ISCA: A Capsule for Quick Revision

It has always been the endeavour of Board of Studies to provide quality academic inputs to the students of Chartered Accountancy Course. Keeping in mind this objective, BoS has decided to come out with a crisp and concise capsule of each subject to facilitate students in quick revision before examination. The second in such series of capsule is on Paper 6: Information Systems Control and Audit of Final Course.
Students may note that this capsule is a tool for quick revision of some significant aspects of ISCA and thus, should not be taken as a substitute for the detailed study of the subject. Students are advised to refer to the relevant Study Material, Practice Manual and Revision Test Paper for May, 2017 examination for comprehensive study and revision.

CHAPTER 1: CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

This chapter facilitates the basic understanding of how to distinguish among key aspects of Enterprise Governance, Corporate Governance, IT Governance, to examine the role of IT in formulating IT strategy, aligning IT as per business strategy and identify key processes and practices required for ensuring value creation from IT; to review IS Risk management strategy based on different types of risks and their impact; and how to use best practices frameworks such as COBIT and GEIT to meet enterprises' need.

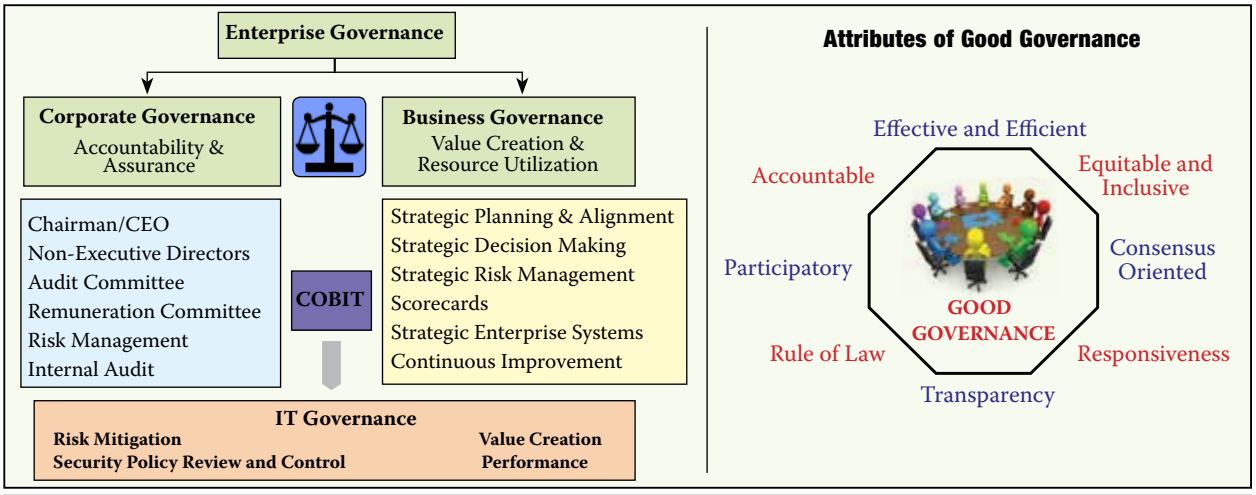
KEY CONCEPTS OF GOVERNANCE

Enterprise Governance is defined as the set of responsibilities and practices exercised by the Board and executive management of an enterprise. The goal is to provide strategic direction to ensure that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

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

Business Governance/ Performance Governance gives an emphasis on business process performance using the analysis, monitoring, reporting and optimization of business processes and business activities, and including process simulation and optimization of desired business outcomes by using real-time, historical and estimated data values.

IT Governance is described as a framework for the organizational structures and associated processes and standards to ensure that IT supports the achievement of strategic objectives of the company.



GOVERNANCE OF ENTERPRISE IT (GEIT)

Governance of Enterprise IT (GEIT)
(Sub-set of Corporate Governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas)

Objectives

- 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.

Benefits

- To provide a consistent approach integrated and aligned with the Enterprise Governance approach.
- To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives.
- To ensure that IT-related processes are overseen effectively and transparently.
- To confirm compliance with legal and regulatory requirements.
- To ensure that the governance requirements for board members are met.

Key Governance Practices

- Evaluate the Governance System
- Direct the Governance System
- Monitor the Governance System

IT Strategy Planning
(Provides direction to deployment of Information System)

Process

- Dynamic in nature.
- To ensure that a process is in place to modify and accommodate changes to enterprise's long range plan and change in IT conditions.

Objectives

- To provide a holistic view of the current IT environment,
- the future direction, and
- the initiatives required to migrate to the desired future environment.

Classification

- Enterprise Strategic Plan;
- Information Systems Strategic Plan;
- Information Systems Requirements Plan;
- Information Systems Applications and Facilities Plan.

Enterprise Strategic Plan	Provides the overall charter under which all units in the enterprise, including the information systems function must operate.
Information Systems Strategic Plan	To focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment.
Information Systems Requirements Plan	The Information System Requirements Plan defines information system architecture for the information systems department. The architecture specifies the major organization functions needed to support planning, control and operations activities and the date classes associated with each function.
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.

COMMITTEE OF SPONSORING ORGANIZATION (COSO)

Internal Control – Integrated Framework

Control Environment	Categorizing the criticality and materiality of each business process and its owner.
Risk Assessment	An assessment of risks associated with each business process.
Control Activities	To manage, mitigate and reduce the risks associated with business process.
Information & Communication	Associated with control activities are information and communication systems.
Monitoring	With modifications made as warranted by changing conditions.

RISK AND RELATED TERMS

Asset

- Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees.

Vulnerability

- Vulnerability is the weakness in the system safeguards that exposes the system to threats.

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.

Risk

- Risk is where threat and vulnerability overlap. That is, we get a risk when our systems have a vulnerability that a given threat can attack.

Counter Measure

- An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure.

Attack

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

Exploit

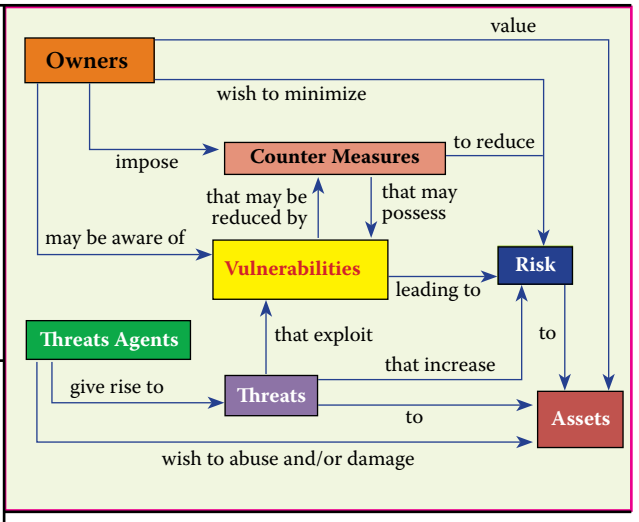
- An exploit is the way or tool by which an attacker uses a vulnerability to cause damage to the target system.

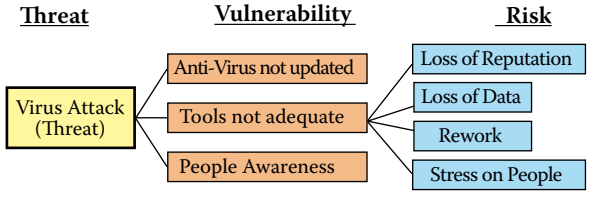
Exposure

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

Likelihood of the Threat

- It is the estimation of the probability that threat will succeed in achieving an undesirable event.





Risk Management Strategies

When risks are identified and analyzed, Risk Management Strategies are used.

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

Key Management Practices of Risk Management

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

Key Metrics

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

COBIT 5
(CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY)

COBIT is a set of best practices for Information Technology management developed by Information Systems Audit & Control Association (ISACA) and IT Governance Institute in 1996. COBIT 5 is the only business framework for the governance and management of enterprise Information Technology.

This evolutionary version COBIT 5 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.

Components in COBIT

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

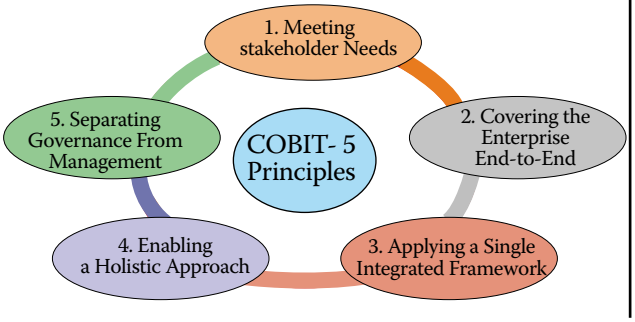
Process Descriptions
- Process Reference Model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.

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

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

Maturity Models
- Assess maturity and capability per process and help to address gaps.

COBIT 5 Principles



Principle 1: Meeting Stakeholder Needs: 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.

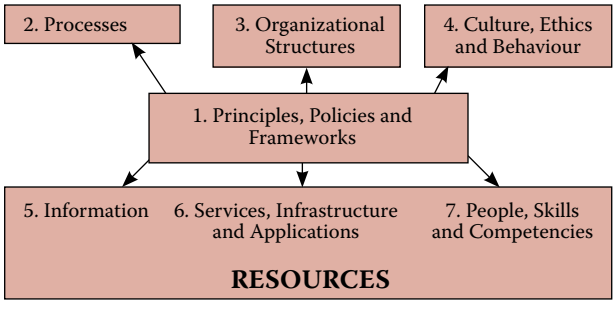
Principle 2: Covering the Enterprise End-to-End: COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

Principle 3: Applying a Single Integrated Framework: 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.

