Safari.

Other types of systems have some unique applications which provide network access to its clients.

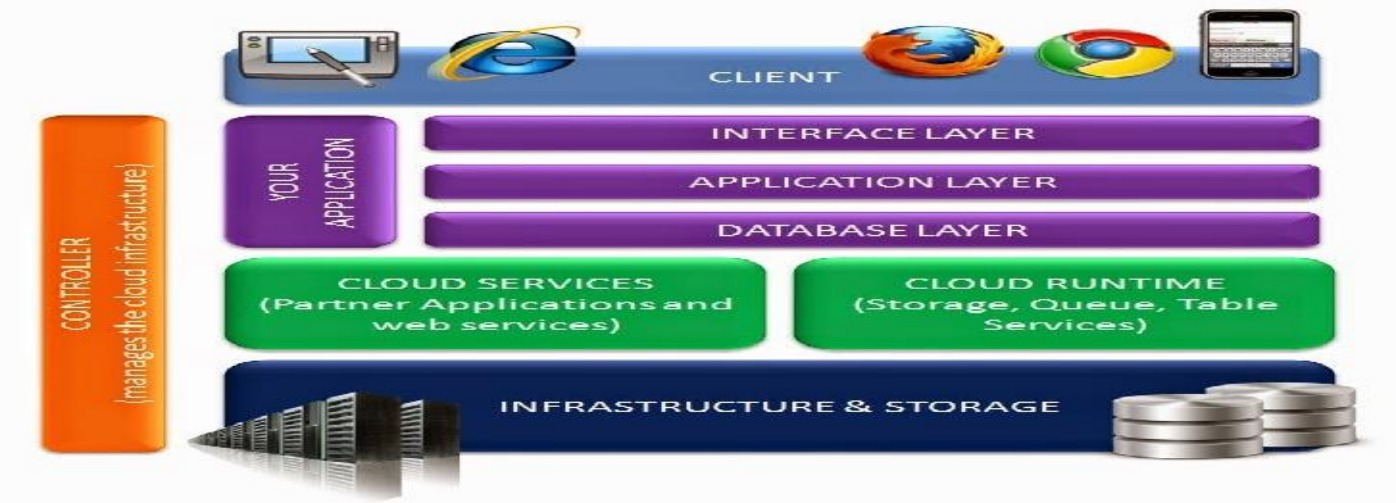
Back End Architecture:

Back end refers to some service facilitating peripherals.

In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers.

Groups of these clouds make up a whole cloud computing system.

Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment.



Cloud Computing Environment

The Cloud Computing environment can consist of multiple types of clouds based on their **deployment** and usage.

1. Private Cloud
2. Public Cloud
3. Community Cloud
4. Hybrid Cloud

1. 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 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.

Certain characteristics of Private Cloud are as follows: (SSW)

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.

Self-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 its 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

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

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.

2. Public Cloud:

These are also called Provider Clouds.

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 3rd parties or vendors over the Internet, and the services are offered on pay-per-use basis.

Public cloud consists of users from all over the world wherein a user can simply purchase resources on an hourly basis and work with the resources which are available in the cloud provider's premises.

Characteristics of Public Cloud are as follows:

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. And this does not involve any cost related to the deployment.
Less Secure	Since it is offered by a 3rd 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

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

5.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.

3.Hybrid Cloud:

This is a combination of both at least 1 private (internal) and at least 1 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. **(1st – private and then public)**

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 2 ways.

A vendor has a private cloud and forms a partnership with a public cloud provider or	a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

Characteristics of Hybrid Cloud are as follows:

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

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

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

4. 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 (eg. mission security requirements, policy, and compliance considerations).

It may be owned, managed, and operated by one or more of the organizations in the community, a 3rd 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 are as follows:

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

1.It **allows** establishing a cost effective private cloud.
2.It **allows** collaborative work on the cloud.
3.It **allows** sharing of responsibilities among the organizations.
4.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.

