CHAPTER -1 CONCEPTS OF GOVERANCE AND MANAGEMENT OF INFORMATION SYSTEMS

Benefits of IT governance in an organisation

- Increased value delivered.
- Increased user satisfaction.
- Improved in supporting business requirements.
- Best cost performance.
- Prevent of IT-related business risk.
- Improved transparency.
- Understanding of IT's contribution to the business.

Conformance / Corporate Governance Dimension

- It provides a historic view and focus on regulatory requirements.
- It covers
  - Roles of chairman and CEO.
  - Role and composition of the Board of Directors, Board committees.
  - Controls assurance and risk management for compliance.
- Committees are usually the nominations committee and the remuneration committee.
- SEBI are example of providing for such compliance form conformance perspective.

Performance / Business Governance Dimension

- It is a pro-active in its approach.
- It is business oriented and takes a forward looking view.
- It focus on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk.
- It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems.
- It is monitored by the audit committee.
- In contrast, the critical area of strategy does not get the same dedicated attention.

Governance of Enterprise IT (GEIT)

- It is a sub-set of corporate governance.
- It facilitates implementation of a framework if IS controls within an enterprise as relevant and encompassing all key areas.
- The objectives of GEIT is " to analyse and articulate the requirements for the governance of enterprise IT".
- It maintain effective enabling structures, principles, processes and practices with clarity of responsibilities to achieve the enterprise's mission, goals and objectives.

Benefits of Governance of Enterprise IT (GEIT)

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

Functions of IT steering committee

- Ensure that long and short-range plans of the IT department are in tune with enterprise goals & objectives.
- Establish size & scope of IT function and sets priorities within the scope.
- Review and approve major IT deployments projects in all their stages.
- Review the status of IS plans & budgets and overall IT performance.
- Review and approve standards, policies and procedures.
- To report to the Board of Directors on IT activities on a regular basis.

Key management practices, required for aligning IT strategy

- Understand enterprise direction
  - Consider the
    - Current enterprise environment.
    - Business processes.
    - Enterprise strategy.
    - Future objectives.
    - External environment of the enterprises.

- Assess the current environment, capabilities and performance
  - Assess the performance of
    - Current internal business and IT capabilities.
    - External IT services.
    - Develop an understanding of the enterprise architecture in relation to IT.
  - Consider the financial impact a potential costs and benefits of using external services.
- Define the target IT capabilities
  - Define the
    - Target business.
    - IT capabilities.
    - Required IT services.
  - IT capabilities should be based on the understanding of the enterprise environment and requirements.
- Conduct a gap analysis
  - Identify the gaps between the current and target environments and consider the alignment of assets.
  - Consider the critical success factor to support the strategy execution.
- Communicate the IT strategy and direction
  - Create awareness and understanding of the business and IT objectives.
  - Captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprises.

Key metrics used for evaluation

- Percentage of IT enabled investments through full economic life cycle.
- Percentage of IT services where expected benefits have been realized.
- Percentage of IT enabled investments where benefits are met or exceeded.
- Percentage of investments business cases with clearly defined and approved expected IT related costs and benefits.
- Percentage of IT services with clearly defined and approved operational cost and expected benefits.

Risk management strategies

- Accept the risk
  - Primary functions of management is managing risk.
  - 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 the risk
  - Risk to be associated with the use of a particular technology, supplier.
  - The risk can be eliminated by replacing the technology with more robust products & by seeking more capable suppliers.
- Share / transfer the risk
  - Risk mitigation can be shared with trading partners and suppliers.
  - Risk may be mitigated by transferring the cost of realized risk to an insurance provider.
- Treat the risk
  - Suitable controls must be devised and implemented to prevent the risk or minimize the risk.
  - Impact of the risk is very low, then management may decide to ignore the risk.

Practices for implementing risk management

- Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
- Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- Provide information on the current state of IT-related exposures and opportunities on a timely manner to all required stakeholders for appropriate response.
- Manage opportunities and reduce risk to an acceptable level as a portfolio
- Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

COBIT 5

- COBIT 5 governance challenges with 5 principles and 7 enablers.
- 5 principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders.

Five principles of COBIT 5

- Principle 1 – Meeting stakeholders needs
  - To create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources.

- COBIT 5 provides all of the required processes to support business value creation through the use of IT.
- Every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own style though the goals, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices.