Principle 4: Enabling a Holistic Approach: COBIT 5 defines a set of enablers to support implementation of a comprehensive governance and management system for enterprise IT.

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.

COBIT 5 Seven Enablers Enabling a Holistic Approach



1. Principles, Policies and Frameworks	Vehicles to translate the desired behaviour into practical guidance for day-to-day management.
2. Processes	Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
3. Organisational Structures	Are the key decision-making entities in an organisation.
4. Culture, Ethics and behaviour	Of individuals and of the organisation; very often underestimated as a success factor in governance and management activities.
5. Information	Is pervasive throughout any organisation, i.e., deals with all information produced and used by the enterprise for keeping the organisation running and well governed.
6. Services, Infrastructure and applications	Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. 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.

CHAPTER – 2 INFORMATION SYSTEMS CONCEPTS

This chapter explains the basic concepts of Information Systems, their types and their applications in businesses and organizations. The chapter also comprehends the knowledge about different types of systems e.g. Open, Closed, Probabilistic, Deterministic, Manual, Physical etc. and to differentiate between data and information.

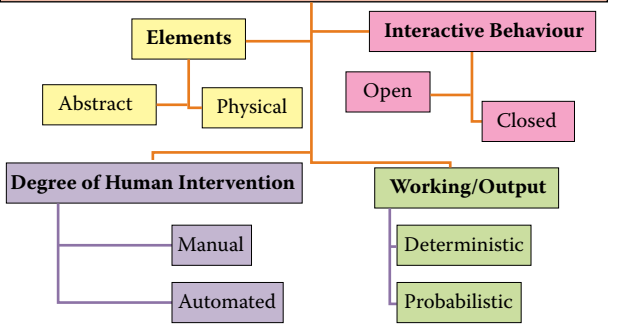
- **Information means Processed Data**

Attributes of Information

- **Availability**
  - Information is useless if it is not available at the time of need.
- **Purpose/Objective**
  - The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.
- **Mode and format**
  - The mode may be in the form of voice, text and combination of these two. Format should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching.
- **Current/Updated**
  - Information should be refreshed from time to time as it usually rots with time and usage.
- **Rate**
  - Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive.
- **Frequency**
  - The frequency with which information is transmitted or received affects its value.
- **Completeness and Adequacy**
  - The information provided should be complete and adequate in itself because only complete information can be used in policy making.
- **Reliability**
  - It is a measure of failure or success of using information for decision-making.
- **Validity**
  - It measures how close the information is to purpose for which it asserts to serve.
- **Quality**
  - It means the correctness of information.
- **Transparency**
  - It is essential in decision and policy making.
- **Value of Information**
  - Defined as value of information when given a set of possible decisions, a decision-maker may select one on basis of the information at hand.

SYSTEM

Defined as a group of interconnected components working towards the accomplishment of a common goal by accepting inputs and producing outputs in an ordered transformation process.



Systems Classification

Element Based Systems

- **Abstract System** - Also known as **Conceptual System or Model** that can be defined as an orderly arrangement of interdependent ideas or constructs.
- **Physical System** is a set of tangible elements, which operated together to accomplish an objective e.g. Computer system.

Interactive Behaviour Based Systems

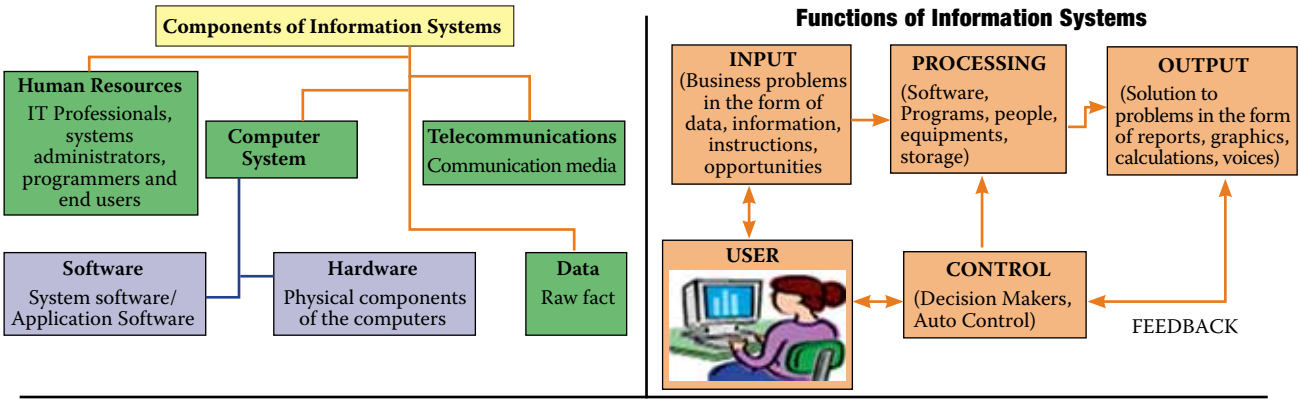
- An **Open System** interacts with other systems in its environment. For example; Information Systems.
- **Closed System** does not interact with the environment and does not change with the changes in environment.

Degree of Human Intervention based

- 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.

Working/ Output Based

- 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** is defined in terms of probable behaviour. For example - inventory system is a probabilistic system where the average demand, average time for replenishment, etc. may be defined.



TYPES OF INFORMATION SYSTEMS

Operational Level Systems that support operational managers in tracking elementary activities.

Knowledge Level Systems that support the business to integrate new knowledge into the business and control the flow of paperwork and enable group working.

Management Level Systems support the middle managers in monitoring, decision-making and administrative activities. This is helpful in answering questions like are things working well and in order? This ensures that business procedures are followed.

Strategic-level Systems (SLS) are for strategic managers to track and deal with strategic issues, assisting long-range planning. Support the senior level management to tackle and address strategic issues and long term trends, both inside organization and outside world.

Transaction Processing System (TPS) is a lowest level of operational level system that manipulates data from business transactions to generate various information products for external use. TPS ensures that business procedures are followed.

Examples are sales order entry, hotel reservations, payroll, employee record keeping, and shipping.

Components – Input, Processing, Storage, Output.

Features – Large volume of data, automation of basic operations, measurable benefits, source of input for other systems.

Office Automation Systems (OAS) refer to the integration of office functions usually related to managing information.

Basic activities include –

Document Capture;

Document Creation;

Receipts and Distribution;

Filling, Search, Retrieval and Follow up;

Calculations; and

Recording Utilization of Resources.

Management Information System (MIS)

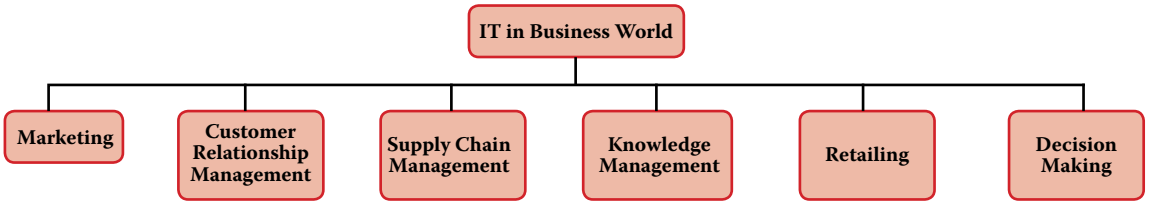
Features –

Management Oriented; Management Directed; Sub-System Concept; Heavy Planning Element; Common Data Flows; Common Database; Integrated and Computerized.

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

Executive Information Systems (EIS) sometimes referred to as an Executive Support System (ESS) serves the strategic level i.e. top level managers of the organization.

TYPES OF SYSTEMS		GROUPS SERVED
Executive Support Systems (ESS)	**STRATEGIC LEVEL SYSTEMS** 5 year Operating Plan, 5 - year Budget Forecasting, 5 - Year Sales Trend Forecasting, Profit Planning, Manpower Planning	**Senior Managers**
Management Information Systems (MIS)	**MANAGEMENT LEVEL SYSTEMS** Sales Management, Inventory Control, Annual Budgeting, Capital Investment Analysis, Relocation Analysis	**Middle Managers**
Decision Support Systems (DSS)	Sales Region Analysis, Production Scheduling, Cost Analysis, Pricing/Profitability Analysis, Contract Cost Analysis	
Knowledge Management Systems(KMS)	**KNOWLEDGE LEVEL SYSTEMS** Engineering Workstations, Graphics Workstation, Managerial Workstations	**Knowledge and Data Workers**
Office Automation Systems (OAS)	Word Processing, Document Imaging, Electronic Calendars	
Transaction Processing Systems (TPS)	**OPERATIONAL LEVEL SYSTEMS** Machine Control, Securities Trading, Payroll, Compensation, Order tracking, Plant Scheduling, Accounts Payable, Training & Development, Order Processing, Material Movement Control, Cash Management, Accounts Receivable, Employee Record Keeping	**Operational Managers**
	Sales & Marketing Manufacturing Finance Accounting Human Resources	



SPECIALIZED SYSTEMS

These are the systems that provide comprehensive end-to-end IT solutions and services (including systems integration, implementation, engineering services, software application customization and maintenance) to various corporations globally.

1. Expert Systems: Expert Systems are highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. These 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. Some of the business application areas of Expert system are Accounting and Finance, Marketing, Manufacturing, Personnel and General business etc.

Benefits	♦ 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 professionals 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.

2. 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 facets of an operation, including product planning, development, manufacturing, sales and marketing.

Components	❖ **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. ❖ **Process Flow:** It is the model that illustrates the way how information flows among the different modules within an ERP system. ❖ **Customer mindset:** To lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system. ❖ **Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.
Benefits	♦ 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.