Cloud Computing Service Models

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	Other Cloud Service Models
different instances of IaaS -NaaS -STaaS -DBaaS -BaaS -DtaaS		different instances of SaaS -EaaS -APIaaS -Taas	-IDaaS -CaaS -DaaS -SECaaS

The National Institute of Standards and Technology (NIST) defines three basic service models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Service Model-1. Infrastructure as a Service (IaaS):

IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand.

This allows users to maximize the utilization of computing capacities without having to own and manage their own resources.

IaaS changes the computing from a physical infrastructure to a virtual infrastructure through virtual computing; storage; and network resources by abstracting the physical resources.

The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs) and design virtual infrastructure, network load balancers etc., based on their needs.

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, OpenStack and Eucalyptus.

A typical IaaS provider may provide the following services (CSNL)

Compute	Computing as a Service includes virtual CPUs and virtual main memory for the Virtual Machines (VMs) that are provisioned to the end users.
Storage	STaaS provides back-end storage for the VM images. Some of the IaaS providers also provide the back end for storing files.
Network	Network as a Service (NaaS) provides virtual networking components such as virtual router, switch, and bridge for the VMs.
Load Balancers	Load balancing as a Service may provide load balancing capability at the infrastructure layer.

Characteristics of IaaS are as follows – WCM-ES

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

Different instances of IaaS

Network as a Service (NaaS)

NaaS, provides users with needed data communication capacity to accommodate cracks 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 3 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(WBIs) 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.

DTaaS is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades.

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.

Service Model-2: 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 result in licensing - based software, whereas PaaS changes the application development from local machine to online.

For example- Google AppEngine, Windows Azure Compute etc.

Typical PaaS providers may provide - PADO

Programming Languages	PaaS providers provide a wide variety of programming languages like Java, PHP, Python, Ruby etc. for the developers to develop applications.
Application Frameworks	PaaS vendors provide application development framework like Joomla, WordPress, Sinatra etc. for application development.
Database	Along with PaaS platforms, 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: - ABCDWO

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

Service Model-3: 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, and the underlying infrastructure.
- 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.

The services provided by SaaS are:

Business Services	SaaS providers provide a variety of business services to startup companies that includes ERP, CRM, billing, sales, and human resources.
Social Networks	Since the number of users of the social networking sites is increasing exponentially, loud computing is the perfect match for handling the variable load.
Document Management	Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.
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: A-COW-HM-B

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

Different instances of SaaS

- **Email as a Service (EaaS)**

This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

- **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.

- **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.

Other Cloud Service Models

- **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.

- **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), 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.

Characteristics of Cloud Computing (H-MPV, H-MAS)

High Scalability	Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
Multi-sharing	With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
Performance	It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
Virtualization	This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
High Availability and Reliability	Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
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.
Agility	The cloud works in the 'distributed mode 'environment. It shares resources among users and tasks, while improving efficiency and agility.
Services in Pay-Per-Use Mode	SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.

Advantages of Cloud Computing (A-CAB-EQ)

Almost Unlimited Storage	Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.
Cost Efficiency	Cloud computing is probably the most cost efficient method to use, maintain and upgrade. It is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
Automatic Software Integration	In the cloud, software integration is usually something that occurs automatically. This means that we do not need to take additional efforts to customize and integrate the applications as per our preferences. This aspect usually takes care of itself. Not only that, cloud computing allows us to customize the options with great ease.
Backup and Recovery	Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
Easy Access to Information	Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
Quick Deployment	Lastly and most importantly, cloud computing gives us the advantage of quick deployment.

	Once we opt, the entire system can be fully functional in a matter of a few minutes.

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.

Components of Mobile Computing: (M^3)

1. Mobile Communication

This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.

2. 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) that use an existing and established network to operate on.

At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network (this server provide communications functionality to allow the handheld device to communicate with the internet or Intranet Infrastructure).

The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.

3. 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 of that appliance 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, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

Limitations of Mobile Computing (HP-TIPS)

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.
Potential health hazards	People who use mobile devices while driving are often distracted from driving are thus assumed to be more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
Transmission interferences	Weather, terrain, and the range from the nearest signal point can all interfere with signal reception.

	Reception in tunnels, some buildings, and rural areas is often poor.
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. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.
Power consumption	When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.
Security Standards	When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards. One can easily attack the VPN through a huge number of networks interconnected through the line.

Issues in Mobile Computing – (RBI-SLR-BEP)

Reliability, coverage, capacity, and cost

At present; wireless network is less reliable, have less geographic coverage and reduced bandwidth, are slower, and cost more than the wired-line network services.

It is important to find ways to use this new resource more efficiently by designing innovative applications.

Business challenges:

In addition to these technical challenges, mobile computing also faces business challenges.

This is due to the lack of trained professionals to bring the mobile technology to the general people and development of pilot projects for testing its capabilities.

Integration with legacy mainframe and emerging client/server applications:

Application development paradigms are changing.

As a result of the IT industry's original focus on mainframes, a huge inventory of applications using communications interfaces that are basically incompatible with mobile connectivity have been accumulated. Still the application development trend is geared towards wired network.

Security Issues: - ALI-CA

Wireless networks have relatively more security requirements than wired network. A number of approaches have been suggested and also the use of encryption has been proposed.

Availability: Ensuring authorized users getting the access they require.

Legitimate: Ensuring that only authorized users have access to services.

Integrity: Ensures unauthorized modification, destruction or creation of information cannot take place.

Confidentiality: Preventing unauthorized users from gaining access to critical information of any particular user.

Accountability: Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.

Location Intelligence

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 of operation to satellite mode as the computer moves from urban and rural areas.

In mobile computing; as computers are working in cells and are being serviced by different network providers, the physical distance may not reflect the true network distance.

A small movement may result in a much longer path if cell or network boundaries are crossed.

It will also lead to updating of the location dependent information as described above.

This can increase the network latency as well as risk of disconnection.

Service connections must be dynamically transferred to the nearest server.

Revising the technical architecture

Mobile users are demanding and are important to the business world.

To provide complete connectivity among users; the current communication technology must be revised to incorporate mobile connectivity.

Additionally, application and data architectures must also be revised to support the demands put upon them by the mobile connectivity.

Bandwidth

Bandwidth utilization can be improved by logging (bulk operations against short requests) and compression of data before transmission.

The technique of caching frequently accessed data items can play an important role in reducing contention in narrow bandwidth wireless networks.

The cached data can help improve query response time.

Since mobile clients often disconnect to conserve battery power the cached data can support disconnected operations.

End-to-end design and performance

Since mobile computing involves multiple networks (including wired) and multiple application server platforms; end-to-end technical compatibility, server capacity design, and network response time estimates are difficult to achieve.

Power Consumption

Mobile Computers will rely on their batteries as the primary power source.

Batteries should be ideally as light as possible but at the same time they should be capable of longer operation times.

Power consumption should be minimized to increase battery life.

Chips can be redesigned to operate at lower voltages.

Power management can also help Individual Components, be powered down when they are idle.

Green Computing

Green computing or Green IT refers to the study and practice of environmentally sustainable computing or IT.

Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.

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 during the product's lifetime, 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).

Green Computing Best Practices-(MR.CRD)

Some of such steps for Green IT include the following:

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 the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials. -Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.
Reduce Paper Consumption	-Reduce paper consumption by use of e-mail and electronic archiving -Use of "track changes" feature in electronic documents, rather than redline corrections on paper; -Use online marketing rather than paper based marketing. -While printing documents, make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins.
Conserve Energy	-Use LCD monitors rather than CRT monitors. -Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC. -Use notebook computers rather than desktop computers. -Power-down the CPU and all peripherals during extended periods of inactivity -Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy. -Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
Recycle	-Dispose e-waste according to central, state and local regulations.

	-Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions. -Manufacturers must offer safe end-of-life management and recycling options when products become unusable. -Recycle computers through manufacturer's recycling services.
Develop a sustainable Green Computing plan	-Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans. -Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines. -Use cloud computing so that multiple organizations share the same computing resources, thus increasing the utilization by making more efficient use of hardware resources.

Bring Your Own Device (BYOD)

Advantages of BYOD – (HI-LIE)

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.
IT reduces support requirement	IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
Lower IT budgets	The employees could involve financial savings to the organization since employees would be using the devices they already possess, thus reducing the outlay of the organization in providing devices to them.
Increased employee efficiency	The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.
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.

Types and Behavior of Social Networks

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. **Example** for this type of network is LinkedIn.

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.
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 centres.
Shopping and Utility Service Networks	The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behavior and send related information for the same to respective marts and stores.
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.
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.
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

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.

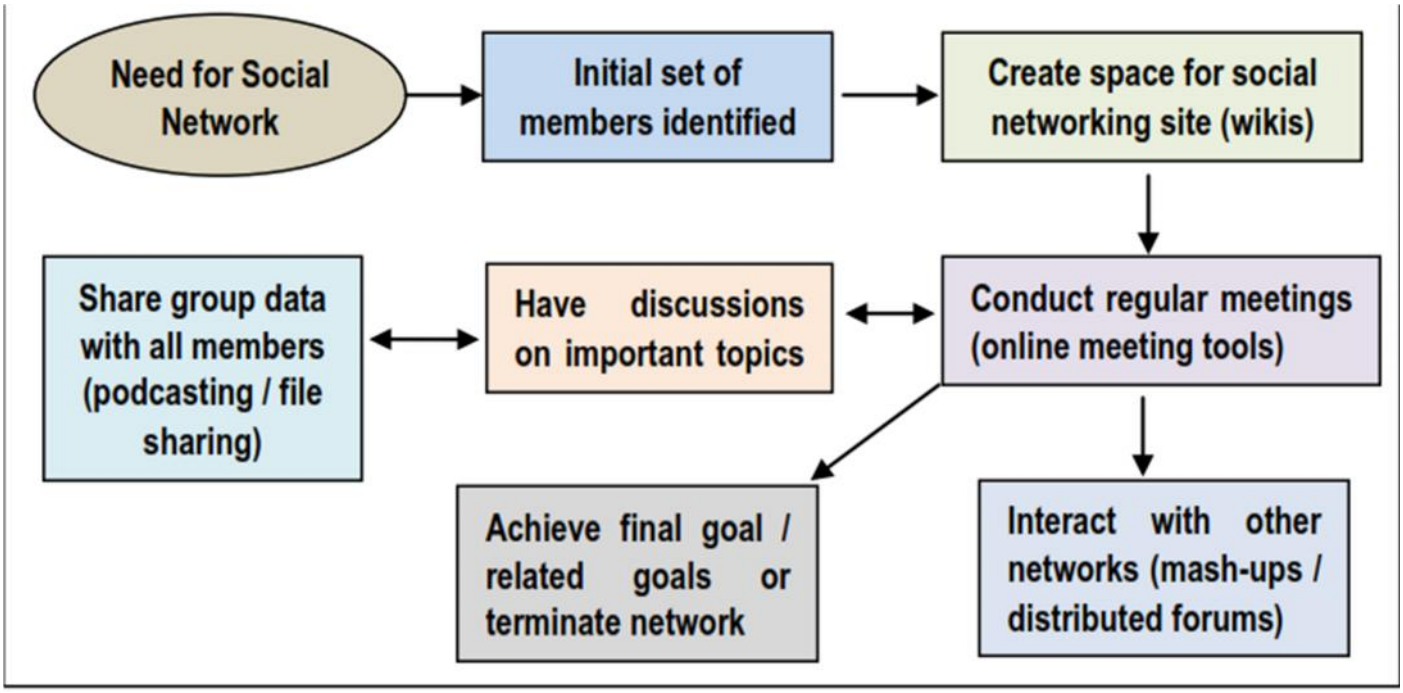
For any social network, there are a number of steps in its life cycle. In each of the life cycle step of an online social network, Web 2.0 concepts have a great influence.

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.

Picture shows - Life Cycle of Social Networks with Web 2.0



Applications of Web 2.0 –(SEM)

1. 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.

2. 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.

3. 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 such as product development, service enhancement, and promotion.

Collaboration with the business partners and consumers can be improved by the companies 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.

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 is 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 smartphones, cars and other household appliances become connected to the web, the Internet will be widespread 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. T

he 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	Web Services
This provides the web user a 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.	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.