- 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 focus treats information and related technologies as asset that need to be dealt with just like any other asset by everyone in the enterprise.
  - It 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.
  - COBIT 5 is a single and integrated framework as its aligns with other latest relevance standards and frameworks.
  - It 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.
  - COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.
  - Enablers are defined as anything that can help achieve the objectives of the enterprise.

- Principle 5 – Separating Governance from Management
  - The COBIT 5 framework makes a clear distinction between Governance and Management.

- Governance:
  - It ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved.
  - Overall governance is the responsibility of the Board of Directors under the leadership of the chairperson.
  - Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

- Management:
  - It plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.
  - Management is the responsibility of the executive management under the leadership of the CEO.

Enablers under COBIT 5

- Enablers are factors, individually and collectively, influence whether something will work-in this case, governance and management of enterprise IT.
- Enablers are driven by the goals cascade i.e. " what the different enablers should achieve".

1. Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
2. Processes describe an organized set of practices and activities to achieve certain objectives and procedure a set of outputs in support of achieving overall IT-related goals.
3. Organizational structures are the key decision-making entities in an enterprises.
4. Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
5. Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but

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

6. Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. Skills and competencies are linked to people and are required for successful completion of all activities for making correct decisions and taking corrective actions.

Internal auditors' review of governance, risk and compliance

- The internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic approach.
- The internal audit make appropriate recommendations of the following objectives:
  - Promoting appropriate ethics and values within the organization
  - Ensuring effective organizational performance management and accountability.
  - Communicating risk and control information to appropriate areas of the organization.
  - Co-ordinating among the board, external & internal auditors and management.
- The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- The internal audit activity must evaluate the contribute to the improvement of risk management processes.
- Risk management processes are monitored through on-going management activities, separate evaluations or both.
- The internal audit activity must evaluate risk exposures relating to the organization's governance, operations and information systems.
- The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

Key management practices for assessing and evaluating the system of internal control

- Continuously monitor, bench mark and improve the control environment and control framework to meet organizational objectives.
- Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively.

- The assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
- Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- Report on identified findings.
- Provide positive assurance opinions, where appropriate and recommendations for improvements relating to identified operational performance, external compliance and internal control system residual risks.

CHAPTER 2 – INFORMATION SYSTEMS CONCEPTS

Characteristics of computer based information systems

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has a number of interrelated and interdependent subsystems or components. No subsystems can function in isolation; it depends on other subsystems for its input.
- If one subsystem or component of a system fails; in most of the cases, the whole system does not work, However, it depends on " how the subsystems are interrelated".
- The way of subsystem work with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of the individual subsystem is of lower priority than the goal of the entire system.

Transaction processing system (TPS)

- TPS is an information system that manipulates data from business transactions.
- Business activities such as sales, purchases etc., involves transaction and these transactions are to be organized and manipulated to generate various information products for internal and external use.
- TPS will thus record and manipulate transaction data into usable information.

Activities involved in Transaction processing system (TPS)

- Capturing data and organizing in files & databases.
- Processing files and databases using application software.

- Generating information in the form of report.
- Processing queries from various quarters of the organization.

Principal components of Transaction processing system (TPS)

- Input
  - Source documents are the physical evidence of inputs into the TPS.
  - Authorizing another operation in the process, standardizing operations by indicating.
    - Which data require recording.
    - What action need to be taken.
  - Input of transactions may also be done in electronic form.
- Processing
  - This involves Journals & Registers.
  - Journals are used to record financial accounting transactions.
  - Registers are used to record other types of data not directly related to accounting.
- Storage
  - Ledgers and files provide storage of data on both manual and computerized systems.
  - The records of a firm's financial accounting transactions are
    - General ledger.
    - Accounts payable ledger.
    - Accounts receivable ledger.
- Outputs
  - Any documents generated from the system is output.
  - Financial reports summarized the results of transaction processing and express these results in accordance with the principles of financial reporting.

Features of Transaction processing systems (TPS)

- TPS is transaction oriented and generally consists of large volumes of data, it requires grater storage capacity.
- The primary objective is to ensure the data are captured quickly and correctly.
- TPS is an important source of up-to-date information regarding the operations of the enterprise.
- TPS reduces the workload of the people associated with operations and improve their efficiency by automating some of the operations.
- Benefits of TPS are tangible and easily measurable.
- TPS is the source of internal information for other information systems.
- TPS important for tactical and strategic decisions as well.