3. Core Banking Systems: Core Banking Systems (CBS) may be defined as back-end systems that process daily banking transactions, and post 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).

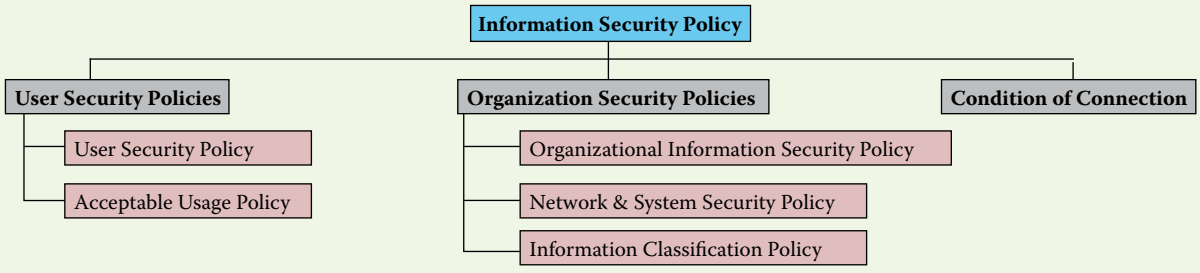
Elements of Core Banking	♦ Making and servicing loans. ♦ Opening new accounts. ♦ Processing cash deposits and withdrawals. ♦ Processing payments and cheques. ♦ Calculating interest. ♦ Customer Relationship Management (CRM) activities. ♦ Managing customer accounts. ♦ Establishing criteria for minimum balances, interest rates, number of withdrawals allowed and so on. ♦ Establishing interest rates. ♦ Maintaining records for all the bank's transactions.

CHAPTER 3 PROTECTION OF INFORMATION SYSTEMS

This chapter provides the understanding on the Information Security Policies and various types of Information Systems Controls.

INFORMATION SECURITY POLICY AND ITS HIERARCHY

Information Security Policy: This policy provides a definition of Information Security, its overall objective and the importance that applies to all users. Various types of Information Security Policies are as follows:



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

CLASSIFICATION OF INFORMATION SYSTEMS' CONTROLS

Objectives of Controls (Based on the time they act)	Nature of IS Resource (Based on Resource its implemented)	Audit Functions (On Auditor's perspective)
Preventive Controls: Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Use of passwords to gain access to a financial system is a preventive control. **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. **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. A Business Continuity Plan (BCP) is a corrective control.	**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. **Physical Access Controls:** These are the 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. **Logical Access Controls:** These are the 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. These controls are implemented to ensure that access to systems, data and programs is restricted to authorized users to safeguard information against unauthorized use, disclosure or modification, damage or loss.	**Managerial Controls:** These are the controls that must be performed to ensure development, implementation, operation & maintenance of IS 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. **Application Controls:** Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions.

MANAGERIAL CONTROLS – SCOPE

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

APPLICATION CONTROLS - SCOPE

Application Controls	Scope
Boundary	Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user.
Input	Input Controls are validation and error detection of data input into system and are responsible for bringing both data and instructions in to information system.
Communication	Responsible for controls over physical components, communication line errors, flows, links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls etc.
Processing	Responsible for computing, sorting, classifying and summarizing data.
Output	To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
Database	Responsible to provide functions to define, create, modify, delete and read data in an information system.

Information Technology General Controls (ITGC)	Financial Controls	Personal Computer Controls
ITGC are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.	These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of applications to general ledger.	**Most common PC Controls:** ❖ Physically locking the system; ❖ Proper logging of equipment shifting must be done; ❖ Centralized purchase of hardware/ software; ❖ Standards set for developing, testing and documenting; ❖ Uses of anti-malware software; ❖ Use of PC and their peripheral must have controls; and ❖ Use of disc locks that prevent unauthorized access to the floppy disk or pen drive of a computer.

MAJOR CYBER ATTACKS

- ❖ **Phishing:** It is the act of attempting to acquire information such as usernames, passwords, and credit card details 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 and hosting malware on websites in an unauthorized manner.
- ❖ **Others:** These are given as follows:
  - **Cracking:** Crackers are hackers with malicious intentions.
  - **Eavesdropping:** It refers to the listening of the private voice or data transmissions, often using a wiretap.
  - **E-mail Forgery:** Sending e-mail messages that look as if someone else sent it is termed as E-mail forgery.
  - **E-mail Threats:** Sending a threatening message to try and get recipient to do something that would make it possible to defraud him is termed as E-mail threats.
  - **Scavenging:** This is gaining access to confidential information by searching corporate records.

IMPACT OF CYBER FRAUDS

- ❖ **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. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- ❖ **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. There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.
- ❖ **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.

SOME 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.

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.

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 using the Internet to disrupt electronic commerce and to destroy company and individual communications.

Logic Time Bombs: These are the programs that lie idle until some specified circumstance 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.

CHAPTER 4 BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

This Chapter introduces the concepts of Business Continuity Management, Business Continuity Planning, Back-ups and Disaster Recovery Planning (DRP).

BUSINESS CONTINUITY PLANNING (BCP)

It is creation and validation of a logistical plan for how an enterprise will recover & restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

OBJECTIVES & GOALS

OBJECTIVES

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

GOALS

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

DEVELOPMENT

Each of these phases are described below:

Phase 1 – Pre-Planning Activities (Project Initiation): This Phase is used to obtain an understanding of the existing and projected computing environment of the organization.

Phase 2 – Vulnerability Assessment and General Definition of Requirements: This phase addresses measures to reduce probability of occurrence of disaster.

Phase 3 – Business Impact Assessment (BIA): A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to identify critical systems, processes and functions; assess economic impact of incidents/ disasters; & assess "pain threshold".

Phase 4 – Detailed Definition of Requirements: During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analyzing alternative recovery strategies. 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.

Phase 6 – Testing/Exercising Program: Testing/ exercising goals are established and alternative testing strategies are evaluated.

Phase 7 – Maintenance Program: It is critical that existing change management processes are revised to take recovery plan maintenance 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 test results.

BUSINESS CONTINUITY MANAGEMENT

(A) Business Continuity Management (BCM) is a very effective management process to help enterprises to manage the disruption of all kinds, providing countermeasures to safeguard from the incident of disruption of all kinds.

(B) Advantages of BCM are that- The enterprise:

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

(C) BCM Policy is a high-level document, which shall be the guide to make a systematic approach for disaster recovery, to bring about awareness among the persons in scope about the business continuity aspects and its importance and to test and review the BCP for the enterprise in scope.

(D) BCM Process: A BCM process should be in place to address the policy and objectives as defined in the Business Continuity Policy by providing organization structure with responsibilities and authority, implementation and maintenance of BCM.

- **BCM – Process:** The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise. The sub-processes are Organization Structure; Implementing Business Continuity and Documentation and Records.
- **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process. This process involves Business Impact Analysis and Risk Assessment.
- **BCM – Strategy Process:** This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. This involves range of strategies - Organization BCM Strategy; Process Level BCM Strategy and Resource Recovery BCM Strategy.
- **BCM – Development and Implementation Process:** This involves the Development of a management framework and a structure of Incident Management, Business Continuity and Business Recovery and Restoration Plans.
- **BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; BCM audit and Review arrangements to identify opportunities for improvement.
- **BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity, business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service. Accessing needs, designing and delivery trainings and measuring results are the activities under this process.

TYPES OF PLANS

Emergency Plan	Back-Up Plan	Recovery Plan	Test 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. ❖ 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.	❖ The Backup Plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system. ❖ The backup plan needs continuous updating as changes occur. ❖ Lists of hardware and software must be updated to reflect acquisitions and disposals.	❖ Recovery Plan sets out procedures to restore full information system capabilities. ❖ Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. ❖ The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first.	❖ 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.

TYPES OF BACK - UPS

Type	Definition	Advantages	Disadvantages	Example
Full Backup	A complete backup of everything you want to backup.	❖ Restores are fast and easy to manage as the entire list of files and folders are in one backup set. ❖ Easy to maintain and restore different versions.	❖ Backups can take very long as each file is backed up again every time the full backup is run. ❖ Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.	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.

Type	Definition	Advantages	Disadvantages	Example
Differential Backup	The backup software looks at which files have changed since you last did a full backup. Then creates copies of all the files that are different from the ones in the full backup.	❖ Much faster backups then full backups. ❖ More efficient use of storage space then full backups since only files changed since the last full backup will be copied on each differential backup run. ❖ Faster restores than incremental backups.	❖ Backups are slower than incremental backups. ❖ Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup. ❖ Restores are slower than with full backups. ❖ Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.	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 backup, it still contains the files backed up on Tuesday.

Type	Definition	Advantages	Disadvantages	Example
Incremental Backup	The backup software creates copies of all the files, or parts of files that have changed since previous backups of any type (full, differential or incremental).	❖ Much faster backups. ❖ Efficient use of storage space as files is not duplicated. Much less storage space used compared to running full backups and even differential backups.	❖ Restores are slower than with a full back-up and differential backups. ❖ Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.	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.

Type	Definition	Advantages	Disadvantages	Example
Mirror Backup	Mirror backups are 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.	❖ 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.	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.

DISASTER RECOVERY PLANNING

Disaster Recovery Planning (DRP) is the factor that makes the critical difference between the organizations that can successfully manage crises with minimal cost and effort and maximum speed, and those that are left picking up the pieces for untold lengths of time and at whatever cost providers decide to charge; organizations forced to make decision out of desperation. The primary goal of any Disaster Recovery Plan is to help the organization maintain its business continuity, minimize damage, and prevent loss.

DRP will specify how the recovery of a function will be performed. Within a DR plan, there will be individual component system recovery plans that would specify steps to recover. The big difference between BCP and DR plan is that a DRP will specify ***how*** the recovery of a function will be performed. Within a DR plan, there will be individual component system recovery plans that would specify steps to recover.

CHAPTER 5 ACQUISITION, DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SYSTEMS

This chapter conceptualizes a systematic approach to Systems Development Life Cycle (SDLC) and reviews its phase activities, methods, tools and controls etc. and provides an analytical understanding of different SDLC models.

SYSTEMS DEVELOPMENT METHODOLOGY

- A formalized, standardized, well-organized and documented set of activities.
- Refers to the process of examining a business situation with the intent of improving it through better procedures and methods.
- A framework to structure, plan and control the process of developing.
- Example - Waterfall Model, Prototyping Model, Incremental Model, Spiral Model, RAD Model and Agile Model.

Characteristics	Description
Process	Project divided into number of identifiable processes, with each process having a starting point and an ending point; comprises several activities; one or more deliverables, and several management control points.
Deliverables	The specific reports and other documentation must be produced periodically during system development.
Sign-offs	Generally provided by users, managers, and auditors that signify approval of the development process and the system being developed.
Testing	Project divided into number of identifiable processes, with each process having a starting point and an ending point; comprises several activities; one or more deliverables, and several management control points.
Training	A training plan for its future users.
Controls	Formal program change controls established to prevent unauthorized changes to computer programs.
Post-implementation Review	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.

SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

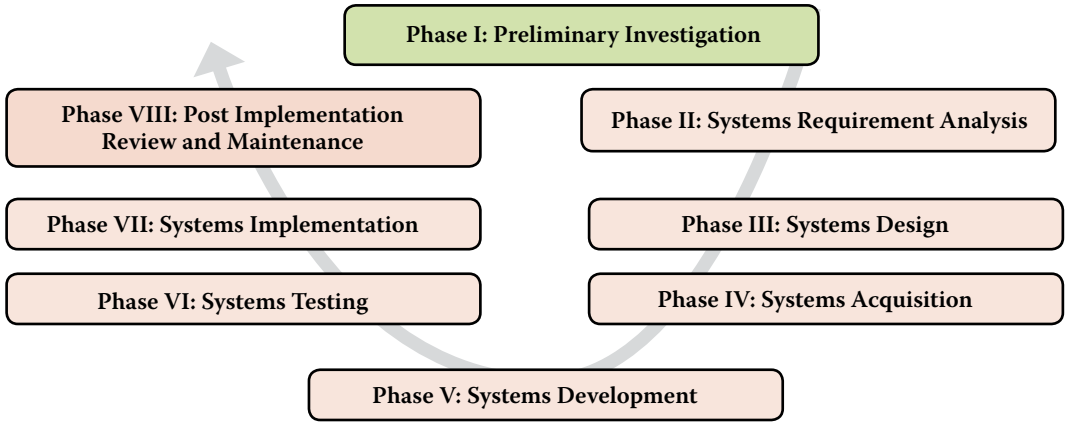
Systems Development Life Cycle (SDLC) consists of a generic sequence of steps or phases in which each phase of the SDLC uses the results of the previous one and provides system designers and developers to follow a sequence of activities. The following phases are involved in the cycle:

Phase I: Preliminary Investigation: A preliminary investigation is normally initiated by some sort of system request. The deliverable of the preliminary investigation includes a report including feasibility study observations.

1. **Identification of Problem**
   Define the problem clearly and precisely.
2. **Identification of Objectives**
   Work out and precisely specify the objectives of the proposed solution.
3. **Delineation of Scope**
   Defines its typical boundaries that clearly and comprehensibly states the extent and defines 'What will be addressed by the solution and what will not be'.
4. **Feasibility Study**
   The likelihood that the proposed system will be useful for the organization is determined on following factors:
   - ❖ **Technical Feasibility:** It answers whether implementation of the project is viable using current technology.
   - ❖ **Financial Feasibility:** This checks for whether the proposed solution may be costly for the user organization.
   - ❖ **Economic Feasibility:** This includes an evaluation of incremental cost and benefit expected if the proposed system is implemented.
   - ❖ **Schedule or Time Feasibility:** – This marks an estimation of time it will take a new system to become operational.
   - ❖ **Resources Feasibility:** Implementing sophisticated software solutions becomes difficult at specific locations because of the reluctance of skilled personnel to move to such locations.
   - ❖ **Operational Feasibility:** This is concerned with finding view of workers, employees, customers and suppliers about the use of new system.
   - ❖ **Behavioural Feasibility:** This refers to the systems, which is to be designed to process data and produce the desired outputs.
5. **Reporting Results to Management**
   Provides one or more solution alternatives and estimates the cost and benefits of each alternative and reports these results to the management.
6. **Internal Control Aspects**
   Management implements proper internal audit team to ensure proper business objectives.

Phase II: System Requirement Analysis: 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.

1. Fact Finding	2. Analysis of the Present Systems	3. System Analysis of Proposed Systems	4. System Development Tools	5. System Specification	6. Roles involved in SDLC	7. Internal Controls
Every system is built to meet some set of needs. To assess these needs - Documents, Questionnaires, Interviews, Observation are some fact-finding tools.	This step involves survey of existing methods, procedures, data flow, outputs, files, input and internal controls should be intensive to fully understand the present system and its related problems.	After thorough analysis, the proposed system specifications' outputs are clearly determined; that results in inferring what inputs, database, methods, procedures and data communications must be employed.	These are used to conceptualize, clarify, document and communicate the activities and resources involved in the organization and its IS . Example – Structured English, Flowcharts, Data Flow Diagrams, Decision Tree, etc.	The systems analyst prepares a document called Systems Requirement Specifications (SRS). SRS contain Introduction, Information Description, Functional Description, Behavioural Description, Validation Criteria, Appendices and SRS Review.	A variety of tasks during the SDLC are performed by Steering Committee / Project Manager/ Project Leader / System Analyst / Team Leader / Developers/ Testers / Auditors etc. based on requisite expertise as well as skills set.	This includes whether present system analysis has been properly done; whether appropriate domain expert was engaged; whether all user requirements of proposed system have been considered; etc.



Phase III: Systems Design: The objective is to design an Information System that best satisfies the users/managerial requirements. It describes the parts of the system and their interaction; sets out how the system shall be implemented using the chosen hardware, software and network facilities; specifies the program and the database specifications and the security plans and further specifies the change control mechanism to prevent uncontrolled entry of new requirements.

Architectural Design	This deals with the organization of applications in terms of hierarchy of modules and sub-modules wherein 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 are identified.
Design of data flow and user interface for proposed system	This includes designing the data / information flow for the proposed system, the inputs that are required are existing data / information flows, problems with the present system, and objective of the new system.
Design of Database	This involves determining its scope ranging from local to global structure and include Conceptual Modeling, Data Modeling, Storage Structure Design and Physical Layout Design.
User Interface design	It involves determining the ways in which users will interact with a system like - 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.
Physical Design	Concentrates on the issues like the type of hardware for client and server application, Operating systems to be used, type of networking, periodical batch processing, online or real-time processing; frequency of I/O etc.
System's Operating Platform	The new hardware/system software platform required to support the application system will then have to be designed for requisite provisions.
Internal Design Controls	The key control aspects at this stage include - Whether management reports were referred by System Designer? Whether all control aspects have been properly covered?, etc.

Phase IV: Systems Acquisition: After a system is designed either partially or fully, the next phase of the systems development starts, which relates to the acquisition of operating infrastructure including hardware, software and services. Such acquisitions are highly technical and cannot be taken easily and for granted. Thereby, technical specifications, standards etc. come to rescue.

Acquisition Standards	Acquiring System Components from vendors	Other Acquisition aspects and practices
This focuses on ensuring security, reliability, and functionality already built into a product.	The organization gets a reasonable idea of the types of hardware, software and services, it needs for the system being developed. Request For Proposal (RFP) from vendors called.	Includes several other acquisition aspects and practices also like – H/w Acquisition; S/w Acquisition; Contracts, S/w Licenses and Copyright Violations, Validation of Vendors' proposals and methods of validating them.

Phase V: Systems Development: This phase is supposed to convert the design specifications into a functional system under the planned operating system environments. Application programs are written, tested and documented, conduct system testing that results into a fully functional and documented system.

Program Coding Standards	Programming Language	Program Debugging	Program Testing	Program Documentation	Program Maintenance
Coding Standards provide simplicity, interoperability, compatibility, efficient utilization of resources and least processing time.	High level P/L such as COBOL, C, C++, Java etc.. Scripting language such as JavaScript, VBScript, and Decision Support or Logic Programming languages such as LISP, PROLOG are used.	Debugging is the most primitive form of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly.	Programmer should plan the testing to be performed, including testing of all the possible exceptions.	The requirements of business data processing applications are subject to periodic change that calls for modification of various programs.	The requirements of business data processing applications are subject to periodic change. This calls for modification of various programs.

Phase VI: Systems Testing: Testing is a process used to identify the correctness, completeness and quality of developed computer software. Different levels of Testing are as follows:

Unit Testing

A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class.

The categories of tests that a programmer typically performs on a program unit are as follows:

Functional Tests: Functional Tests check 'whether programs do, what they are supposed to do or not'.

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.

Stress Tests: Stress testing is a form of testing that involves testing beyond normal operational capacity, often to a breaking point, to observe the results.

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.

Integration Testing

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

Bottom-up Integration: It is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system.

Top-down Integration: It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module. 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.

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. In the context of the integration testing, 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.

System Testing

It is a process in which software and other system elements are tested as a complete system. 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:

Recovery Testing: This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'.

Security Testing: The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, availability authentication, authorization, and non-repudiation.