Management Information Systems (MIS

- MIS is a computer based system that provides flexible and speedy access to accurate data.
- MIS support managers at different levels to take at top level or middle level management decisions to fulfil organizational goals.
- Nature of MIS at different levels has different flavours and they are available in the form of reports, tables, graphs and charts or in presentation format using some tools.
- MIS can help in making effective, structured reports relevant for decisions of day-to-day operations.
- Reports and displays can be made available on demand, periodically or whenever exceptional conditions occur.

Characteristics of Management information systems (MIS)

- MIS is not necessarily for top management only but may also meet the information requirements of middle level.
- It is necessary that management should actively direct the system's development efforts.
- For system's effectiveness, it is necessary for management to devote sufficient amount for their 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.
- An integrated information system has the capability of generation 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.
- MIS designer must be present while development of MIS and should consider future enterprise objectives and requirements of information as per its organization structure.
- 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.
- MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system.

Misconceptions about Management information system (MIS)

- Any computer based information system is MIS.
- Any reporting system is MIS.
- MIS is a management technique.
- MIS is a bunch of technologies.
- The study of MIS is about use of computers.

- More data in reports generated results in more information to managers.
- Accuracy plays vital role in reporting.

Constraints of operating Management information system (MIS)

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing a system, which operates properly.
- Experts usually face the problem of selecting which sub-system of MIS should be installed and operated first.
- Due to varied objectives of business concerns, the approach adopted by exports for designing and implementing MIS is no-standardised.
- Non-cooperation form staff is a crucial problem, which should be handled tactfully.
- Some staff should also be involved in the development and implementation of the system to buy-in their participation.

Limitations of Management information systems (MIS)

- The quality of the outputs of MIS is basically governed by the quality of input and processes.
- MIS is not substitute for effective management, which means that it cannot replace managerial judgement in making decisions in different functional areas.
- MIS cannot provide tailor-made information packages suitable for every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative facto slide morale and attitude of members or organization.
- MIS is less useful for making non-programmed decisions. Such decisions are not routine and thus require information, which may not be available from existing MIS.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

Decision support system (DSS)

- It can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problem in their own way.
- 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 to made decisions.
- DSS supports the human decision-making process, rather than becoming a means to replace it.

Characteristics of Decision support system (DSS)

- This supports decision making and occurs at all levels of management.
- It should be able to help groups in decision making.
- It should be flexible and adaptable.
- DSS focuses on decisions rather than data and information.
- DSS can be used for solving structured problem.
- DSS should be user-friendly.
- DSS should be extensible and evolve over-time.
- DSS is used mainly for decision making rather than communicating decisions and training purposes.

Decision support system (DSS) in Accounting

- Cost accounting system
  - Managing costs in this industry requires controlling cost of supplies, expensive machinery, technology and a variety of personnel.
  - DSS can accumulate these product costs to calculate total costs per unit.
  - Managers may combine cost accounting DSS with other applications.
  - Combining the applications allow managers to measure the effectiveness of specific operation processes.
- Capital budgeting system
  - Decision makers need to supplement analytical techniques such as NPV, IRR with decision support tools that consider some benefits of new technology not captured in strict financial analysis.
  - Using this DSS, accountants, managers and engineers identify and prioritize to consider the financial, non-financial, quantitative and qualitative factors in their decision-making processes.
- Budget variance analysis system
  - A computerized DSS to generate monthly variance reports for division comptrollers.
  - The system allows these comptrollers to graph, view, analyse and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the system.
  - The DSS thus helps the comptrollers create and control budgets for the cost-centre mangers reporting to them.
- General decision support system
  - Planning languages used in DSS are general purpose and therefore have the ability to analyse many different types of problems.
  - These type of DSS are a decision-maker's tools.

- Expert choice analysis these judgements and presents the decision maker with the best alternative.

Expert

- An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to solve a problem.
- Expert System is software system that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such experts.
- A characteristic of Expert System is its ability to declare or explain the reasoning process that was used to make decisions.
- Some of the business applications of Expert System are:
  - **Accounting and Finance:** It provides tax advice and assistance, helping with credit authorization decisions, selecting forecasting models, providing investment advice.
  - **Marketing:** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centres, assisting with marketing timing decisions, determining discount policies.
  - **Manufacturing:** It helps in determining whether a process is running correctly, analysing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and facility layouts.
  - **Personnel:** It is useful in assessing applicant qualifications, giving employees assistance in filling out forms.
  - **General Business:** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

Benefits of Experts

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

Implications of Information Systems in business

- Information Systems help managers in efficient decision-making to achieve organizational goals.
- An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.
- Information Systems help in making right decision at the right time i.e. just on time.
- A good Information System may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though Information systems may be utilized by managers in unusual situations.
- Information System is viewed as a process; it can be integrated to formulate a strategy of action or operation.

Information

- Information means processed data that have been put into a meaningful and useful context.
- Data consists of facts, values or results, and information is the result of relation between data.
- Information is essential because it adds knowledge, helps in decision making, analysing the future and taking action in time.
- Information products produced by an information system can be represented by number of ways.

Attributes of Information

- It is a very important aspect of information. Information is useless if it is not available at the time of need.
- Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data.
- The modes of communicating information to humans should be in such a way that it can be easily understand by the people.
- Format also plays an important role in communicating the idea.
- The information should be refreshed from time to time as it usually rots with time and usage.
- It is a measure of failure or success of using information for decision making. If information leads to correct decision on many occasions, we say the information is reliable.
- It means the correctness of information. For example, the correct status of inventory is highly required.
- Validity measures how close the information is to the purpose for which it asserts to serve.

Executive Information Systems

- It is sometimes referred to as an Executive Support System.
- It serves the top level managers of the organization.
- ESS creates a generalized computing and communications environment rather than providing any pre-set applications or specific competence.

Characteristics of Executive Information Systems

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

CHAPTER – 3 PROTECTION OF INFORMATION SYSTEMS

Various types of Information Security polices and their hierarchy

- This policy sets out the responsibilities and requirements for all IT system users.
- This sets out the policy for acceptable use of email, Internet services and other IT resources.
- This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information.
- This policy sets out detailed policy for system and network security and applies to IT department users.
- This policy sets out the policy for the classification of information.
- This policy sets out the Group policy for connecting to the network.

Key components of a good security policy

- The Security Infrastructure.
- Security organization Structure.
- Inventory and Classification of assets.
- Physical and Environmental Security.
- Identity Management and access control.
- IT Operations management.

- IT Communications.
- Business Continuity Planning.
- Monitoring and Auditing Requirements.

Five interrelated components of internal controls

- Control Environment
  - Elements that establish the control context in which specific accounting systems and control procedures must operate.
  - The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee.
  - The methods used to plan and monitor performance and so on.
- Risk Assessment
  - Elements that identify and analyse the risks faced by an organisation and the way the risk can be managed.
  - Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation.
- Control Activities
  - Elements that operate to ensure transactions are authorized
    - adequate documents and records are maintained
    - assets and records are safeguarded
    - independent checks on performance and valuation of records
  - Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.
- Information and Communication
  - Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.
- Monitoring
  - Elements that ensure internal controls operate reliably over time.

Preventive Controls & Examples

- Preventive controls are those inputs, which are designed to prevent an error and omission.
- An example of a preventive control is the use of passwords to gain access to a financial system.
- Only, the implementation methodology may differ from one environment to the other.

Examples
- Employ qualified personnel.
- Access control.

- Documentation.
- Authorization of transaction.
- Firewalls.
- Anti-virus software.
- Passwords.

Characteristics of preventive controls

- A clear-cut understanding about the vulnerabilities of the asset;
- Understanding probable threats; and
- Provision of necessary controls to prevent probable threats from materializing.

Corrective Controls & Examples

- 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.

Examples

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

Characteristics of the corrective controls

- 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 processing systems to minimize future occurrences of incidents.

Financial Controls

- These controls are generally defined as the procedures exercised by the system user personnel over source.
- These areas exercise control over transactions processing using reports generated by the computer applications.
    - to reflect un-posted items
    - non-monetary changes

  - item counts
- The amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger.

Major financial control techniques

- Authorization
  - This entails obtaining the authority to perform some act typically accessing such assets as accounting or application entries.
- Budgets
  - These are estimates of the amount of time or money expected to be spent during a particular period, project, or event.
  - Budgets must be compared with the actual performance and possible resolution.
- Cancellation of documents
  - This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
- Documentation
  - This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.
- Dual control
  - This entails having two people simultaneously access an asset.
  - Dual access divides the access function between two people: once access is achieved, only one person handles the asset.
- Sequentially numbered documents
  - These are working documents with pre-printed sequential numbers, which enables the detection of missing documents.
- Safekeeping
  - This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

Boundary Controls

- The major controls of the boundary system are the access control mechanisms.
- Access control mechanism links authentic users to resources, they are permitted to access.
- The access control mechanism has three steps of identification, authentication and authorization with respect to the access control policy.