Stress or Volume Testing: It involves testing beyond normal operational capacity, often to a breaking point, to observe the results.

Performance Testing: This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

Final Acceptance Testing

During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users. It is classified as under:

Quality Assurance Testing: It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance policy, methodology and prescriptions.

User Acceptance Testing: It ensures that the functional aspects expected by the users have been well addressed in the new system.

Phase VII: Systems Implementation: Generic key activities involved in Systems Implementation include Conversion of data to the new system files; Training of end users; Completion of user documentation; System changeover; and Evaluation of the system at regular intervals. Some of generic activities that are performed are as follows:

Equipment Installation

An installation checklist should be developed now with operating advice from the vendor and system development team.

Training Personnel

A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system.

System Change-Over Strategies

Conversion/changeover is the process of changing over or shifting over from the old system (may be the manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover, as it may put many resources/assets/operations at risk. The four types of popular implementation strategies are as follows:

- **Direct Implementation / Abrupt Change-Over:** With this strategy, the changeover is done in one operation, completely replacing the old system in one go.
- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually.
- **Pilot Changeover:** With this strategy, the new system replaces the old one in one operation but only on a small scale.
- **Parallel Changeover:** This is considered the most secure method with both systems running in parallel over an introductory period.

Conversion Activities

Conversion includes all those activities, which must be completed to successfully convert from the previous system to the new information system.

- **Procedure Conversion:** Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes.
- **File Conversion:** Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed.
- **System Conversion:** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one.
- **Scheduling Personnel and Equipment:** Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.

Phase VIII: Post Implementation Review and Systems Maintenance: A well-formalized review must be undertaken including some of the systems maintenance activities, such as adding new data elements, modifying reports, adding new reports; and changing calculations.

Post Implementation Review: A Post Implementation Review answers the question "Did we achieve what we set out to do in business terms?"

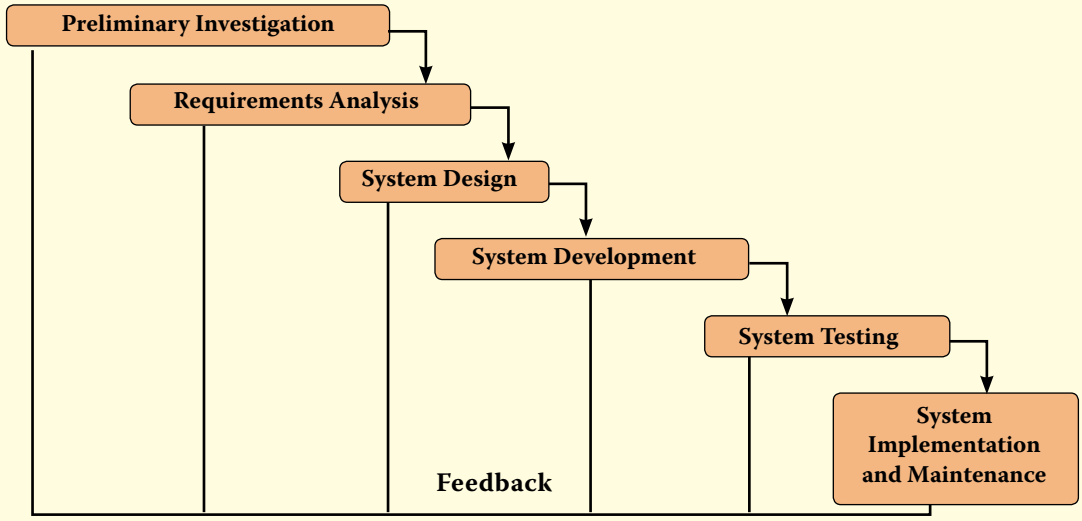
- **Development Evaluation:** It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained.
- **Operational Evaluation:** It tries to answer the questions related to functional aspects of the system.
- **Information Evaluation:** An information system should also be evaluated in terms of information it provides or generates.

System Maintenance: As key personnel change positions in the organization, new changes will be implemented, which will require system updates at regular intervals. It can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during the executions.
- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

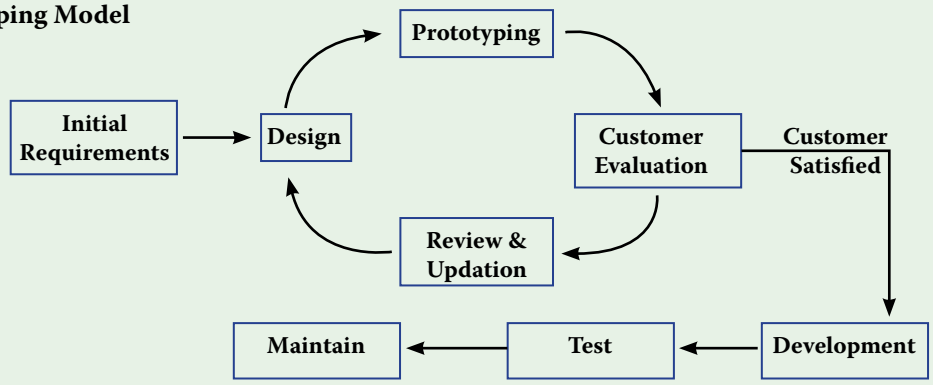
POPULAR SDLC MODELS

1. Waterfall Model



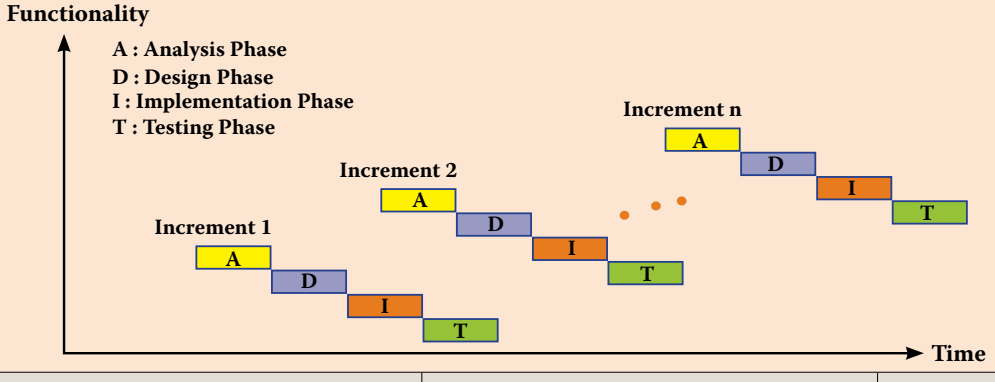
Concept	Advantages	Weaknesses
Project is divided into sequential phases, with some overlap and splash back/feedback acceptable between phases (in modified versions of Waterfall Model). ❖ **Preliminary Investigation** – Looking at the drawbacks in the existing system, establishing the need of propose system and applying cost benefit criteria in the proposed application. ❖ **Requirement Analysis** – Determining user information requirements and what they want from the new system. ❖ **Systems Design** – Designing the user interface, files to be used, and information processing functions to be performed by system. ❖ **System Development** – Designing, coding, compiling, testing, and documenting programs and system procedures and forms for the users of system. ❖ **System Testing** – Final testing of the system and formal approval and acceptance by management and users. ❖ **System Implementation and Maintenance** – Ongoing running of the system and subsequent modification considering problems detected.	❖ A waterfall model is easy to follow and can be implemented for any size project. ❖ A waterfall model helps find problems earlier on which can cost a business less than if it was found later. ❖ Requirements will be set and these would not be changed. ❖ Documentation is produced at every stage of a waterfall model, thus allowing people/new team to understand what has been done and what is to be done. ❖ Progress of system development is measurable. ❖ The orderly sequence ensures reliability, quality, adequacy and maintainability of developed software.	❖ **Inflexible**- rigid in requirement gathering and not open for change in requirement; ❖ **Slow**- as each phase is linear; ❖ **Costly and cumbersome.** ❖ If requirements change, the Waterfall model may not work.

2. Prototyping Model



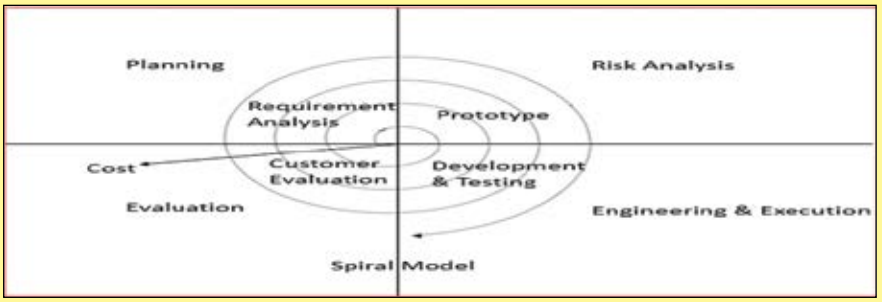
Concept	Advantages	Weaknesses
Prototyping is the process of quickly putting together a working model (a prototype) to test various aspects of a design, illustrate ideas or features and gather early user feedback. A small or pilot version called a **'Prototype'** is developed that is built quickly and at a lesser cost. 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. The basic idea here is that instead of freezing the requirements before a design or coding can proceed, a throwaway prototype is built to understand the requirements. This prototype is developed based on the currently known requirements. By using this prototype, the client can get an "actual feel" of the system, since the interactions with prototype can enable the client to better understand the requirements of the desired system.	❖ Users are actively involved in the development. ❖ Users can try the system and provide constructive feedback during development. ❖ Quicker user feedback is available leading to better solutions. ❖ An operational prototype can be produced in weeks. ❖ Users become more positive about implementing the system as they see a solution emerging that will meet their needs. ❖ Prototyping enables early detection of errors. ❖ Since in this methodology a working model of the system is provided, the users get a better understanding of the system being developed. ❖ Missing functionality can be identified easily.	❖ Each iteration builds on the previous iteration and further refines the solution. This makes it difficult to reject the initial solution as inappropriate and start over. ❖ Formal end-of-phase reviews do not occur. Thus, its is very difficult to contain the scope of the prototype. ❖ System documentation is often absent or incomplete, since the primary focus is on development of the prototype. ❖ System backup and recovery, performance, and security issues can be overlooked. ❖ Leads to implementing and then repairing way of building systems. ❖ Practically, this methodology may increase the complexity of the system as scope of the system may expand beyond original plans. ❖ Incomplete application may cause application not to be used as the full system was designed. ❖ Incomplete or inadequate problem analysis.