Boundary Control techniques

- Cryptography
  - A cryptographic technique clear text into 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, substitution and product cipher.
- Passwords
  - User identification by an authentication mechanism normally with strong password may be a good 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 unsuccessful entry attempts.
- Personal Identification Numbers
  - PIN is similar to a password.
  - Using a random number stored in its database and sent independently to a user after identification.
  - It can also be a customer selected number.
- Identification Cards
  - Identification cards are used to store information required in an authentication process.
- Biometric Devices
  - Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

Major update to database controls

- 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.
- During processing, ensure that all the transactions till the end of the file marker are processed and similarly when processing master records, all records till end to master file marker are processed.
- Multiple transactions can occur based on a single master record.
- When mapping between the masters records 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. If the suspense account has a non-zero balance, it reflects the errors to be corrected.

Major Report controls

- Application programs use many internal tables to perform various functions.
- Any changes or errors in these tables would have an adverse effect on the organizations basic functions. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.
- 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.
- Similar to the update controls, the suspense account entries are to be periodically monitored with the respective error file and action taken on time.
- The back-up and recovery strategies together encompass the controls required to restore failure in a database.
- Recovery strategies involve roll-forward or the rollback methods.

Classification of information

- Information classification does not follow any predefined rules.
- It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business.
- The classification of information further determines the level of control and security requirements.
- Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality.

Different classifications of information

- Top Secret
  - Highly sensitive internal information that could seriously damage the organization if such information were lost or made public.
  - Information classified as Top Secret information has very restricted distribution and must be protected at all times.
  - Security at this level should be the highest possible.
- Highly Confidential
  - Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations.
  - Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants, patient's medical records.

- Such information should not be copied or removed from the organization's operational control without specific authority.

- Proprietary
  - Information of a proprietary nature that define the way in which the organization operates.
  - Such information is normally for proprietary use to authorized personnel only.
- Public Documents
  - Information in the public domain; annual reports, press statements etc.; which has been approved for public use.

Major data integrity policies

- Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- All software must be tested in a suitable test environment before installation on production systems.
- The division of environments into Development, Test, and Production is required for critical systems.
- Backups must be sent offsite for permanent storage.
- Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes.
- A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

Time Bomb

- A physical time bomb explodes at the time it is set for (unless somebody forces it to explode early), likewise the computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed.
- The computer clock initiates it.

Logic Bomb

- Logic bombs are activated by combination of events.
- This code segment, on execution, may cause destruction of the contents of the memory on deleting a file.
- These bombs can be set to go off at a future event.

Trojan horse

- These are malicious programs that are hidden under any authorized program.
- Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action.
- The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it.
- A Trojan may:
  - Change or steal the password or
  - May modify records in protected files or
  - May allow illicit users to use the systems.

Worms

- A worm does not require a host program like a Trojan to replicate itself.
- Worm program copies itself to another machine on the network.
- Since worms are stand-alone programs, they can be detected easily in comparison to Trojans and computer viruses.

Asynchronous attacks

- They occur in many environments where data can be moved asynchronously across telecommunication lines.
- Numerous transmissions must wait for the clearance of the line before data being transmitted.
- Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack.
- These attacks are hard to detect because they are usually very small pin like insertions.

Various forms of asynchronous attacks

- Data Leakage
  - Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- Wire-tapping
  - This involves spying on information being transmitted over telecommunication network.
- Piggybacking
  - This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.

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

Key ways to control remote and distributed data processing applications

- 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 unauthorized users from accessing the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled.

Three processes of Access Control Mechanism

- Identification
- Authentication
- Authorization

Identification & Authentication

- Users identify themselves to the access control mechanism by providing information.
- To validate the user, his entry is matched with the entry in the authentication file.
- The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

Authorization

- There are two approaches to implementing the authorization module in an access control mechanism.
  - Ticket oriented
    - In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access.
    - Ticket oriented approach operates via a row in the matrix.
    - Each row along with the user resources holds the action privileges specific to that user.