3. Incremental Model



Concept	Advantages	Weaknesses
The Incremental model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is defined as finished when it satisfies all its requirements. This model combines the elements of the waterfall model with the iterative philosophy of prototyping. The Incremental model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is decomposed into several components, each of which are designed and built separately (termed as builds).	❖ After each iteration, regression testing is conducted in which faulty elements of the software are quickly identified because few changes are made within any single iteration. ❖ Generally easier to test and debug than other methods of software development because relatively smaller changes are made during each iteration. This allows for more targeted and rigorous testing of each element within the overall product. ❖ Customer can respond to features and review the product for any needful changes.	❖ Resulting cost may exceed the cost of the organization. ❖ As additional functionality is added to the product, problems may arise related to system architecture which were not evident in earlier prototypes.

4. Spiral Model



Concept	Advantages	Weaknesses
Spiral model is a combination of sequential and prototype model. There are specific activities which are done in one iteration (spiral) where the output is a small prototype of the large software. The same activities are then repeated for all the spirals till the entire software is built. 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.	❖ High amount of risk analysis hence, avoidance of risk is enhanced. ❖ Good for large and mission-critical projects. ❖ Strong approval and documentation control. ❖ Additional Functionality can be added later. ❖ Software is produced early in the software life cycle.	❖ Can be a costly model to use. ❖ Risk analysis requires highly specific expertise. ❖ Project's success is highly dependent on the risk analysis phase. ❖ Does not work well for smaller projects.

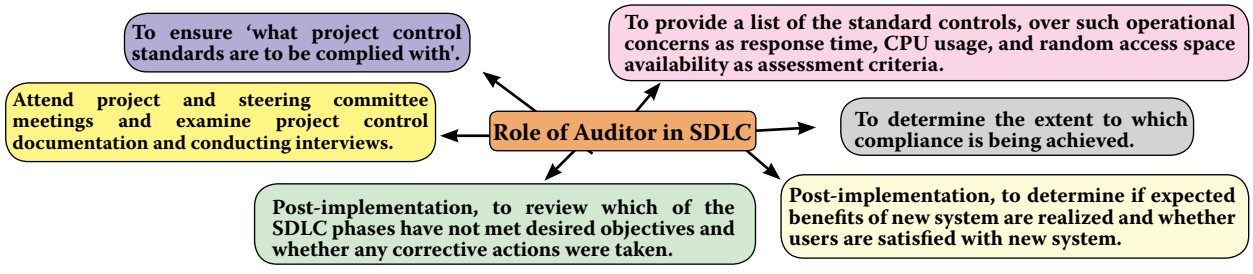
5. Rapid Application Development (RAD) Model: The RAD (Rapid Application Development) model is based on prototyping and iterative development with no specific planning involved. The process of writing the software itself involves the planning required for developing the product. RAD focuses on gathering customer requirements through workshops or focus groups, early testing of the prototypes by the customer using iterative concept, reuse of the existing prototypes (components), continuous integration and rapid delivery.

Concept	Advantages	Weaknesses
RAD approaches to software development but less emphasis on planning tasks and more emphasis on development. In contrast to the waterfall model, which emphasizes rigorous specification and planning, RAD approaches emphasize the necessity of adjusting requirements in reaction to knowledge gained as the project progresses. Features of model are: ❖ Rapid Application Development. ❖ Emphasizes on a short development cycle. ❖ A "high speed" adaptation of the waterfall model. ❖ Uses a component-based construction approach. ❖ May deliver software within a very short time (e.g. 60 to 90 days) if requirements are well understood and project scope is constrained.	❖ Reduced development time. ❖ Increases reusability of components. ❖ Quick initial reviews occur. ❖ Encourages customer feedback. ❖ Integration from very beginning solves a lot of integration issues.	❖ Depends on strong team and individual performances for identifying business requirements. ❖ Only system that can be modularized can be built using RAD. ❖ Requires highly skilled developers/ designers. ❖ High dependency on modeling skills. ❖ Inapplicable to cheaper projects as cost of modeling and automated code generation is very high.

6. Agile Model: Agile modelling is a methodology for modelling and documenting software systems based on best practices. It is an organized set of s/w development methodologies based on iterative and incremental development. This is an organized set of software development methodologies based on the ***iterative*** and ***incremental*** development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change.

Concept	Advantages	Weaknesses
Agile Manifesto is based on following 12 features: ❖ Customer satisfaction by rapid delivery of useful software; ❖ Welcome changing requirements, even late in development; ❖ Working software is delivered frequently (weeks rather than months); ❖ Working software is the principal measure of progress; ❖ Sustainable development, able to maintain a constant pace; ❖ Close, daily co-operation between business people and developers; ❖ Face-to-face conversation is the best form of communication (co-location); ❖ Projects are built around motivated individuals, who should be trusted; ❖ Continuous attention to technical excellence and good design; ❖ Simplicity; ❖ Self-organizing teams; and ❖ Regular adaptation to changing circumstances.	❖ Customer satisfaction by rapid, continuous delivery of useful software. ❖ People and interactions are emphasized rather than process and tools. Customers, developers and testers constantly interact with each other. ❖ Working software is delivered frequently (weeks rather than months). ❖ Face-to-face conversation is the best form of communication.	❖ In case of some software deliverables, especially the large ones, it is difficult to assess the effort required at the beginning of the software development life cycle. ❖ There is lack of emphasis on necessary designing and documentation. ❖ The project can easily get taken off track if the customer representative is not clear of what outcome that they want. ❖ Only senior programmers can take the kind of decisions required during the development process. Hence it has no place for newbie programmers, unless combined with experienced resources.

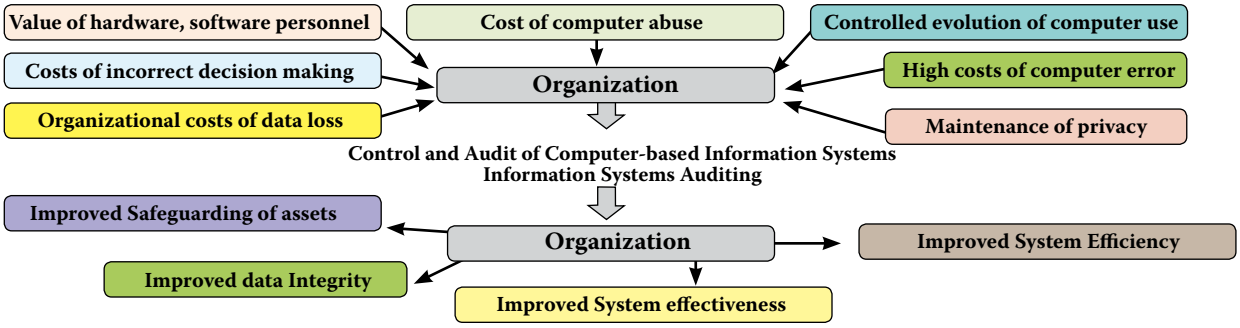
ROLE OF AUDITOR IN SDLC



CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS

This chapter comprehends the knowledge about the Information Systems Audit, its need, methodology and related standards. The chapter also provides an insight to various types of controls, their related concepts and their audit.

NEED AND CONTROL OF INFORMATION SYSTEMS' AUDIT

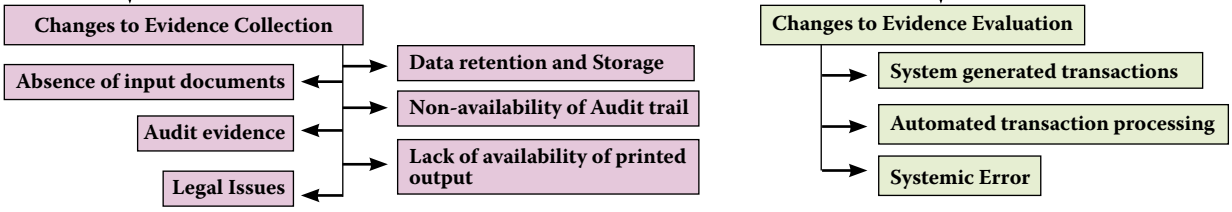


NEED AND CONTROL OF INFORMATION SYSTEMS' AUDIT	
Organisational Costs of Data Loss	Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
Cost of Incorrect Decision Making	Management and operational controls taken by managers involve detection, investigations and correction of the processes.
Value of Computer Hardware, Software and Personnel	These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
Costs of Computer Abuse	Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets.
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.
High Costs of Computer Error	In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
Maintenance of Privacy	Data collected in a business process contains private information about an individual that needs to be maintained.
INFORMATION SYSTEMS' AUDIT OBJECTIVES	
Asset Safeguarding Objectives	The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
Data Integrity Objectives	Data integrity important from the business perspective of the decision maker, competition and the market environment.
System Effectiveness Objectives	Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
System Efficiency Objectives	To optimize the use of various information system resources along with the impact on its computing environment.