- List oriented
  - In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

Locks on Doors with respect to physical access controls

- Cipher locks
  - Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time.
- Bolting Door Locks
  - A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should be not be duplicated.
- Electronic Door Locks
  - A magnetic or embedded chip-based plastics card key or token may be entered into a reader to gain access in these systems.
  - The reader device reads the special code that is internally stored within the card activates the door locking mechanism.

Major dimensions under which the impact of cyber frauds on enterprises

- Cyber frauds lead to actual cash loss to target company/organization.
- Entities hit by cyber frauds are caught in legal liabilities to their customers.
- These entities need to ensure that such data is well protected.
- News that an organization's database has been hit by fraudsters, leads to loss of competitive advantage. There have been instances where share prices of such companies went down, when the news of such attach percolated to the market.
- Cyber-attack may expose critical information in public domain.
- The above situation may lead to misuse of such information by enemy country.

Major techniques to commit cyber frauds

- It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network.
- 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.
- It refers to the unauthorized copying of company data such as computer files.
- It refers to using the Internet to disrupt electronic commerce and to destroy company and individual communications.

- It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- The unauthorized use of special system programs to bypass regular system controls and perform illegal acts.

CHAPTER – 4 BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Objectives of Business Continuity planning

- Provide for the safety and well-being of people on the premises at the time of disaster
- Continue critical business operations
- Minimise the duration of a serious disruption to operations and resources
- Minimise immediate damage and losses
- Facilitate effective co-ordination of recovery tasks
- Identify critical lines of business and supporting functions

Methodology of developing a Business Continuity

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

Eight phases Methodology of developing a Business Continuity

- Pre-Planning Activities.
- Vulnerability Assessment and General Definition of Requirements.
- Business Impact Analysis.
- Detailed Definition of Requirements.
- Plan Development.
- Testing Program.
- Maintenance Program.
- Initial Plan Testing and Plan Implementation.

The key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement of developing a Business Continuity Plan

- A thorough Security Assessment of the computing and communications environment including
  - personnel practices
  - physical security
  - operating procedures
  - backup and contingency planning
  - systems development and maintenance
  - database security etc.
- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Define the scope of the planning effort.
- Analyse, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.

Major documents that should be the part of a Business Continuity Management system

- The business continuity policy.
- The business impact analysis report.
- The aims and objectives of each function.
- The business continuity strategies.
- The business continuity plans.
- Local Authority Risk Register.

- Exercise schedule and results.
- Training program.

Maintenance tasks undertaken in the development of a BCP

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

Various types of system's back-up for the system

- Full Backup
  - A full backup captures all files on the disk for backup.
  - With a full backup system, every backup generation contains every file in the backup set.
  - However, the amount of time and space such a backup takes large amount of data.
- Incremental Backup
  - An incremental backup captures files that were created or changed since the last backup, regardless of backup type.
  - This is the most economical method, as only the files that changed since the last backup are backed up.
  - This saves a lot of backup time and space.
  - Incremental backup are very difficult to restore.
  - To start with recovering the last full backup, and then recovering files, which were charged subsequently from every subsequent incremental backup.
- Differential Backup
  - A differential backup stores files that have changed since the last full backup.
  - If a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up.
  - Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup.

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

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.
- When the situations that invoke the plan have been identified, four aspects of the emergency plan must be articulated.
  (i) the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'.
  (ii) the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.
  (iii) any evacuation procedures required must be specified.
  (iv) return procedures must be defined.

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.
- 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.
- 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.

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 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.

Issues that should be considered by the security administrators while drafting the contract

If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues.

- How soon the site will be made available subsequent to a disaster.
- The number of organizations that will be allowed to use the site concurrently in the event of a disaster.
- The period during which the site can be used.
- The conditions under which the site can be used.
- The facilities and services the site provider agrees to make available.
- What controls will be in place for working at the off-site facility.

Contents of a Disaster Recovery and Planning Document

- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies the process for maintaining the plan.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels, supplies and transport arrangements.

CHAPTER 6 AUDITING OF INFORMATION SYSTEMS

Performance of evidence collection and understanding the reliability of controls.

- 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.
- Transaction data may be entered into the computer directly without the presence of supporting documentation.
- 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 the auditor to directly access the electronic data retained on the client's computer.
- Certain transactions may be generated automatically by the computer system.
- The use of computers to carry out trading activities is also increasing.
- The public and private sector intend to make use of EDI and electronic trading over the Internet.

Skills that is generally expected of an IS auditor (or) Good understanding of the Information Technology by the Auditor

- Sound knowledge of business operations, transactions, practices and compliance requirements.
- A good understanding of information Risks and Controls.
- Knowledge of IT strategies, policy and procedural controls.
- Ability to understand technical and manual controls relating to business continuity.
- Good knowledge of Professional Standards and Best Practices of IT controls and security.

Types of IS Audits

- Systems and Application:
  - An audit to verify that systems and applications are appropriate, efficient, and adequately controlled to ensure valid, reliable, secure 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 abnormal conditions.
- 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.
- 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.
- Telecommunications, Intranets, and Extranets
  - An audit to verify that controls are in place on the client and on the network connecting the clients and servers.

Major stages of IS Audits

- Auditors determine the main area/s of focus based on the scope-definitions agreed with management.
- During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan.
- Gathering evidence by interviewing staff and managers, reviewing documents, and observing processes etc.
- SWOT or PEST techniques can be used for analysis.

- Reporting to the management is done after analysis of evidence gathered and analysed.
- Preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

Good understanding of the technology environment and related control issues

- Analysis of business processes and level of automation.
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses.
- 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 and the government.
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems.
- Finally, Studying Information Technology policies, standards, guidelines and procedures.

Key steps for a risk-based approach to make an audit plan

- 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 likelihood and severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Snapshots

- Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records.
- The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application.
- These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

Audit Hooks

- There are audit routines that flag suspicious transactions.
- 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 may display a message on the auditor's terminal.

System Control Audit Review File (SCARF) Technique

- 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 on a special audit file- the SCARF master files.
- Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up.

Various types of information collected by using SCARF technique

- SCARF audit routines provide an independent check on the quality of system processing.
- Organizations have to adhere to the policies, procedures and standards of the organization.
- SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- SCARF can be used to monitor different types of application system exceptions.
- SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- Snapshots and extended records can be written into the SCARF file and printed when required.
- Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

Advantages of continuous audit techniques

- Evidence would be available more timely and in a comprehensive manner.
- The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.

- 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.
- 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.
- 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 of Continuous Audit techniques

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

Audit trails can be used to support security objectives

- 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.
  - Depending upon how much activity is being logged and reviewed; real time detection can impose a significant overhead on the operating system, which can degrade operational performance.
  - After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

- Reconstructing Events
  - Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors.
  - Audit trail analysis also plays an important role in accounting control.
- Personal Accountability
  - Audit trails can be used to monitor user activity at the lowest level of detail.
  - Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

Two main categories of Data Management Controls

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

(ii) Back-up Controls
- Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster and the organization can retrieve its files and databases.
- Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss.

Major risks relating to personal computers

- Personal Computers (PC) are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
- Pen drives can be transported from one place to another, as a result of which data theft may occur.
- Segregation of duty is not possible, owing to limited number of staff.
- Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
- The operating staff may not be adequately trained.

Security measures that could be exercised to overcome risks relating to personal computers

- Physically locking the system.
- Proper logging of computer.
- Centralized purchase of hardware and software.
- Uses of antimalware software.
- The use of personal computer and their peripherals must be controlled.

Major processing controls

- Run-to-run totals 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.
- Two or more fields can be compared and cross verified to ensure their correctness.
- Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.
- Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing.
- Exception reports are generated to identify errors in the data processed.

Major audit issues of operational layer with reference to application security audit

- User Accounts and Access Rights
  - This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities.
  - Auditor needs to always ensure the use of unique user IDs, and these need to be traceable to individuals for whom they are created.
  - In case, guest IDs are used, then these should be tested.
- Password Controls
  - In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum
  - Auditor needs to check whether there are applications where password controls are weak.
  - In case such instances are found, then auditor may look for compensating controls against such issues.
- Segregation of Duties
  - As frauds due to lack of segregations increase across the world, importance of the Segregation of Duties also increases.
  - Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to the 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.

CHAPTER 8 –EMERGING TECHNOLOGIES

Cloud Computing

- Cloud computing simply means the use of computing resources as a service through networks, typically the Internet.
- With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources.
- Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service.
- With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software.
- The best example of cloud computing is *Google Apps* where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

Goals of Cloud Computing

- To access services and data from anywhere at any time.
- To consolidate IT infrastructure into a more integrated and manageable environment.
- To reduce costs related to IT energy/power consumption.
- To enable or improve "Anywhere Access" (AA) for ever increasing users.
- To enable rapid provision of resources as needed.