EFFECT OF COMPUTERS ON AUDIT

To examine Effect of Computers on IS Audit

(The auditor should be competent to independent evaluation as to whether the business process activities are recorded and reported as per established standards or criteria.)



INFORMATION SYSTEMS' AUDITOR

SKILL SET

- ❖ Sound knowledge of business operations, practices and compliance requirements;
- ❖ Should possess the requisite professional technical qualification and certifications;
- ❖ Good understanding of information Risks & Controls;
- ❖ Knowledge of IT strategies, policy & procedural controls;
- ❖ Ability to understand technical and manual controls relating to business continuity; and
- ❖ Good knowledge of Professional Standards and Best Practices of IT controls & security.

FUNCTIONS (To Assess)

- ❖ Inadequate information security controls;
- ❖ Inefficient use of resources, or poor governance;
- ❖ Ineffective IT strategies, policies and practices; and
- ❖ IT-related frauds (including phishing, hacking etc.)

INFORMATION SYSTEMS' AUDIT

The **Information Systems (IS) Audit** process is to evaluate the adequacy of internal controls about both specific computer program and the data processing environment. The IS Audit of an IS environment may include one or both:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.
- Assessment of the efficiency and effectiveness of the IS environment.

INFORMATION SYSTEMS' AUDIT

CATEGORIES

Systems and Application: To verify that systems & 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.

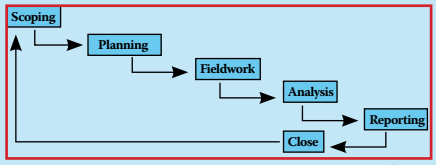
Information Processing Facilities: To verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

Systems Development: To ensure that the systems are developed in accordance with generally accepted standards for systems development.

Management of IT and Enterprise Architecture: To verify that Information Technology management has developed an organizational structure & procedures to ensure a controlled & efficient environment for information processing.

Telecommunications, Intranets, and Extranets: To verify that controls are in place on the client (end-point device), server, and on the network connecting the clients and servers.

STEPS



Scoping and pre-audit survey: Auditors determine main area/s of focus based on scope-definitions agreed with management.

Planning and preparation: The scope is broken down into greater levels of detail, usually involving generation of audit work plan or risk-control-matrix.

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

Analysis: SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

Reporting: Reporting to the management is done after analysis of evidence is gathered and analysed.

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

TOOLS

Snapshots: The snapshot software is built into system at those points where material processing occurs which takes images of flow of any transaction as it moves through application.

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.

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.

Continuous and Intermittent Simulation (CIS): This technique can be used to trap exceptions whenever the application system uses a DBMS.

Audit Hooks: These are audit routines that flag suspicious transactions.

AUDIT TRAIL

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

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained.

- ❖ The Accounting audit trail shows the source and nature of data and processes that update the database.
- ❖ The Operations audit trail maintains record of attempted or actual resource consumption within a system.

Audit Trail Objectives: Audit trails can be used to support security objectives in three ways:

- ❖ **Detecting unauthorized access to the system:** 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.
- ❖ **Facilitating the reconstruction of events:** Audit analysis can be used to reconstruct steps that led to events such as system failures, security violations by individuals, or application processing errors.
- ❖ **Promoting 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 behaviousr.

MANAGERIAL CONTROLS - AUDIT TRAILS

Managerial Controls	Audit Trails
Top Management and Information Systems Management Controls	❖ **Planning:** Auditors need to evaluate whether top management has formulated a high-quality IS's plan that is appropriate to the needs of an organization or not. ❖ **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources. ❖ **Leading:** Auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. ❖ **Controlling:** 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.
System Development Management Controls	❖ **Concurrent Audit:** Auditors assist the team in improving the quality of systems development for the specific system they are building and implementing. ❖ **Post -implementation Audit:** Auditors seek to help an organization learn from its experiences in the development of a specific application system. ❖ **General Audit:** Auditors seek to determine whether they can reduce extent of substantive testing needed to form an audit opinion about management's assertions relating to financial statements for systems effectiveness & efficiency.
Programming Management Controls	❖ **Planning:** Auditors must evaluate how well the planning work is being undertaken. ❖ **Control:** Auditors must evaluate whether the nature of and extent of control activities undertaken are appropriate for different types of s/w that are developed or acquired. ❖ **Design:** Auditors should find out whether programmers use some type of systematic approach to design. ❖ **Coding:** Auditors should seek evidence to check whether programmers employ automated facilities to assist them with their coding work.

	❖ **Testing:** Auditor's primary concern is to see that unit testing; integration testing of the system testing has been undertaken appropriately. ❖ **Operation and Maintenance:** Auditors need to ensure effectively & timely reporting of maintenance needs occurs & maintenance is carried out in a well-controlled manner.
Data Resource Management Controls	Auditors should determine what controls are exercised to maintain data integrity. They might employ test data to evaluate whether access controls and update controls are working.
Quality Assurance Management Controls	Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring and reporting function.
Security Management Controls	Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; and check whether organisations have opted appropriate Disaster Recovery and Insurance plan or not.
Operations Management Controls	Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

APPLICATION CONTROLS - AUDIT TRAILS

Application Controls	Audit Trails
Boundary	This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.
Input	This maintains the chronology of events from the time data and instructions are captured and entered an application system until the time they are deemed valid and passed onto other subsystems within the application system.
Communication	This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.
Processing	The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.
Output	The audit trail maintains the chronology of events that occur either to the database definition or the database itself.
Database	The audit trail maintains the chronology of events that occur from the time the content of the output is determined until time users complete their disposal of output because it no longer should be retained.

CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUES

This chapter provides the knowledge about various sections of IT Act and its rules as relevant for assurance and assessing the impact of non-compliance. Furthermore, it also provides the knowledge about various regulatory bodies such as RBI, SEBI and IRDA.

INFORMATION TECHNOLOGY ACT

The Information Technology Act was enacted on 17th May 2000, primarily to provide legal recognition for electronic transactions and facilitate e-commerce. The IT Act was amended by passing of the Information Technology (Amendment) Act 2008 (Effective from October 27, 2009).

[Chapter II] Digital Signature and Electronic Signature This chapter of IT Act gives legal recognition to electronic records and digital signatures. It contains only Section 3. The section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature.	
[Section 3]	Authentication of Electronic Records
[Section 3A]	Electronic Signature
[Chapter III] Electronic Governance This chapter specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt. This chapter contains sections 4 to 10.	
[Section 4]	Legal Recognition of Electronic Records
[Section 5]	Legal Recognition of Electronic Signatures
[Section 6]	Use of Electronic Records and Electronic Signatures in Government and its agencies
[Section 6A]	Delivery of services by Service Provider
[Section 7]	Retention of Electronic Records
[Section 7A]	Audit of Documents, etc. maintained in Electronic form
[Section 8]	Publication of rules, regulation, etc., in Electronic Gazette
[Section 9]	Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form
[Section 10]	Power to make rules by Central Government in respect of Electronic Signature
[Section 10A]	Validity of contracts formed through electronic means
[Chapter V] Secure Electronic Records and Secure Electronic Signatures Chapter V sets out the conditions that would apply to qualify electronic records and digital signatures as being secure. It contains sections 14 to 16.	
[Section 14]	Secure Electronic Record
[Section 15]	Secure Electronic Signature
[Section 16]	Security Procedures and Practices
[Chapter IX] Penalties, Compensation and Adjudication This chapter contains sections 43 to 47, out of which sections 43 to 45 deal with different nature of penalties. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudication Officer for holding an inquiry in relation to certain computer crimes and for awarding compensation.	
[Section 43]	Penalty and Compensation for damage to computer, computer system, etc.
[Section 43A]	Compensation for failure to protect data
[Section 44]	Penalty for failure to furnish information return, etc.
[Section 45]	Residuary Penalty

[Chapter XI] Offences Apart from giving recognition to electronic contracts, the IT Act identifies certain acts as "Computer Crimes" and provides penalties for these offences. The Act lists common crimes that can be perpetuated in the electronic society and specifies penalty. The Computer crimes that are recognized by the Act could affect hackers; Digital Contract parties; The Digital IC users; Netizen; Web Site owners/Content creators; Software professionals; Auditors and Certifying authorities web hosting firms. Chapter XI deals with offences under the IT Act.	
[Section 65]	Tampering with Computer Source Documents
[Section 66]	Computer Related Offences
[Section 66A]	Punishment for sending offensive messages through communication service, etc.
[Section 66B]	Punishment for dishonestly receiving stolen computer resource or communication device
[Section 66C]	Punishment for identity theft
[Section 66D]	Punishment for cheating by personation by using computer resource
[Section 66E]	Punishment for violation of privacy
[Section 66F]	Punishment for cyber terrorism
[Section 67]	Punishment for publishing or transmitting obscene material in electronic form
[Section 67A]	Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
[Section 67B]	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
[Section 67C]	Preservation and Retention of information by intermediaries
[Section 68]	Power of the Controller to give directions
[Section 69]	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
[Section 69A]	Power to issue directions for blocking for public access of any information through any computer resource
[Section 69B]	Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
[Section 70]	Protected system
[Section 70A]	National nodal agency
[Section 70B]	Indian Computer Emergency Response Team to serve as national agency for incident response

[Section 71]	Penalty for misrepresentation
[Section 72]	Penalty for breach of confidentiality and privacy
[Section 72A]	Punishment for Disclosure of information in breach of lawful contract
[Section 73]	Penalty for publishing Electronic Signature Certificate false in certain particulars
[Section 74]	Publication for fraudulent purpose
[Section 75]	Act to apply for offences or contraventions committed outside India
[Section 76]	Confiscation
[Chapter XII] Intermediaries not to be liable in Certain Cases This chapter contains Section 79 that provides details of the exemption from liability of intermediary in certain cases.	
[Section 79]	Exemption from liability of intermediary in certain cases

[Chapter XIIA] Examiner of Electronic Evidence	
[Section 79A]	Central Government to notify Examiner of Electronic Evidence
[Chapter XIII] Miscellaneous	
[Section 80]	Power of police officer and other officers to enter, search, etc.
[Section 81]	Act to have Overriding effect
[Section 81A]	Application of the Act to electronic cheque and truncated cheque
[Section 84B]	Punishment for abetment of offence
[Section 84C]	Punishment for attempt to commit offences
[Section 85]	Offences by Companies

VARIOUS AUTHORITIES FOR SYSTEMS CONTROL AND AUDIT

1. IRDA for Systems Control and Audit (IRDA): The **Insurance Regulatory and Development Authority of India (IRDA)** is the apex body overseeing the insurance business in India. It protects the interests of the policyholders, regulates, promotes and ensures orderly growth of the insurance in India. Information System Audit aims at providing assurance in respect of Confidentiality, Availability and Integrity for Information systems. It also looks at their efficiency, effectiveness and responsiveness. It focuses on compliance with laws and regulations.

2. RBI for System Control and Audit: The **Reserve Bank of India (RBI)** is India's central banking institution, which formulates the monetary policy about the Indian rupee. The Reserve Bank of India (RBI) has been at the forefront of recognizing and promoting IS Audit internally and across all the stakeholders including financial institutions. RBI provides guidelines on key areas of IT implementation by using global best practices. They have constituted various expert committees who review existing and future technology and related risks and provide guidelines, which are issued by all stakeholders. Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the IT related risks are managed.

3. SEBI for Systems Control and Audit: The **Securities and Exchange Board of India (SEBI)** is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market - The issuers of securities; The investors, and the market intermediaries. Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders.

SECURITY STANDARDS

1. ISO 27001 - This standard is the foundation of Information Security Management. **ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-Technical Commission (IEC))** defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is a standard written by the world's best experts in the field of information security and aims to provide a methodology for the implementation of information security in an organization. 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 best possible way in organization.

2. STANDARD ON AUDITING (SA) 402 - (SA) 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24; "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002. The revised Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor.

3. INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) - The ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (ITILv3), it is published in series of five core publications, each of which covers an ITSM lifecycle stage. ITIL has rapidly been adopted across the world as the standard for best practice in the provision of IT services. ITIL assists in establishing a business management approach and discipline to IT Service Management.

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)

SERVICE STRATEGY
- Provides guidance on clarification and prioritization of service-provider investments in services.
- Includes functions in IT Service Generation, Service Portfolio Mgt.; Financial Mgt.; Demand Mgt. and Business Relationship Management.

SERVICE DESIGN
- Provides good-practice guidance on design of IT services, processes, and other aspects of service management effort;
- Includes functions in Service Catalogue; Service Level Mgt.; Availability; Capacity; IT Service Continuity Mgt.; Information Security Mgt. and Supplier Management.

SERVICE TRANSITION
- Relates to delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than BAU;
- Includes functions in Service Transition Planning & Support; Change Mgt.; Service Asset & Configuration Mgt.; Release & Deployment Mgt.; Service Validation and Testing; Change Evaluation; and Knowledge Mgt.

SERVICE OPERATION
- Provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers;
- Includes functions in Functions Incident Management; Request Fulfillment; Access Management; Event Management, and Problem Management.

Continual Service Improvement

(Aims to align and realign IT services to changing business needs by identifying/ implementing improvements to IT services that support business processes).

CHAPTER – 8 EMERGING TECHNOLOGIES

This chapter introduces the Emerging Technologies like Cloud Computing, Mobile Computing, Green Computing etc. and their perspectives.

I. Grid Computing: Grid computing is a network of computing or processor machines managed with a kind of software such as middleware, to access and use the resources remotely. Grid Services provide access control, security, access to data including digital libraries and databases, and access to large-scale interactive and long-term storage facilities.

Grid Computing is more popular due to the following reasons:

- ❖ It can make use of unused computing power, and thus, it is a cost-effective solution (reducing investments, only recurring costs).
- ❖ Enables heterogeneous resources of computers to work cooperatively and collaboratively to solve a scientific problem.

II. Cloud Computing: Cloud Computing is both, a combination of software and hardware based computing resources delivered as a networked service. This model of IT-enabled services enables anytime access to a shared pool of applications and resources. These applications and resources can be accessed using a simple front-end interface such as a Web browser, and thus enabling users to access the resources from any client device including notebooks, desktops and mobile devices.

Architecture	Characteristics	Advantages
❖ **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. ❖ **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.	❖ High Scalability ❖ Agility & Multi-sharing ❖ High Availability and Reliability ❖ Services in Pay-Per-Use Mode ❖ Virtualization ❖ Performance & Maintenance	❖ Cost Efficiency ❖ Almost Unlimited Storage ❖ Backup & Recovery ❖ Automatic Software Integration ❖ Easy Access to Information ❖ Quick Deployment

Types of Cloud			
Private Cloud	**Public Cloud**	**Community Cloud**	**Hybrid Cloud**
This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits.	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.	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).	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.
Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud)	Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis	It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises.	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.

Service Models		
Infrastructure as a Service (IaaS)	**Platform as a Service (PaaS)**	**Software as a Service (SaaS)**
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.	PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider. PaaS changes the application development from local machine to online.	SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.
This allows users to maximize the utilization of computing capacities without having to own and manage their own resources. Different instances are - NaaS, STaaS, DBaaS, BaaS, and DTaaS.	PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases.	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.

Cloud Computing Security Issues
❖ **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality.
❖ **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.
❖ **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP).
❖ **Governance:** Due to the lack of control over employees and services, it creates problems relating to design, implementation, testing & deployment. So, there's a need of governance model, which controls standards, procedures & policies of organization.
❖ **Trust:** Deployment model provided a trust to the Cloud environment. An organization has direct control over security aspects as well as the federal agencies even have responsibility to protect the information system from the risk.
❖ **Compliance and Legal Issues:** There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. One of the major troubles with laws is that they vary from place to place, and users have no assurance of where the data is located physically.
❖ **Privacy:** Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity.
❖ **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before virtualized application environment, which is being hosted on virtual machine to watch 'what is happening in system'.
❖ **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing.
❖ **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model.
❖ **Identity Management and Access control:** The key critical success factor for Cloud providers is to have a robust federated identity management architecture and strategy internal in the organization.
❖ **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that Cloud provider has transparent response process in place & sufficient mechanisms to share information during & after an incident.
❖ **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that Cloud provider employs in its multi-tenant software architecture, and evaluate the risks required for the organization.
❖ **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have complete access to server with all rights for monitoring/maintenance of server.

Cloud Computing Implementation/Adaptation Issues
❖ **Threshold Policy:** To test if the program works, develops, or improves and implements; a threshold policy is of immense importance in a pilot study before moving the program to the production environment. This involves the checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand.
❖ **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors.
❖ **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'.
❖ **Unexpected Behaviour:** It's important to test application in cloud with a pilot study to check for unexpected behaviour.
❖ **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project.
❖ **Environment Friendly Cloud Computing:** One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data centre and replacing them with cloud computing systems reduces energy for running and cooling hardware.

III. 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.

Components	Limitations	Advantages
❖ **Mobile Communication:** Refers to infrastructure put in place to ensure that seamless and reliable communication goes on. ❖ **Mobile Hardware:** This includes mobile devices/device components that range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA). ❖ **Mobile Software:** It is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications.	❖ Insufficient Bandwidth ❖ Security Standards ❖ Power consumption ❖ Transmission interferences ❖ Potential health hazards ❖ Human interface with device	❖ Security Issues like Confidentiality; Integrity; Availability; Legitimate Accountability and Bandwidth; ❖ Location Intelligence; ❖ Power Consumption; ❖ Revising technical architecture; ❖ Reliability, coverage, capacity, and cost; ❖ Integration with legacy mainframe and emerging client/server applications; ❖ End-to-end design and performance; and ❖ Business challenges

IV. Green Computing: Green Computing or Green IT refers to the study and practice of environmentally sustainable computing or IT. In other words, it is the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way.

Best Practices	❖ Develop a sustainable Green Computing plan ❖ Recycle ❖ Make environmentally sound purchase decisions ❖ Reduce Paper Consumption ❖ Conserve Energy

V. BYOD (Bring Your Own Device): This refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application.

Advantages	Emerging Threats
❖ Happy Employees ❖ Lower IT budgets ❖ IT reduces support requirement ❖ Early adoption of new Technologies ❖ Increased employee efficiency	❖ **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. ❖ **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. ❖ **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'. ❖ **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy.

WEB 2.0 AND WEB 3.0 TECHNOLOGIES

Web 2.0 Technology	Web 3.0 Technology
❖ Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. ❖ The two major contributors of Web 2.0 are the technological advances enabled by Ajax (Asynchronous JavaScript and XML) and other applications and other applications such as RSS (Really Simple Syndication) and Eclipse that support the user interaction and their empowerment in dealing with the web. ❖ The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner.	❖ Known as the Semantic Web, this describes sites wherein the computers will generate raw data on their own without direct user interaction. ❖ Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. ❖ Web 3.0 Technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence. ❖ The two major components of Web 3.0 are as follows: • **Semantic Web:** 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 • **Web Services:** It is a software system that supports computer - to - computer interaction over the Internet. ❖ An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence. ❖ Web 3.0 helps to achieve a more connected open and intelligent web applications using the concepts of natural language processing machine learning, machine reasoning and autonomous agents.