Front end architecture with reference to Cloud Computing

- 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 with reference to Cloud Computing

- Back end refers to some service facilitating peripherals.
- In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers.
- Groups of these clouds make up a whole cloud computing system.
- Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment.
- Usually, every application would have its individual dedicated server for services.

Public cloud

- This environment can be used by the general public.
- This includes individuals, corporations and other types of organizations.
- Typically, public clouds are administrated by third parties and the services are offered on pay-per-use basis.
- Business models like SaaS and public clouds complement each other and enable companies to leverage shared IT resources and services.

Advantages of public cloud

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.

  Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.

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.
- They are built primarily by IT departments within enterprises, utilization of infrastructure resources within the enterprise with applications using the concepts of grid and virtualization.

Advantages of private clouds

- Allow usage of low-cost servers and hardware while providing higher efficiencies.
- High levels of automation is largely responsible for reducing operations costs and administrative overheads.

However, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently.

Infrastructure as a Service (IaaS)

- It provides the infrastructure required to host the services by ourselves.
- In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure.
- Examples of IaaS providers include: Amazon EC2, Azure Services Platform, Dyn DNS, Google Compute Engine, HP Cloud etc.

Platform as a Service (PaaS)

- Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server.
- Application developers can develop and run their software solutions on a cloud platform without the cost.
- In PaaS, one can make applications and software on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want.
- Examples of PAAS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard etc.

Software as a Service (SaaS)

- SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure.

Network as a Service (NaaS)

- It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services.
- NaaS involves optimization of resource allocation by considering network and computing resources as a whole.
- Some of the examples are: Virtual Private Network, Mobile Network Virtualization etc.

Communication as a Service (CaaS)

- CaaS is an outsourced enterprise communication solution that can be leased from a single vendor.
- 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 large capital investments.
- Examples are: Voice over IP, Instant Messaging, Collaboration and Videoconferencing application using fixed and mobile devices.

Characteristics of Cloud Computing.

- Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
- The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency.
- Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
- This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- 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.

Advantages of Cloud Computing

- Cost Efficiency
  - Cloud computing is probably the most cost efficient method to use, maintain and upgrade.
  - Traditional desktop software costs companies a lot in terms of finance.
  - Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- Unlimited Storage
  - Storing information in the cloud gives us almost unlimited storage capacity.
  - Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.

- Backup and Recovery
  - Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device.
  - Most cloud service providers are usually competent enough to handle recovery of information.
  - This makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
- Automatic Software Integration
  - 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.
- 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
  - Cloud computing gives us the advantage of quick deployment.
  - Once opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes.
  - The amount of time taken here will depend on the exact kind of technology that we need for our business.

Challenges (disadvantages) to Cloud Computing

- Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities.
- Integrity refers to the prevention of unauthorized modification of data.
- Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP).
- Availability can be affected temporarily or permanently, and a loss can be partial or complete.
- Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability.

Tangible benefits of mobile computing

- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables us to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Hybrid Cloud

- This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications.
- It is typically offered in either of two ways.
- A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

Mobile Computing

- It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link.
- Mobile voice communication is widely established throughout the world.
- An extension of this technology is the ability to send and receive data across these cellular networks.
- It allows users to transmit data from remote locations to other remote or fixed locations.
- This proves to be the solution of the biggest problem of business people on the move.

BYOD

- BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices.
- It means employees are welcome to use personal devices to connect to the corporate network to access information and application.
- The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours.

- Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

Web 2.0

- Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability of people to collaborate and share information online.
- Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users.
- Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information.
- Web 2.0 has been used more as a marketing term than a Computer Science based term.
- The power of Web 2.0 is the creation of new relationships between collaborators and information.

Green IT

- Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient, environmentally friendly and responsible way.
- Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.
- The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime.
- To promote the recyclability or biodegradability of defunct products and factory waste.
- Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

Steps can be followed for Green IT

- Power-down the CPU and all peripherals during extended periods of inactivity.
- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- Use notebook computers rather than desktop computers whenever possible.

- Minimize the use of paper and properly recycle waste paper.
- Dispose of e-waste according to central, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centres.
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity.