

Ch-1 CONCEPT OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEM

1.1. Concept of Governance:

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.

GOVERNANCE	ENTERPRISE GOVERNANCE	CORPORATE GOVERNANCE
<ul style="list-style-type: none">•All means and mechanism that will enable stakeholder to have an organised mechanism for evaluation, monitoring compliances and performance.	<ul style="list-style-type: none">•Set of responsibilities & practices exercised by the board and executive management to ensure proper monitoring, objectives are achieved, risks are managed properly.	<ul style="list-style-type: none">•System by which a company or enterprise is directed & controlled to achieve the objectives of increasing shareholder value by enhancing the economic performance.

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.

BENEFITS OF GEIT: M.A.R.E.

- M**onitoring → The IT related processes are seen effectively and transparently.
- A**pproach → Ensures consistency in approach and in alignr with enterprises strategy.
- R**equirements are met → Ensures governance requiremen board are met.
- E**nsures that IT related decisions are taken in tune with enterprise strategy.

BENEFITS OF GOVERNANCE:

1. Increased value delivered through enterprise
2. Increased user satisfaction with IT services.
3. Better cost performance of IT.
4. Improved transparency and understanding of
5. Improved compliance with law.

Evaluate the governance system:

- Have communication with stakeholders, document the requirements,
- Make judgment on the current and future design of the governance of enterprise IT.

Direct the governance system:

- Inform leader and obtain their support.
- Guide the structures, processes and practices in line with agreed governance principle, decision making principles.

Monitor the governance system:

- Monitor the effectiveness and performance of the enterprises governance of IT.
- To ascertain whether the mechanism is working efficiently or not.

Key
Governance
Practices of
GEIT

1.2. Control as per COSO:

1. **Control Environment:** Entity need to develop and maintain controlled environment.
2. **Risk assessment:** Necessity of regular assessment of the risks
3. **Control activities:** Control activities must be developed to manage, mitigate and reduce risk associated with business processes.
4. **Information and communication:** Information needed to conduct, manage and control business processes.
5. **Monitoring:** Internal control processes must be continuously monitored and adaptable to changing conditions

1.3. Key functions of IT steering committee:

1. To ensure long & short-term plans of IT department are in tune with the organization objectives and goals.
2. To review and approve standards, policies & procedures.
3. To establish size and scope of IT functions & set priorities.
4. To review & approve IT deployment projects in all stages.
5. To make decision on IT deployment & implementation.
6. To facilitate implementation of IT security within enterprise

1.4. IT STRATEGY PLANNING:

IT STRATEGY PLANNING PROCESS

1. Planning process must be dynamic in nature.
2. Process owner must ensure that process must be in place to ensure modification in IT plans as per change in IT conditions.
3. It must be ensured that IT function resources are allocated on basis consistent with the long term plan.

STRATEGIC PLANNING

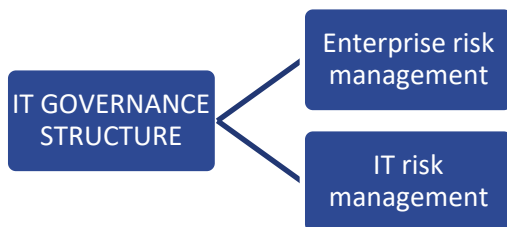
1. Refers to planning undertaken by the top management,
2. Towards meeting long term objectives of the enterprises.
3. There are 3 levels of managerial activity in an enterprise.

IT Strategic planning in enterprises can be classified into 4 categories

ENTERPRISE STRATEGIC PLAN	INFORMATION SYSTEMS STRATEGIC PLAN	INFORMATION SYSTEMS REQUIREMENT PLAN	INFORMATION SYSTEMS APPLICATIONS AND FACILITIES PLAN
This plan encompasses the overall charter of the enterprises under which all units, including information systems must operate.	IS strategy focus on striking balance between IT opportunities & business requirement. It requires strategic planning process to be undertaken at regular interval for long term planning. And this plans to be translated into operational plans	Enterprise needs to have defined information structure so as to optimise the requirement from the information system. So, business has to ensure that business information model Have to be reviewed periodically to optimise the use of the information	On the basis of information systems architecture, management can develop an information systems applications and facilities. The senior management is responsible for developing and implementing the long & short term missions and goals. plan period vary from 1-3 years

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 data 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.

1.5. RISK MANAGEMENT:

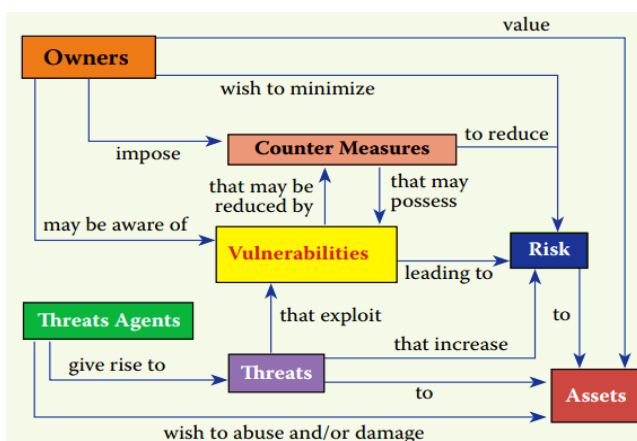


SOURCES OF THE RISK

BUSINESS RELATED	OTHER FACTORS
Commercial and legal relationship	Human Behavior
Technology and technical Issues	Natural Events
Management Activities and Controls	Individual Activities

COUNTER MEASURE:

An action, device, procedure, technique that reduces the vulnerability of a system or Component is termed as counter measure.



ASSETS:

Asset can be defined as something of value to the organization. Example information in e-form, software system, employees...

VULNERABILITY:

It is the weakness in the system safeguard that exposes system to THREATS.

THREATS:

Any entity, circumstances with the potential to harm the software system or component through unauthorized access, destructions or modifications.

EXPOSURE:

It is the extent of the loss to the organization when a materialized (occurs). For instance, loss of business, loss of reputation, violation of the privacy etc.

LIKELIHOOD:

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

ATTACK:

It is the set of action designed to compromise confidentiality & availability of an information system.

RISK:

It is likelihood that an organisation would face vulnerability becoming harmful. Risk analysis is a process of identifying the magnitude of the risk and their impact on entity.



1.6 COBIT 5:

As per COBIT, information is the success drivers but also it can't be ignored that it also raises governance and management issues too. This section explains need for using approach and latest thinking for reviewing and implementing governance and management of enterprise IT.

Need for COBIT by enterprise

- Enterprise needs good, reliable, repeatable data on which they can take good business decision.
- COBIT 5 is made and is customised to suit all the enterprises irrespective of their size, industries and geographical areas
- COBIT 5 provides enterprises a tool necessary to understand, utilise, implement and direct important IT related activities.
- COBIT 5 is intended to deliver business benefits to enterprises:
- Increased use of IT experts, user satisfaction, less IT related risks etc.
- Development of IT related business solutions.
- Increased enterprise wide involvement in IT related activities.

Components of COBIT

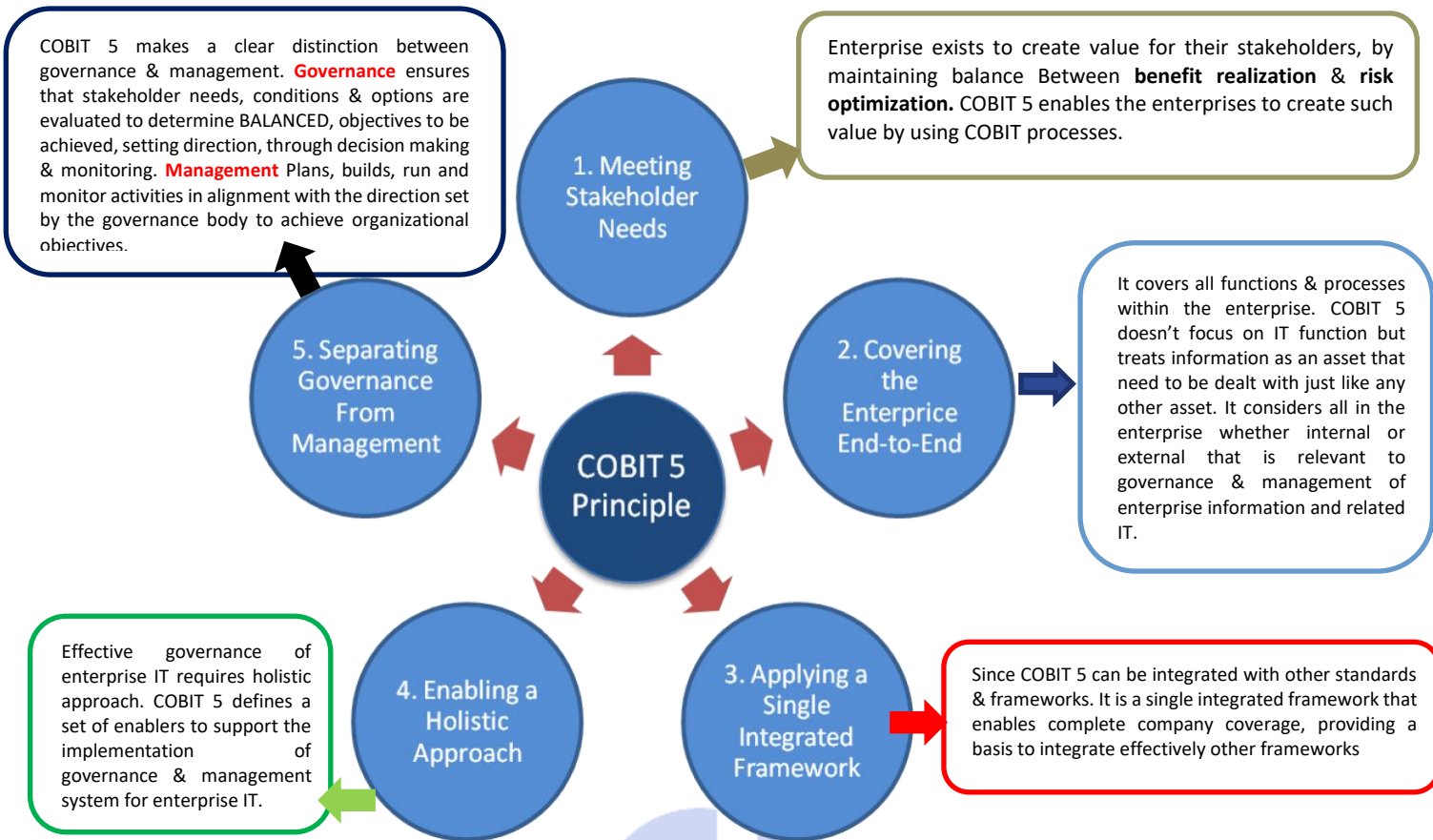
- FRAMEWORK**
 - Organise IT governance objectives and good practices by IT domains and processes and links to business requirement.
- PROCESS DESCRIPTION**
 - Common language for everyone in the entity. The processes map to responsibilities areas of plan, build, run and monitor.
- CONTROL OBJECTIVES**
 - Provide comprehensive requirements to be considered by the management for effective control for the processes.
- MANAGEMENT GUIDELINES**
 - Helps in assigning responsibilities, agree on objective, measure performance.
- MATURITY MODEL**
 - Organise IT governance objectives and good practices by IT domains and processes.

Benefits of COBIT

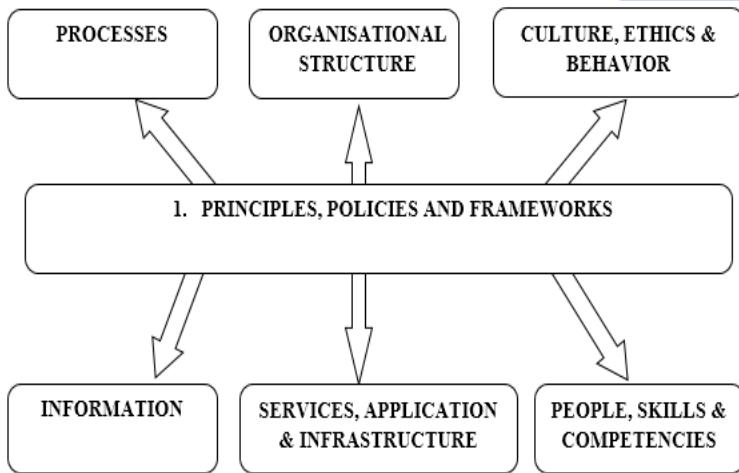
- ENTITY GOALS AND IT:**
 - 1.COBIT 5 enables enterprises in achieving their objectives for governance and management of enterprise IT.
 - 2.COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risks level and resource use.
 - 3.COBIT 5 enables IT to be governed in such a manner that to ensure full end-to-end business and IT functional areas of responsibilities, considering the interest of internal and external stakeholders.
- GENERAL BENEFITS:**
 - 1.COBIT 5 supports compliance with relevant laws, regulations, agreements and policies.
 - 2.COBIT 5 is useful for all types of organization whether commercial or not.

COBIT 5 can be tailored to meet the enterprise's need. Because of its open design, it can be applied to meet needs related to:

- Information security
- Risk Management
- Financial Processing
- Assurance Activities
- Governance & Management of enterprise IT
- Legislative & regulatory compliance



COBIT 5 ENABLERS



Principles, policies & framework	Vehicles to translate the desired behavior into practical guidance for day-to-day management.
Process	Describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
Organizational structure	Are the key decision-making entities in an organisation.
Culture, ethics & behavior	Of individuals and of the organization; very often underestimated as a success factor in governance and management activities.
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.
Service, app. & infrastructure	Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
People skill & competencies	Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Way to remember above points

In **organisation structure** there are **people with skill & competencies** that use **information** to introduce **principles, policies & framework** in the processes so that there exists **good culture, ethics & behavior**. After all this, company can provide **quality services, infrastructure & applications**.

USING COBIT 5 for IS assurance



There are some key practices for assessing and evaluating the internal control system

PART A : MONITORING ASPECTS	
MONITORING OF:	
Internal Controls	Continuously monitor benchmark and improve IT control environment in order to meet the organizational needs.
Business Process Efficiency	Following things are covered under this review of internal control: Review operation of controls (How controls work in entity) --Review of monitoring & test evidences to ensure controls are effectively operating. --Maintain of evidences such as per periodic testing of controls, independent assessment etc.
Report Control Deficiencies	--Identify deficiencies in controls and analyze the root cause of such deficiencies. --Report such deficiencies to the stakeholders.
Perform Control self-assessment	--Encourage management to take positive ownership of control improvement through continuous program of self-assessment.

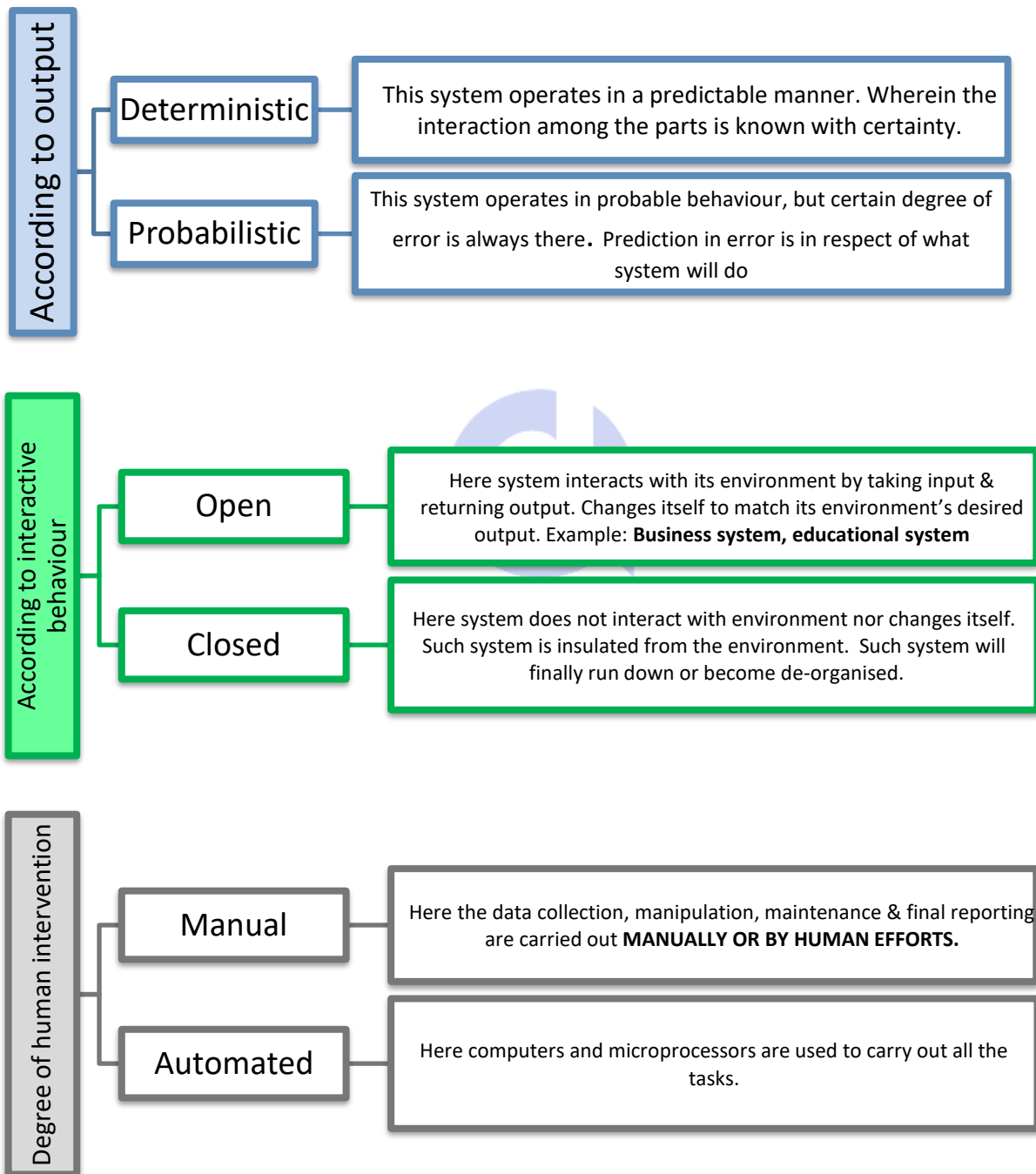
PART B : INITIATIVE ASPECTS	
Plan Assurance Initiatives	-- Plan assurance initiative based on enterprise objectives, -- Assurance objectives, strategy priorities, inherent risk resource constraint
Scope Assurance Initiatives	--Define and agree with management on scope of assurance initiative based on assurance objectives.
Execute Assurance Initiatives	--Execute planned assurance initiatives. --prepare report on identified findings. --Provide assurance opinions, recommendation for improvements related to operational performance, external compliance & internal controls.

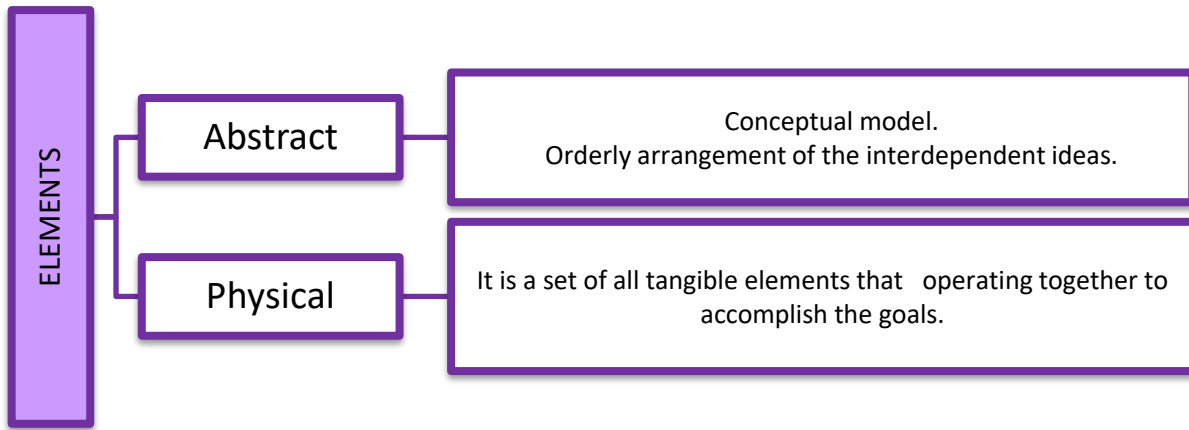
CHAPTER 2: INFORMATION SYSTEM CONCEPT

2.1 Definition of Information System:

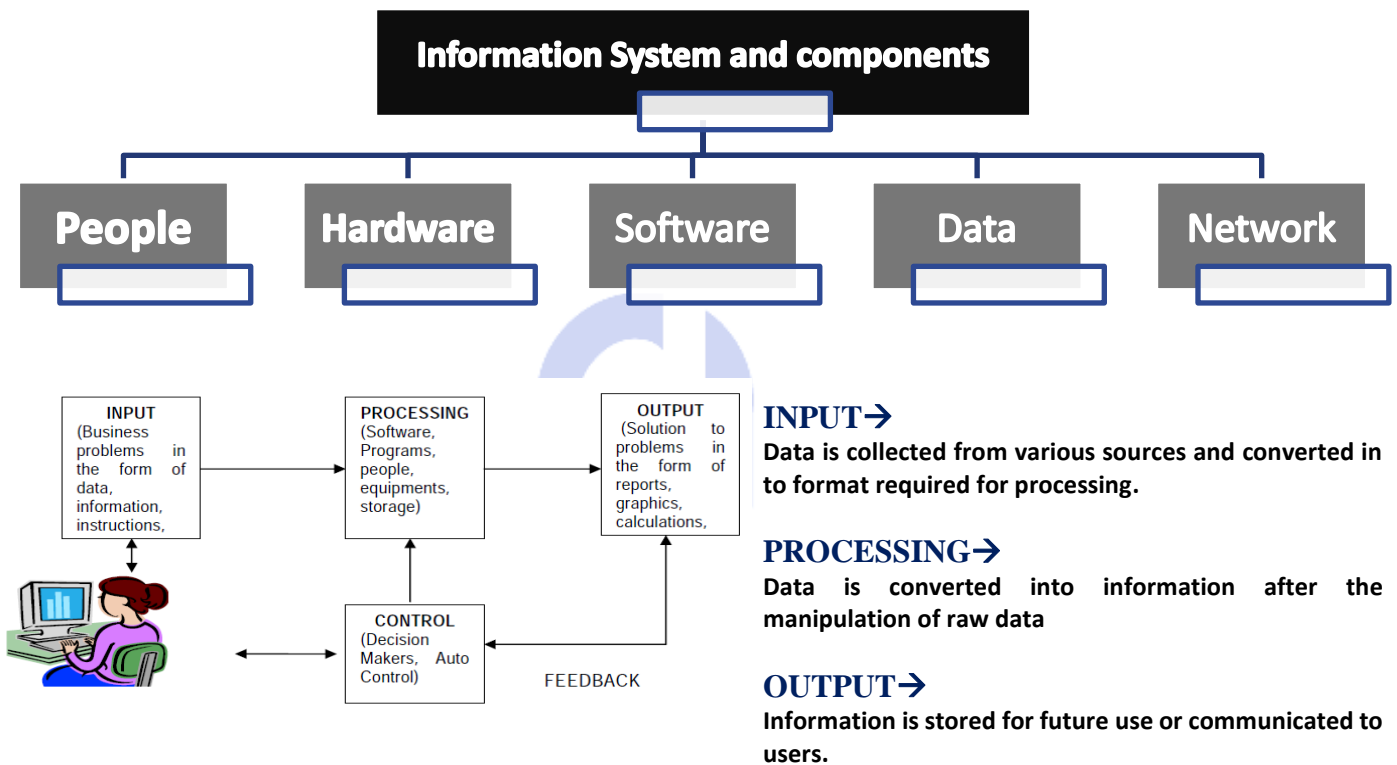
This Information system is termed as system that comprises of people, computer system, data and network that helps to COLLECT, STORE AND ANALYSE DATA to produce the desired information for the functioning, betterment and expansion of the business.

2.2 Overview of information systems and practical aspect of its application in enterprise processes:





2.3 Information System and components:



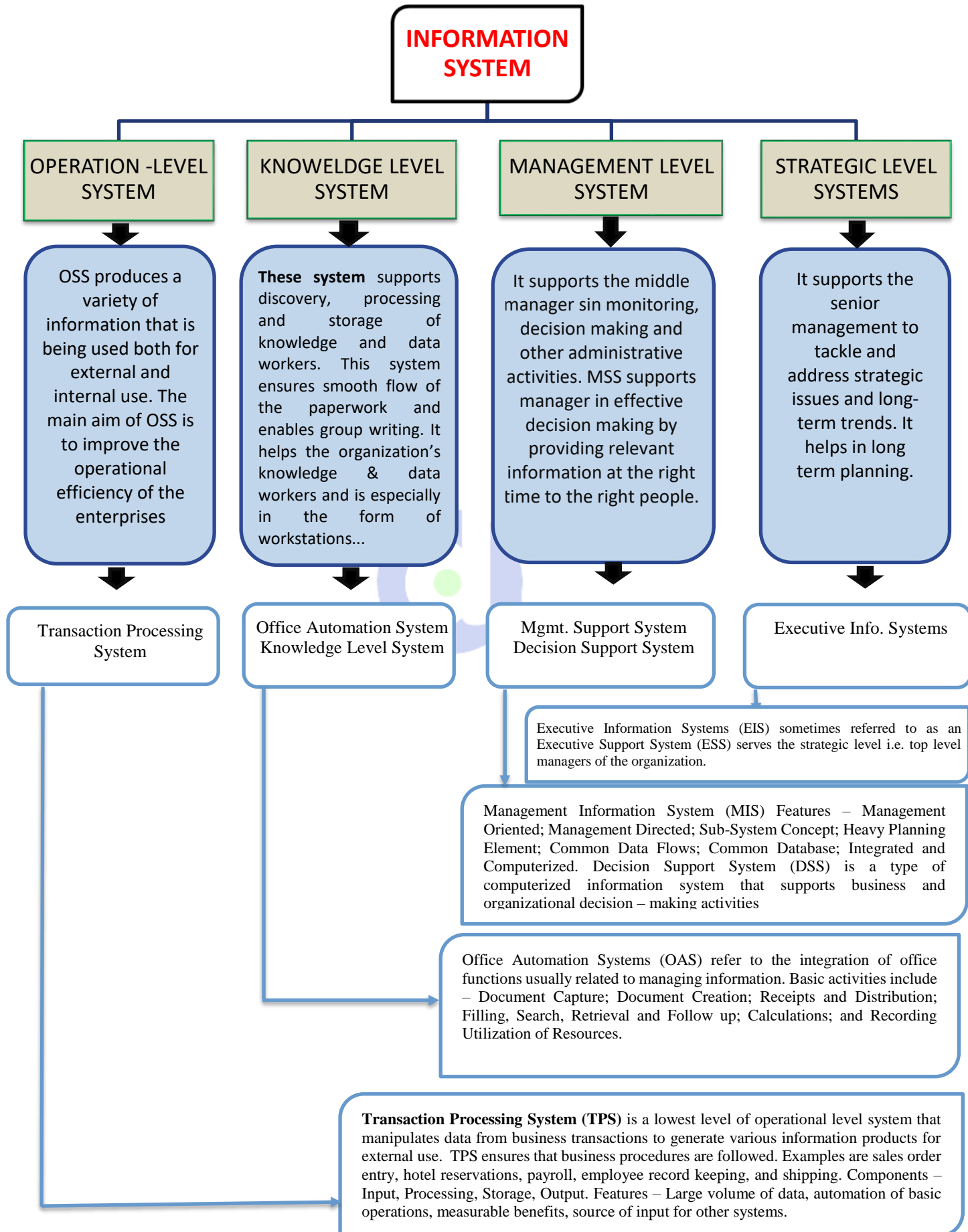
STEPS IN INFORMATION SYSTEM MODEL COMPRISES

IMPORTANT CHARACTERISTICS OF COMPUTER BASED INFORMATION SYSTEM

Code: F.O.I.L.

1. If one sub system Fails, the whole system may work or not that depends on how sub systems are inter-related.
2. All systems work for predetermined Objectives & is designed & developed accordingly.
3. All sub-system in a system Interacts with each other and can't work in isolation.
4. Work done by individual sub system is integrated to achieve the central goal of the system. Low priority is given to importance to individual sub system.

2.4 Types of Information System:

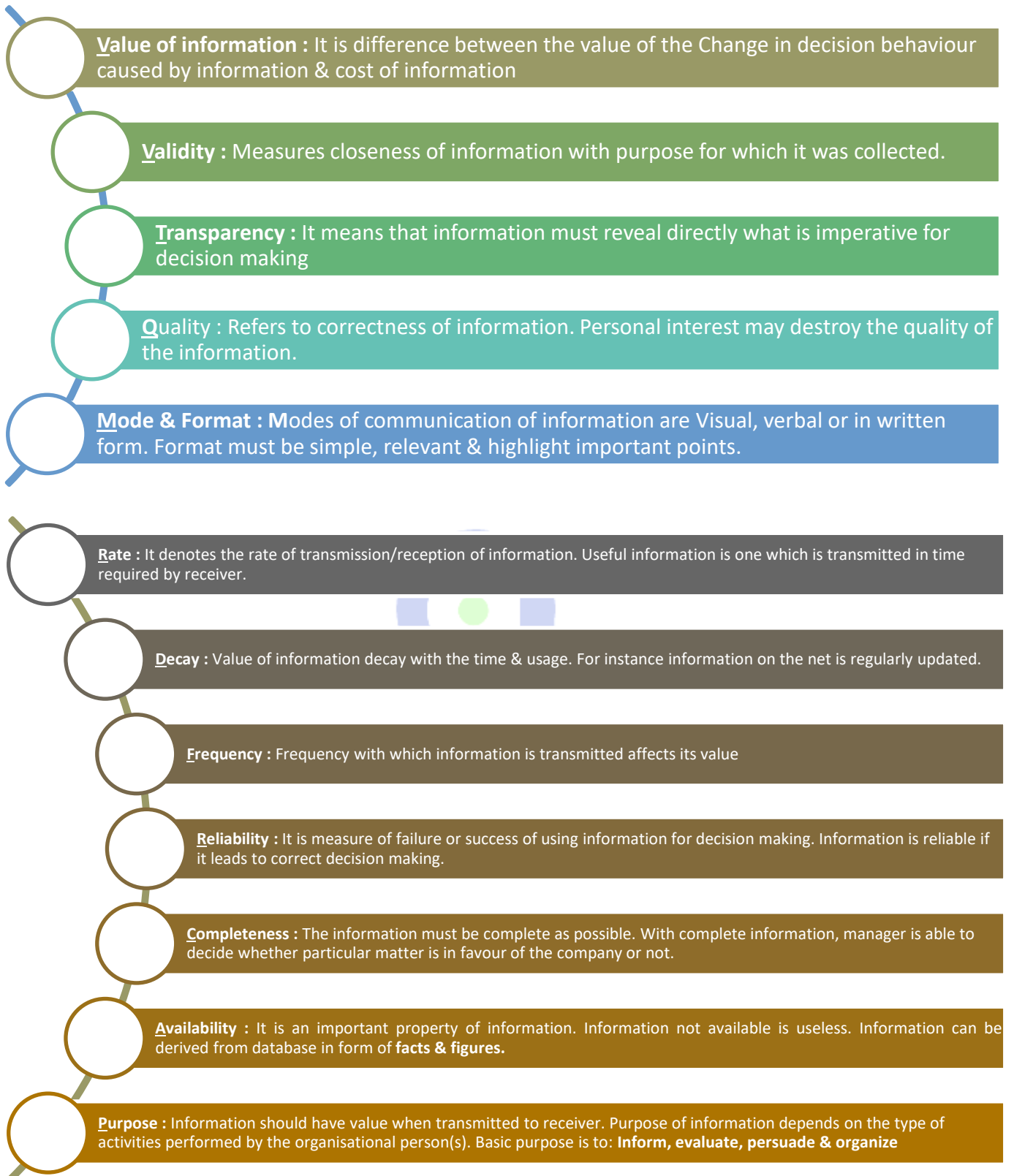


2.5 Specialized System:

 <p>Expert systems are software systems that imitate the reasoning process of the human experts. A characteristic of expert system is the ability to declare or explain the reasoning process. Expert system explains the reasoning process that was used to take the decision.</p>	<p>Expert systems are software systems that imitate the reasoning process of the human experts. A characteristic of expert system is the ability to declare or explain the reasoning process. Expert system explains the reasoning process that was used to take the decision.</p>
<p>Benefits of Expert System CODE TO REMEMBER: F.R.I.E.S</p>	<p>Free from fatigue: Expert systems are not subject to fatigue, emotional or busy. Real life expert: Expert system put information in active form so that it just likes analysis by a real life expert solving the problems. Information preservation: Expert systems preserve knowledge that might be lost because of any unwanted happening. Expert touch: Expert systems assist novices (New to the field) in thinking the way as experts do. Strategic Tool: Expert system is an effective strategic tool in areas of cutting cost, improving products & marketing products.</p>
<p>Qualities of Expert System CODE TO REMEMBER: C.E. – S.A.D.</p>	<p>Complexity: Expert system requires logical inference processing, which may not be handled by conventional (traditional) processing systems. Expertise: Solution to a problem requires efforts of the experts i.e. only few people possess that knowledge to solve the problem. Structure: The system must be capable to cope with ILL-STRUCTURED, uncertain, missing & conflicting data. Availability: One or more experts are capable of communicating how they are solving the problem to which the expert system will be applied. Domain: The domain/subject area of the problem is relatively small & limited to a relatively well defined problem area.</p>
 <p>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.</p>	<p>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.</p> <p>Components of ERP: Software component, process flow, customer mindset and change management.</p>
<p>Benefits of ERP CODE TO REMEMBER: U. – S.C.R.A.P.</p>	<p>Uniform process establishment: Establish uniform processes that are based on recognized best business practices. Faster Collection of Receivables: Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors. Satisfaction Improvement: Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times. Reduce Costs: Reduced inventory costs resulting from better planning, tracking and forecasting of requirements. Redundant Data Reduction: Reduce redundant data entry and processes and in other hand it shares information across the department. Actual Cost Tracking: Track actual costs of activities and perform activity based costing. Streamlining Processes: Streamlining processes and workflows with a single integ system.</p>
<p>Core Banking System</p>	<p>Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices. Normal core banking functions will include transaction accounts, loans, mortgages and payments. Banks make these services available across multiple channels like ATMs, Internet banking, and branches. Most commonly, Core Banking System (CBS) may be defined as a back-end system that processes daily banking transactions, and posts updates to accounts and other financial records.</p>

2.6 Attributes of Information:

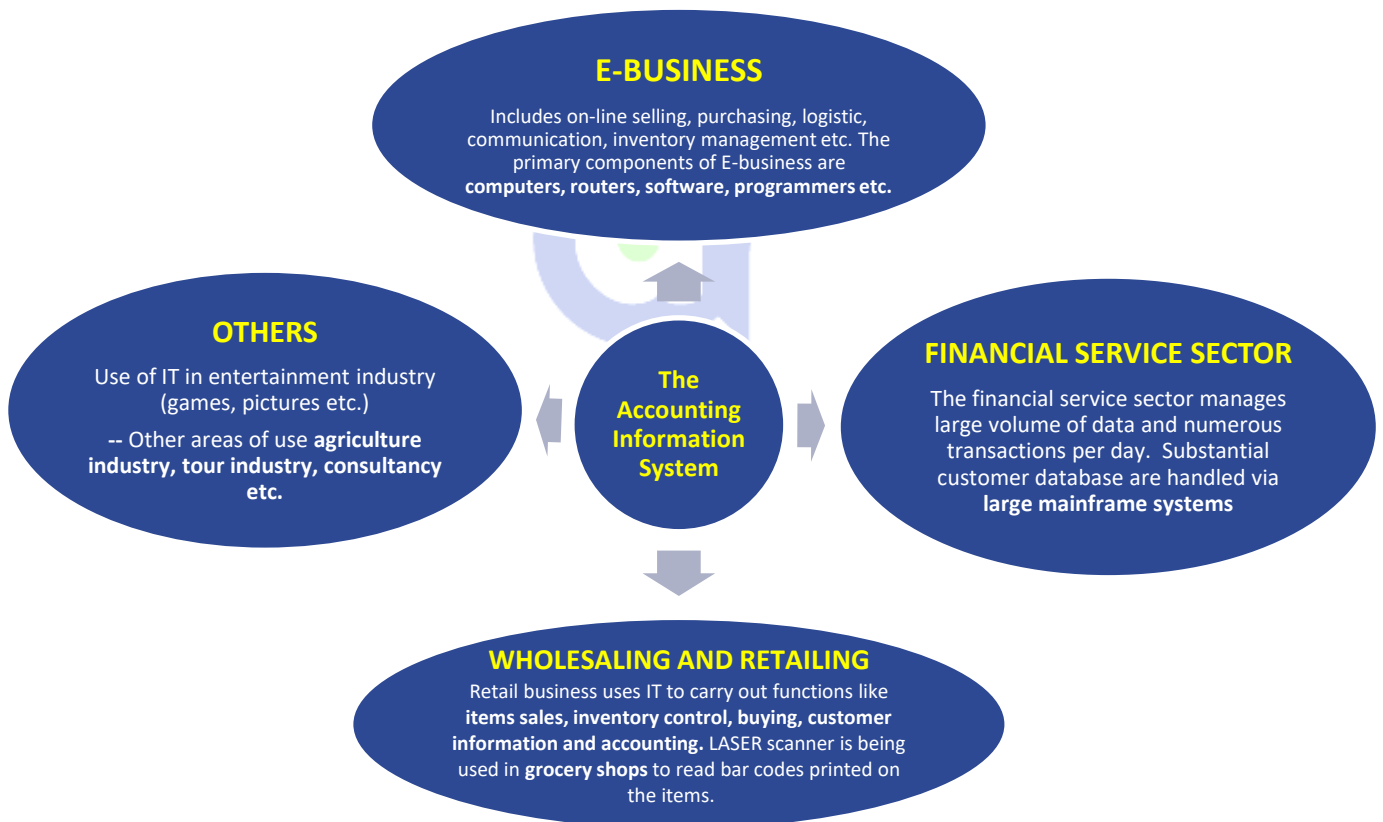
We ($\sqrt{2}$) - done TQM & RD (TQM & R&D kari) - FR(For) - CAP



2.7 Role of Information in Business:



2.8 The accounting Information System:



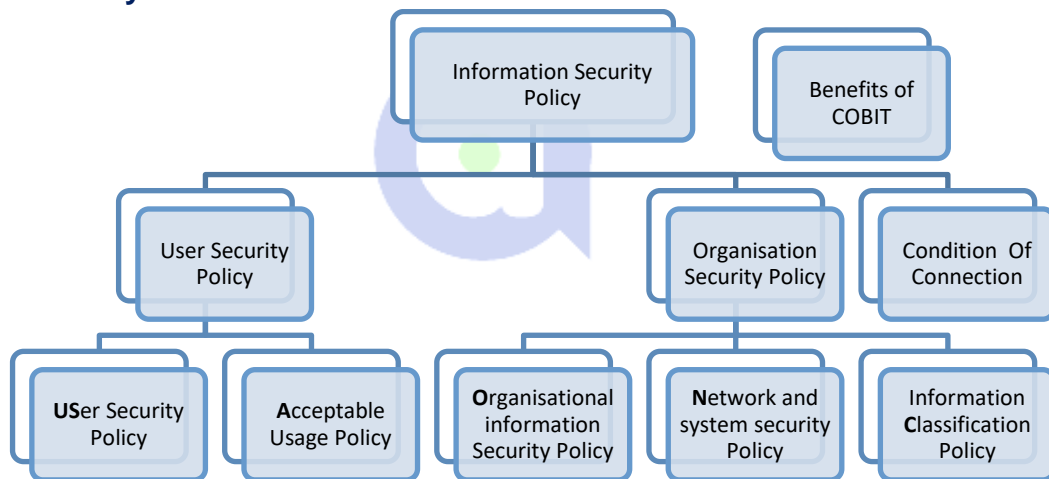
3.1 Need for protection of Information System:

CODE TO REMEMBER: E² – D.I.E.T.



1. **E**limination Of distance, time and space as constraints.
2. **E**lectronic attacks.
3. **D**evolution of management and control
4. **I**nterconnectivity of systems.
5. **E**xternal factors such as **legislature, legal and regulatory requirements or technological development.**
6. **T**echnology usage is worldwide.

3.2 Information Security Policies:



Information Security Policy CODE TO REMEMBER: U.S.A. - O.N. - C

USER SECURITY POLICY

U**S**er Security Policy: This set out the responsibilities & requirements from information security.

Accceptable Usage policy: This policy defines rules for use of email and internet services.

CONDITION OF CONNECTION

ORGANISATION SECURITY POLICY

Organizational Information security policy: Defines group of policies for security of information assets and IT systems.

Network and system security policy: This policy defines rules for network & data communication security.

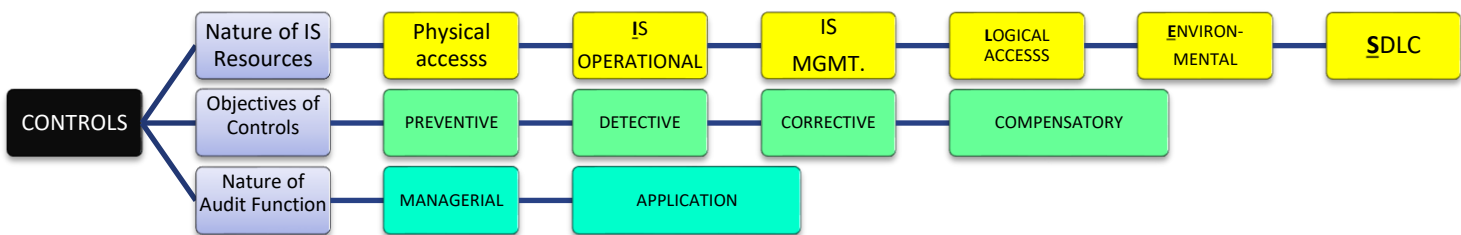
Information Classification Policy: This policy defines rules for classification of information.

3.3 Classifications of Controls:

Classification of Information system control Systems

Objectives of Controls (Based on the time they act)	Nature of IS resources (Based on source it implemented)	Audit Functions (On Auditor's perspective)
<p>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.</p> <p>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.</p> <p>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.</p>	<p>Environmental Controls: These are the controls relating to IT environment such as power, air-conditioning, Uninterrupted Power Supply (UPS), smoke detection etc.</p> <p>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, etc.</p> <p>Logical Access Controls: These are the controls relating to logical access to information resources. 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.</p>	<p>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.</p> <p>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.</p>

3.4 Categories of Controls:



Description of controls:

Environmental Controls	Information System resources	Hardware and media, IS Support infrastructure, documentation, supplies, people.
	Environmental Issues and exposures + Counter Measures	Fire Damage – Smoke detector, Fire Extinguisher. Electrical Shock - Electrical Surge Protector. Equip. Failure - Wiring Placed in Electric Panels.

Physical Access Controls	Physical Access Issues & Exposures Code to Remember: U.B.I. - M.A.D.E	Result due to intentional violation of access path: <u>U</u> nauthenticated entry <u>B</u> lackmail <u>I</u> nformation disclosure publicly. <u>M</u> odification of semester equipment & information. <u>A</u> buse of data processing resources. <u>D</u> amage or theft of documents or equipment <u>E</u> mbezzlement.
	Physical Access Controls	Locks on doors – Cipher Lock, Bolting door. Physical Identification medium Logging on Utilities. Other Means – Cameras, Alarms, Fencing etc
Logical Access Controls	Meaning	It is also known as electronic or technological controls. It restricts the access of resources through programs, applications and network channels to authorized users only
	Type of Exposures	Technical Exposures → Data diddling, bombs, Trojan Horse, worms, rounding down, salami technique, trap doors. Computer Crime Exposures → Financial loss, legal repercussion, loss of credibility, blackmail, information disclosure, sabotage, spoofing. Asynchronous Attacks → Data leakage, wire-tapping, piggybacking, computer shut down.
Managerial Controls	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 exercised 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	Boundary Password, Cryptography, PIN, identification Cards Input Source document controls, data coding control & Validation controls.	Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. 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.

	<p>Communication Controls ensuring no data loss, no transmission impairment</p>	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.
	<p>Processing Processor, Real Memory & Virtual Memory controls</p>	Responsible for computing, sorting, classifying and summarizing data.
	<p>Output Printed data report, word document, CD or Floppy.</p>	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.
	<p>Database</p>	Responsible to provide functions to define, create, modify, delete and read data in an information system
Data Resource Management Control	Activities involved in maintaining integrity of database	Definition control, Existence/backup Controls, Access Controls, Update Controls, Concurrency Controls and Quality Controls.



Information Technology General Controls (ITGC)

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.



Financial Controls

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, nonmonetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of applications to general ledger.



Personal Computer Controls

Most common PC Controls:

- (a) Physically locking system;
- (b) Proper logging of equipment shifting must be done.
- (c) Centralized purchase of hardware/ software;
- (d) Standards set for developing, testing and documenting;
- (e) Uses of anti-malware software;
- (f) Use of PC and their peripheral must have controls; and;
- (g) 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.

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.

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, unauthorized 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.

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.

4.1 Introduction:

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

4.2 Advantage of business continuity:

- (a) Proactively assess the risks or threat scenario (खतरों की scenario का आकलन).
- (b) Enterprise has planned response to disruptions which may cause the damage and minimize the impact of the damages. (Business खतरों के लिए तैयार है by using planned response).
- (c) Enterprise is able to demonstrate a response through process of regular testing and trainings.



4.3 Business Continuity plan:

OBJECTIVES & GOALS

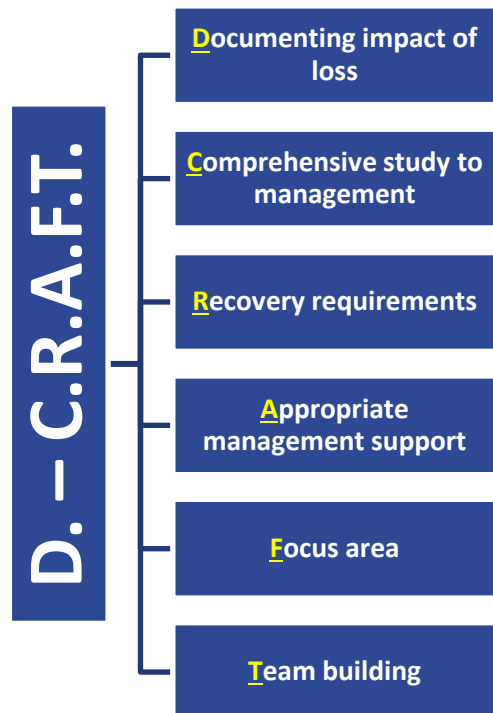
OBJECTIVES:

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

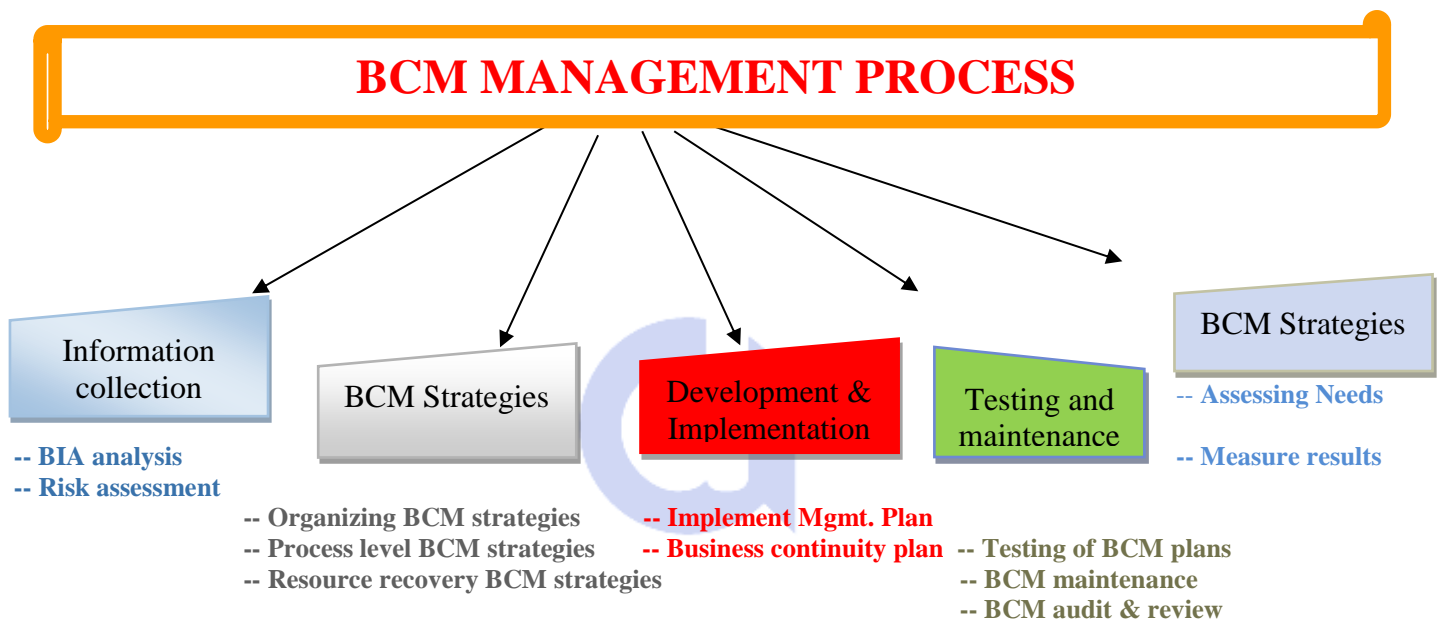
Identify weaknesses and implement a disaster prevention program;
 Minimize the duration of a serious disruption to business operations;
 Facilitate effective co-ordination of recovery tasks; and
 Reduce the complexity of the recovery effort.

DEVELOPING A BUSINESS CONTINUITY PLAN



8 P H A S E S	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 5: Plan Development: During this phase, recovery plans components are defined and plans are documented.
	Phase 2: Vulnerability Assessment and General Definition of Requirements: This phase addresses measures to reduce probability of occurrence of disaster.	Phase 6: Testing/Exercising Program: Testing/ exercising goals are established and alternative testing strategies are evaluated.

O F D E V E L O P M E N T	<p>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”.</p> <p>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.</p>	<p>Phase 7: Maintenance Program: It is critical that existing change management processes are revised to take recovery plan maintenance into account.</p> <p>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.</p>
--	--	---

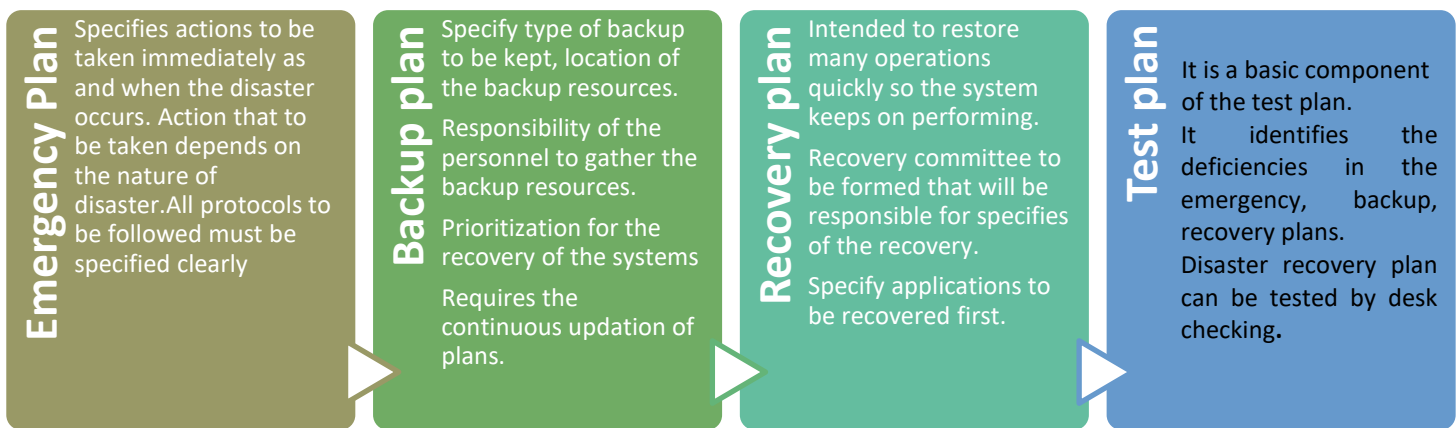


BUSINESS CONTINUITY MANAGEMENT PROCESS	<p>Organizational structure: The organisation must nominate a person or team with appropriate seniority and authority to be accountable for BCM policy implementation and maintenance. It should clearly define the person responsible for the business continuity within the enterprise and responsibilities.</p> <p>Implementing Business Continuity in The Enterprise and Maintenance: In establishing and implementing the BCM system, managers from each function on the site represent their areas of the operations. They are wholly responsible for the on-going operation and maintenance of the system. Top management must appoint manager (BCM) who will be responsible for the policy implementation and maintenance. The policy must be communicated to all stakeholders with appropriate training.</p> <p>BCM Documentation and Records: All documents are subject to document control and record control processes. The following documents are being classified as part of business continuity management system:</p> <p>Policy includes→</p> <ol style="list-style-type: none"> 1. The business continuity plans. 2. The business continuity management system 3. Business continuity strategies. 4. The business continuity policy.
---	--

<p>CLASSIFICATION OF CRITICAL ACTIVITIES</p>	<p>Business Categorization: In deciding whether a function is vital/essential/desirable, following parameters are considered – Loss of revenue, loss of reputation, decrease in customer satisfaction and loss of productivity.</p> <p>Disaster Scenario: This includes nature of disaster (major, minor, trivial and catastrophic). Business impact matrix is used for assessing the risk and as such referred to be risk assessment matrix. Below is the graphical representation of this matrix:</p> <div data-bbox="384 456 1225 1205" data-label="Diagram"> <pre> graph TD L["LIKELIHOOD (The Probability of a risk or the occurrence of the disaster)"] C["CONSEQUENCES (The severity of the impact or extent of damage caused by the risk)"] L --- L1["Definite(Scaled 3) A risk that is almost certain during project execution."] L --- L2["Likely (Scaled 2) A risk that has 60-80% chances of occurrence."] L --- L3["Unlikely (Scaled 1) A risk that has less than 10% chances of occurrence."] C --- C1["Insignificant (Scaled 1) Risk that cause negligible amount of damage"] C --- C2["Minor (Scaled 2) Risk that may result in some damage not significant."] C --- C3["Major (Scaled 3) Risk with significant large impact which can lead to great amount of loss."] C --- C4["Catastrophic (Scaled 4) Risks that can make whole project unproductive ."] L --- C </pre> </div>
<p>BCM STRATEGY PROCESS</p>	<p>“A war broke out between two nations. Both the nations’ armed forces will try to protect his nation from the invasion of enemy. As such the heads of the armed forces will make strategy to cope up with the invasion in order to protect the nation” Now replacing the words: NATION protect करना है : Critical functions of the enterprises. ARMED FORCES : Enterprise. STRATEGY : Strategy of enterprise. <i>(जैसे सेना दुश्मन से राष्ट्र की रक्षा करता है similarly व्यापार के कार्यों की रक्षा के लिए strategy is necessary by enterprise)</i> There is need for implementing the strategies for protecting critical functions (nation) by the enterprise (Armed forces). For example, establish the procedures for backing up files and applications. Establish contracts and agreements to protect the critical functions.</p>
<p>BCM DEVELOPMENT AND IMPLEMENTATION PROCESS</p>	<p>An enterprise should have an incident management team, crisis management team for an effective response and recovery from the disruption. Some of BCP Plans:</p> <ul style="list-style-type: none"> • Incident Management Plan To manage the initial phase of an incident, the crisis is handled by IMP. IMP should have top management support with appropriate budget for development & maintenance. Features of a good IMP: -- They should be flexible, feasible and relevant. -- It must be easy to read and understand. -- It must provide basis for managing all possible issues including shareholder issues etc. • Business Continuity Plan: To recover or maintain the activities in the event of the disruption to a normal operation.

<p>BCM TESTING AND MAINTENANCE PROCESS</p>	<p>BCM Testing</p> <p>Code to Remember: R.I.C.E.D</p>	<p>A BCP has to be tested for any flaws that may be inherited in the planning and implementation phase. Responsibility for keeping the BCP updated has to be clearly defined in the BCP plans. BCM testing must be within the scope of BCP plans. The testing includes testing of technical, logistical, procedural, and other operational system, BCM arrangements and infrastructure, technology and telecommunication recovery, relocating of staff etc. It also improves BCP capability by:</p> <ol style="list-style-type: none"> Practicing Recovery ability of the enterprise. Identification of all critical activities and their dependencies and priorities of the enterprise and ensure that BCP incorporated all. Confidence building among the exercise participants. Effectiveness and timeliness of restoration activities is being validated. Demonstrating competence of the primary response team and their alternatives.
	<p>BCM Maintenance</p>	<p>The BCM maintenance process demonstrates the documented evidences of management and governance of enterprise's business continuity program. It is important to keep documentation up-to date. This includes contract, agreements etc. If additional is being introduced, that must be maintained and periodically replaced. Following activities are undertaken in the maintenance phase:</p> <ol style="list-style-type: none"> Determine ownership and responsibilities for maintaining BCP strategies. Determine the maintenance process to update plan. Determine the maintenance regime to ensure plans remain up-dated. Ensure that any structural, organizational, operational changes are communicated to those who are accountable for updating the plans.
<p>BCM TRAINING PROCESS</p>	<p>Code to Remember: E.C.L.A.I.R.</p>	<p>While developing BCM, competencies required for personnel assigned specific management responsibilities within the system have been determined. Some of the competencies that company require:</p> <ol style="list-style-type: none"> Encourage to take calculated risks. Culture of positivity is created and promoted. Listen to other, their ideas, views and opinions. Acknowledges contribution by the colleagues. Integrity. Resolve problems by involving team member.

4.4 Business Continuity plan:



4.5 Backup plan:

Type of Back up	Meaning	Advantage	Disadvantage
Full Backup	<ol style="list-style-type: none"> 1. Captures all files on the disk. 2. Every back up generated files contains all the data. 3. But it involves good amount of money & time in taking backup 	<ol style="list-style-type: none"> 1. Restores are fast and easy to manage. 2. Easy to maintain & Restore different versions. 	<ol style="list-style-type: none"> 1. Backup can take long time to complete. 2. Consumes most storage spaces.
Mirror Backup	<ol style="list-style-type: none"> 1. It is identical to full backup. 2. Here files are not compressed in zip files & not password protected. 3. Most frequently used for taking backup. 	<ol style="list-style-type: none"> 1. Backup is clean and don't contain old files 	<ol style="list-style-type: none"> 1. Source File may be deleted accidentally.
Incremental Backup	<ol style="list-style-type: none"> 1. Captures files that were created/ changed since last back up. 2. This is the most economical method 3. Incremental backups are difficult to restore. 	<ol style="list-style-type: none"> 1. Faster backup. 2. Efficient use of space as all files doesn't get duplicated. 	<ol style="list-style-type: none"> 1. Restores are slower and complicated.
Differential Backup	<ol style="list-style-type: none"> 1. Stores files that have changed since last full backup. 2. So if a file is changed after full back up, differential backup is taken. 	<ol style="list-style-type: none"> 1. Faster backup than full backup. 2. Efficient use of space since files changed till last time will be copied. 3. Faster restore as compared to incremental backup. 	<ol style="list-style-type: none"> 1. Restores are slower and complicated. 2. Backup slower than that of incremental backup.

4.6 Disaster Recovery Procedure Plan:

Disaster Recovery Procedure Plan			
<u>M</u> AINTEENANCE PLANS	<u>E</u> MERGENCY PROCEDURES	<u>P</u> ERSONNEL	<u>F</u> ACILTIES
<ol style="list-style-type: none"> 1. Maintenance schedule, specifying how & when plan to be tested. 2. Conditions for activating plans, which describe the process to be followed before each plan is activated. 	<ol style="list-style-type: none"> 1. Emergency procedures to be taken following an incident which may affect business operations & human life. 2. Resumption procedures that describe the action to be taken to get back to normal business operations. 3. Contingency plans will document list & its testing recovery procedures. 	<ol style="list-style-type: none"> 1. Awareness & educational facilities to provide an understanding about the organization. 2. Responsibilities of individuals to execute the components of plan. 3. List of phone number of all employees. 4. Name of employees trained for the emergency situation 5. List of vendors doing business with the organization. 	<ol style="list-style-type: none"> 1. Details of airlines, hotels & transport agreements. 2. Location of data & program files, data dictionary. 3. Insurance papers & claim forms. 4. Medical procedures to be followed in case of injury.

5.1 Introduction:

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.

5.2 Reasons of failure to achieve systems development objectives:

<p>Reason for Failure</p> <p>Code to Remember: T. - M.U.D.</p>	<p>Reasons that most of the organization fails to achieve their systems development objectives are:</p> <p>Technological related issues Management related issues User related issues Developer related issues</p>
--	---

5.3 System Development Methodology:

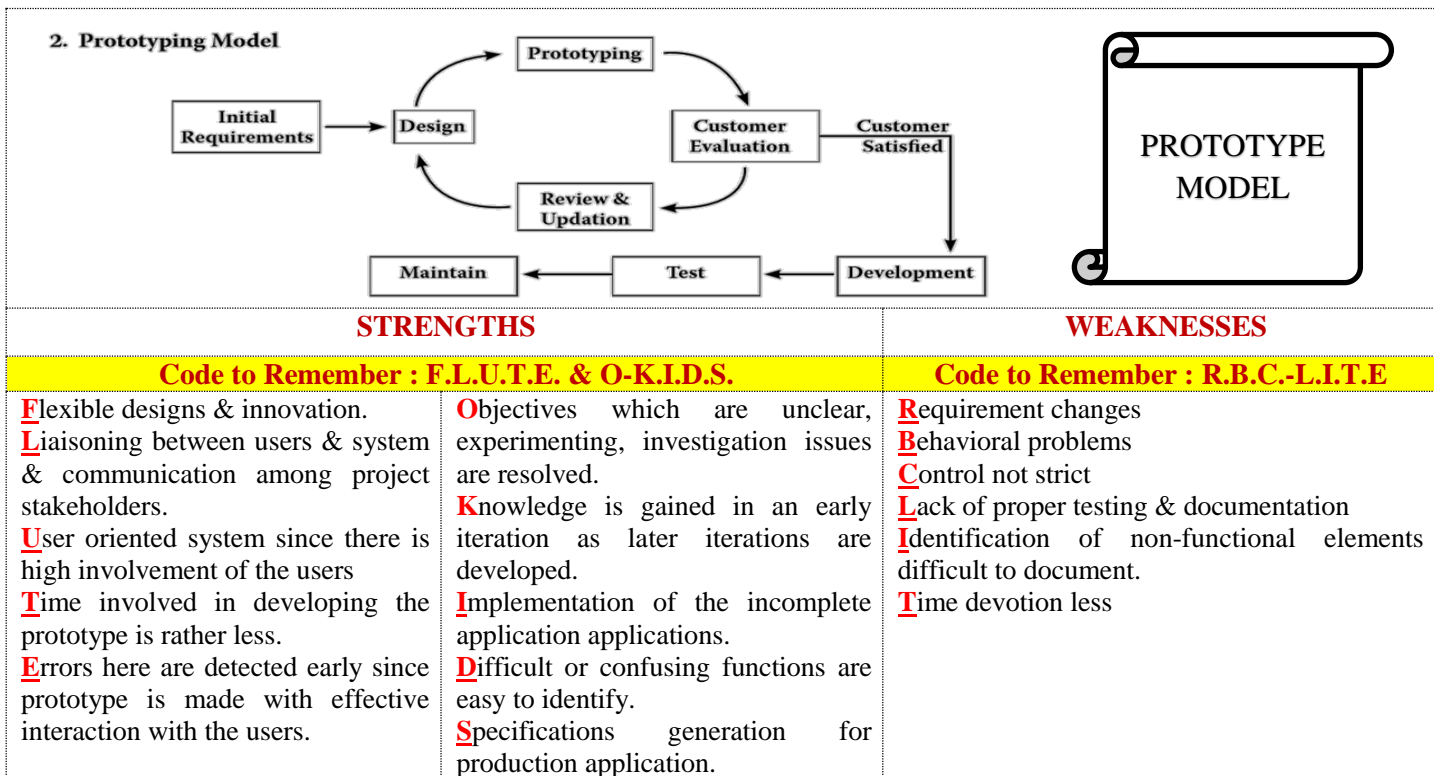
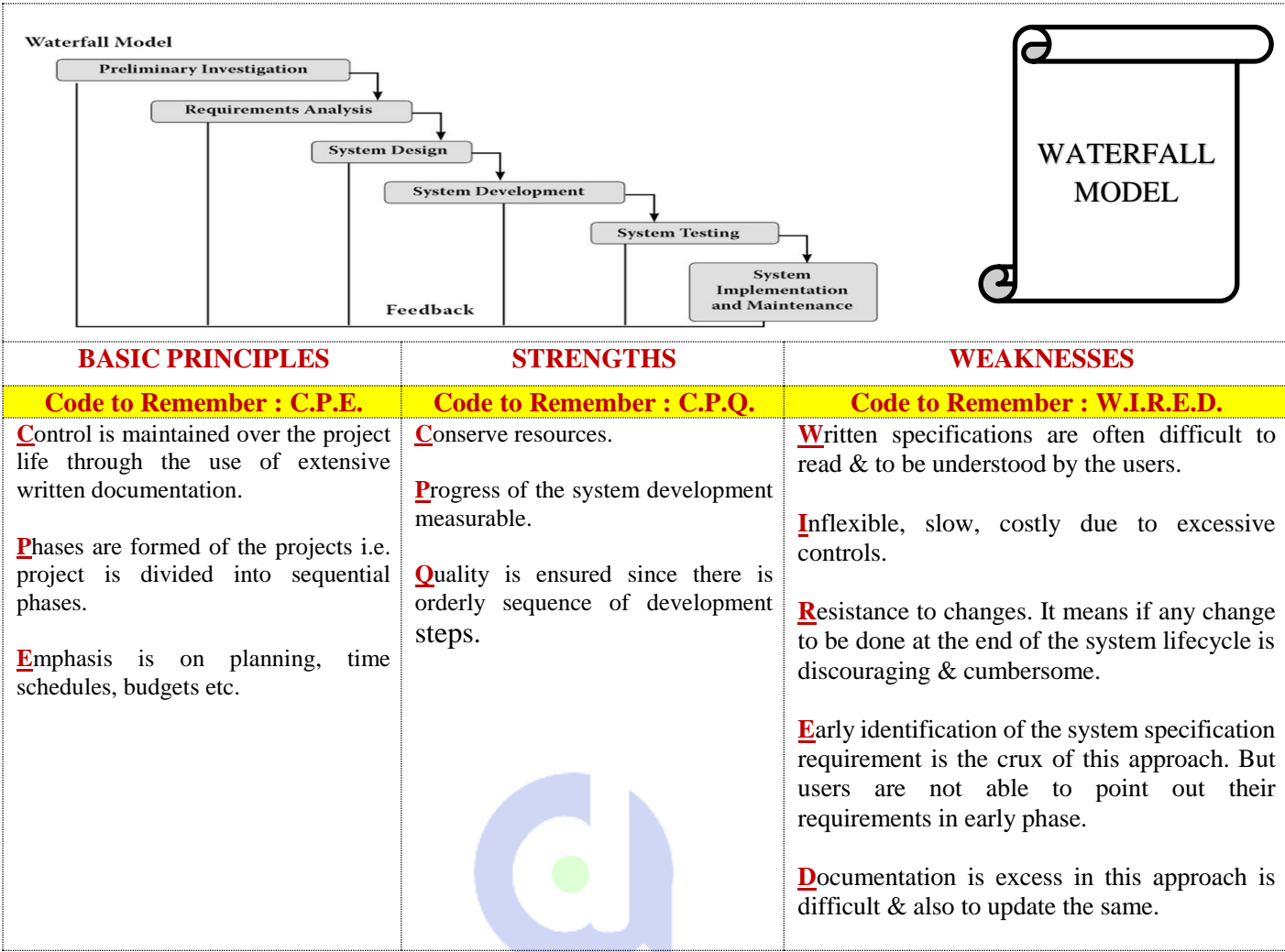
It is a formularized, standardized, documented set of activities used to manage a system development project. The methodology is characterized by the following:

1. Project is divided in to a number of identifiable processes & each has a starting & ending point.
2. Specific reports & other documentation must be produced periodically to make development personnel accountable.
3. Users including auditor, managers are required to participate in the project.
4. The system must be tested thoroughly prior to implementation.
5. Training plan for those who will operate & use the system.
6. Post implementation review of all developed systems.

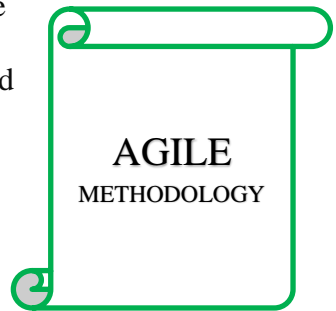
Characteristics	Description
Process	Project divided into number of identifiable processes, with each process having a starting point and an ending point; comprises several activities; one or more deliverables, and several management control points.
Deliverables	The specific reports and other documentation 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.

5.4 Approaches to system development:

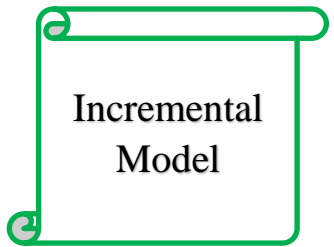
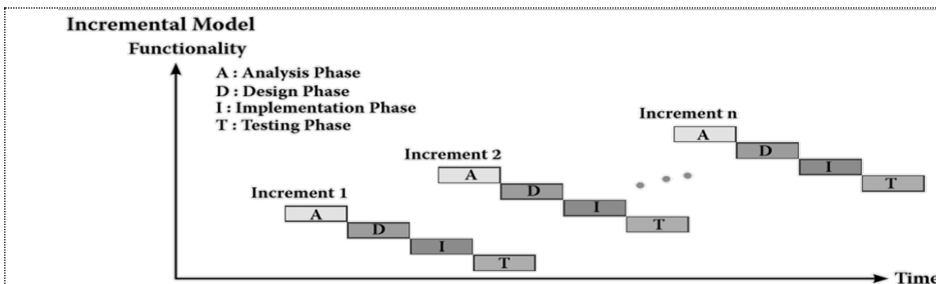
<p>Code to Remember</p> <p>W – P.A.I.R.S.</p>	<p>Waterfall: Linear Framework type Prototyping: Iterative framework type. Agile methodologies Icremental: Combination of linear & iterative type. Rapid Application Development: Iterative framework type. Spiral: Combination linear & iterative framework Type.</p>
--	---



AGILE MODELLING is a methodology for modeling 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.



BASIC PRINCIPLES	STRENGTHS	WEAKNESSES
<p>Code to Remember : D.O.S.-C.A.S.E.</p>	<p>Code to Remember: Q-C.A.D.</p>	<p>Code to Remember : V.A.R.I.E.D.</p>
<p>Development: Development is maintained at a constant pace. Organized Team: One of the major benefits of the agile methodologies is that it has self-organized team which can tackle all the problems. Simplicity: Cooperation: There is close & daily cooperation between business people & the developers. Adaptive to changes: Regular adaptive to changing circumstances. Satisfaction to customer: Customer satisfaction by rapid delivery of useful software. Excellence: There is continuous attention to the technical excellence & good design.</p>	<p>Quality software: One of the benefits of this methodology is the delivery of high quality software in least possible time & satisfied customer. Communication is effective: Face to Face communication & continuous inputs from the users leaves no probability of any work based on any guesses. Adaptive team: Agile methodology has the concept of the adaptive team, which responds quickly to the changing requirements. Documentation: Here the document is crisp(less) & to the point hence saving time.</p>	<p>Verbal communication: Under agile methodology, more emphasis is on verbal communication with customer rather than documenting or preparing manuals. Accessing incapability: In case of software which is rather large in size, it is difficult to access the efforts required in the beginning of software development life cycle. Rework required: Agile require rework. Because of lack of long term planning, rework is often required to integrate the agile project with other components of the software. Integration difficulty Experienced programmers Designing & documentation</p>



STRENGTHS	WEAKNESSES
<p>code to Remember: D.M.-KFC</p>	<p>Code to Remember : O – R.A.W.</p>
<p>Delivery of system: One of the benefits of this methodology is the delivery of system to its customer as and when the component of the system is ready. Monitoring the changes: Gradual implementation of the components of the system Knowledge: Potential exists for the exploitation or using the knowledge gained in early incremental phases as later incremental phases are developed. Flexibility: This type of models are indeed flexible & less costly if requirement or scope changes. Control Maintained: Moderate control is maintained over the project life by having proper & written documentation. It's just like blue print of project on which basis project deviation, if any, is measured & controlled.</p>	<p>Overall consideration lacks: There is usually lack of consideration of the business problems & technical requirements when the concentration is on the smaller parts/components of the system Rigid: Each phase of an iteration is rigid & do not overlap each other. Architectural issues: Problems may arise relating to architectural since at the time of developing the system not all requirements are known. Well defined interface required.</p>

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.



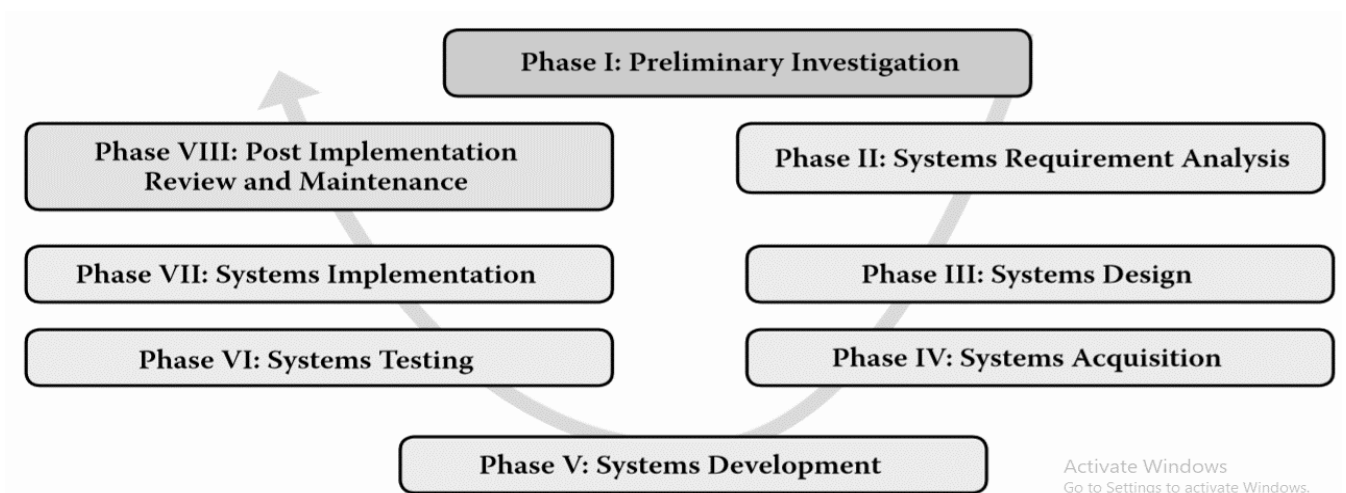
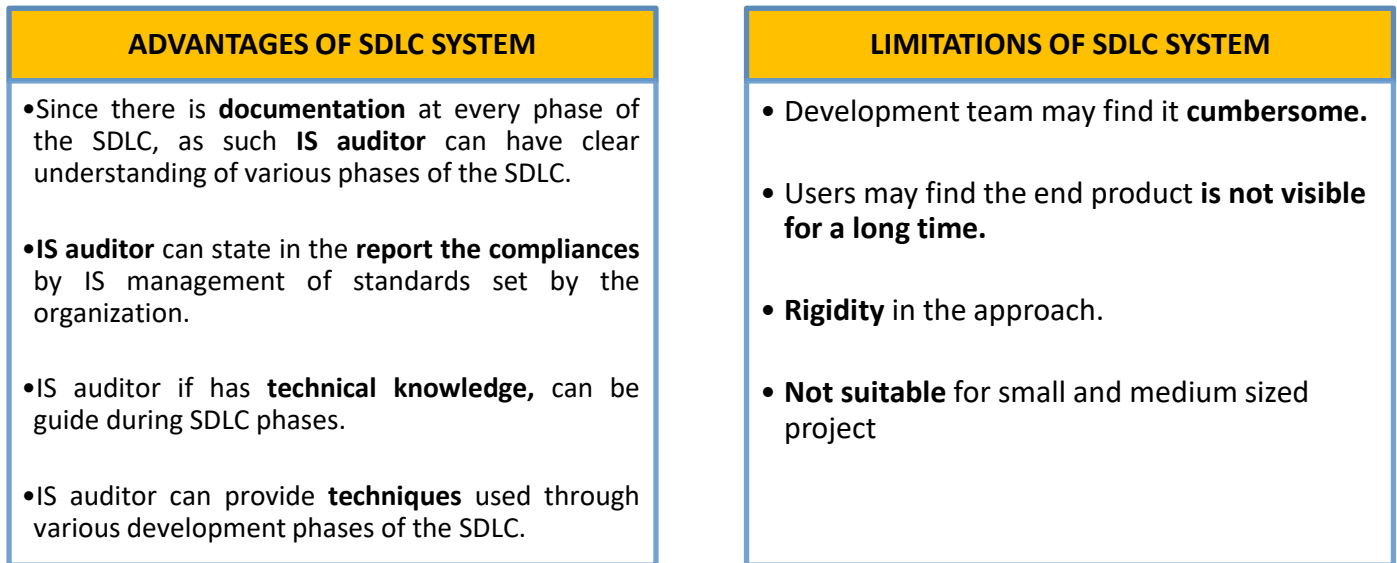
BASIC PRINCIPLES	STRENGTHS	WEAKNESSES
Code to Remember : F.U.N.- Q. - D.R.P.	Code to Remember: O.H. - I.C. - S.R.S	Code to Remember : Q. -M.R. - VRD
<p>Fast development of system: Since we have already discussed that the element of planning is minimal, as such this approach is able to produce the high quality system in a quick time at a very low investment cost.</p> <p>User involvement: Active user involvement is imperative.</p> <p>Needs of business: In this approach key emphasis is on the business needs rather than on the technical or engineering issues.</p> <p>Quality system: Aims to produce quality system quickly, through the use of iterative prototyping & various development tools i.e. DBMS, Graphical user interface, Codes etc.</p> <p>Documentation: Produces necessary documentation to facilitate future development & maintenance.</p> <p>Risk reduces: Aims to reduce inherent project risk by breaking the project into smaller segments.</p> <p>Prioritization criteria: Project control involves prioritizing development & defining deadlines for the projects undertaken.</p>	<p>Operational version of application: Under the RAD approach, operational version of an application is available much faster & earlier than other approaches.</p> <p>Initial review possible: Quick initial reviews are possible.</p> <p>Cost: RAD produces system more quickly, as such this approach tends to produce systems at low cost.</p> <p>Stakeholder involvement: Since the user's involvement is much more under this approach, as such there is indeed great level of commitment & involvement.</p> <p>Rapid changes possible: Provides the ability to rapidly changes the system design as required by users</p> <p>Saving: RAD helps in saving time, money and human efforts.</p>	<p>Quality compromise: More speed & lower cost may lead to lower overall system quality.</p> <p>Misalignment: Since system is developed in a quick time as such it might be possible that sufficient information is not there with the developers. As such there may be possibility that developed system may get MISALIGNED.</p> <p>Reuse difficulty: Modules which are constructed in a quick time lack usability in future years.</p> <p>Violation of standards: There may be chances where violation of programming standards is there. It involves inconsistent documentation etc.</p> <p>Requirement issues: Since in RAD it is possible to incorporate changes rapidly as required by users, as such it might be possible that project may end with high requirements than needed.</p> <p>Design inconsistency: Potential for design inconsistency within and across the system</p>

SPIRAL MODEL

STRENGTHS	WEAKNESSES
Code to Remember: R.B.I	Code to Remember : L.E.T.S-C
<p>Risk avoidance: Enhance risk avoidance.</p> <p>Best Methodology selecting tool: Useful in selecting the best methodology to follow for development of given software</p> <p>Incorporation of other methodologies: Can incorporate waterfall, prototype & incremental methodologies. It provides guidance in knowing the best combination of the system models & software.</p>	<p>Limiting reusability: Such model is highly customized to project. Thus it is complex & limits reusability.</p> <p>Exact composition not measurable: It is difficult to determine the exact composition of development methodologies to use for each cycle.</p> <p>Termination point absence: There is no clear termination point or deadline between the cycles.</p> <p>Skilled manager required: How to apply this model in a given practical business situation.</p> <p>Control absence: lack of established control.</p>

5.5 System development Life Cycle:

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.

<p>Code to Remember:</p> <p>P.O.S.-F.M.</p>	<p>Problem Identification.</p> <p>Object Identification.</p> <p>Scope Delineation.</p> <p>Feasibility Study</p> <p>Management Reporting.</p>
--	---

P.O.S	Feasibility Study	Management Reporting
<p>1. Identification of Problem: Define the problem clearly and precisely. The analyst working on the preliminary investigation accomplish the following objectives- Understanding Project request. Size of the project is determined. Feasibility study made. Cost & benefit analysis. Acquaintance with mgmt.</p> <p>2. Identification of Objectives: Work out and precisely specify the objectives of the proposed solution. For instance, more time involved in doing reservation in railway, as such the objective “To introduce a system whereby passengers could buy the ticket online faster & in real time”</p> <p>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’.</p>	<p style="text-align: center;">Code to Remember B.E.S.T. - F.L.O.R.</p> <p>Behavioral Feasibility: This refers to the systems, which is to be designed to process data and produce the desired outputs.</p> <p>Economic Feasibility: This includes an evaluation of incremental cost and benefit expected if the proposed system is implemented.</p> <p>Schedule or Time Feasibility: This marks an estimation of time it will take a new system to become operational.</p> <p>Technical Feasibility: It answers whether implementation of the project is viable using current technology.</p> <p>Financial Feasibility: This checks for whether the proposed solution may be costly for the user organization.</p> <p>Legal: Is the solution valid in legal terms?</p> <p>Operational Feasibility: This is concerned with finding view of workers, employees, customers and suppliers about the use of new system.</p> <p>Resources Feasibility: Implementation of sophisticated software solutions becomes difficult at specific locations because of the reluctance of skilled personnel to move to such locations.</p>	<p>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.</p> <p>Internal Control Aspects Management implements proper internal audit team to ensure</p>

Phase II: Preliminary Investigation →

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.

Code to Remember T—C.P.S. (The Connaught Place’s)

The Fact Finding	Current system Analysis	Proposed system Analysis	System Development Tools
D.O. - .I.Q.	H.I.D.-M-O.I.M.A.		C.A.P
Every system is built to meet some set of needs. To assess these needs - Documents, Observation, Interviews Questionnaires, are some fact-finding tools.	This step involves: H istorical aspect review I nput analysis D ata files maintained reviewed M ethod, procedure & data communication review. O utput analysis I nternal control review M odel the existing & logical system. A nalysis of overall present system	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: C onceptualize, clarify, document & communicate the activities; A nalysis present operations; P ropose new improved design: Example: Structured English, Flowcharts, Data Flow Diagrams, Decision Tree, 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.
Data Design	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	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.

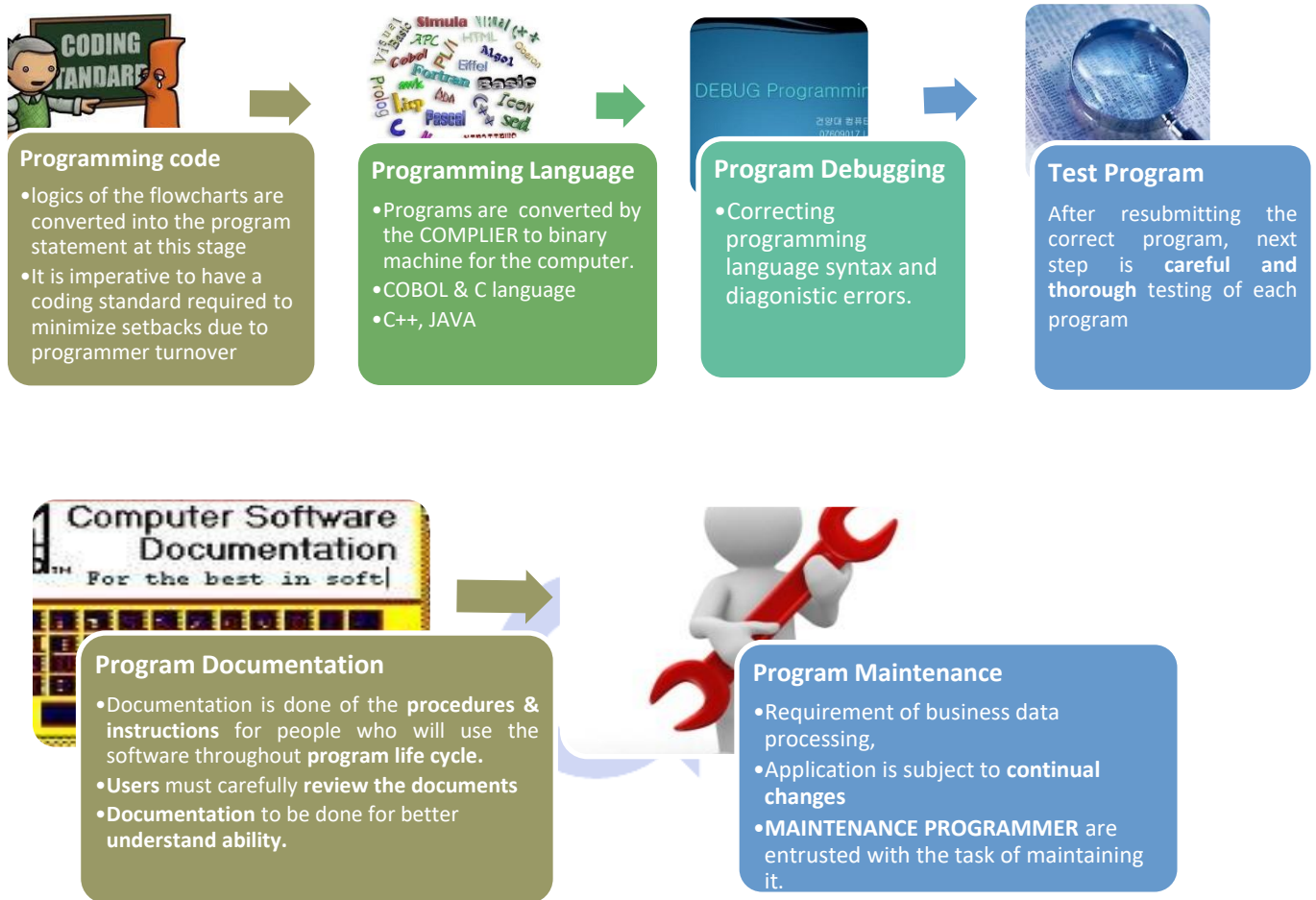
Phase IV: Systems Acquisition:

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 Standard	Acquisition Systems 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. Consideration in case of acquisition of both hardware and software: Vendor selection Geographical location of the vendor Presentation by the selected vendor Evaluation of user's feedback	Includes several other acquisition aspects and practices also like – H/w Acquisition; S/w Acquisition; Contracts, S/w Licenses and Copyright Violations, <u>Validation of Vendors' proposals V.M.B.-P.C.</u> Vendor support. Maintenance cost of each proposal. Cost & Benefit analysis of each proposed. Performance capabilities of each proposed system. <u>Methods of validating them. B.P. - C.P.T.</u> Bench marking problem Public evaluation report: Checklists Point-scoring analysis Test problems

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.



Phase VI: Systems Testing:

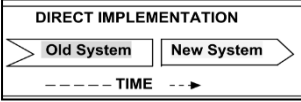
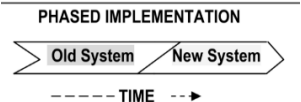
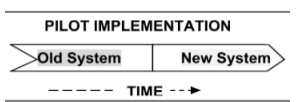

Testing is a process used to identify the correctness, completeness and quality of developed computer software. Different levels of Testing are as follows:

<p>SYSTEM TESTING</p>	<p>UNIT TESTING</p> <p>Code to Remember: F-S²P²</p>	<p>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. following are 5 categories of TEST:</p> <ol style="list-style-type: none"> Functional tests: It checks “whether program do what they are supposed to do”. Structural tests: These tests are concerned with examining the internal processing logic of the software system. Stress Test: Testing that is used to determine the stability of a given system. Parallel tests: These tests are designed to OVERLOAD a program in various ways in order to test the limitations of the system. Performance tests: It should be designed to verify the response time, execution time, the throughput, memory utilization etc.
------------------------------	---	---

INTERGATION TESTING	<p>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:</p> <p>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 subsystem testing, and then testing of the entire system.</p> <p>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.</p>				
REGRESSION TESTING	<p>Each time a new module is added as part of integration testing, the software changes. this may cause problems in the functioning of the previous system that run flawlessly. regression testing ensures that changes or corrections have not introduced new errors.</p>				
SYSTEM TESTING	<p>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:</p> <p>RECOVERY TESTING: This testing involves “How well the application is able to recover from CRASHES, HARDWARE FAILURES & other problems”.</p> <p>SECURITY TESTING: This is the process to determine that an INFORMATION SYSTEM protects the DATA and maintains functionality as required or not.</p> <p>PERFORMANCE TESTING: This testing is used to determine THE SPEED/EFFECTIVENESS OF A computer, network, software programs and devices.</p> <p>STRESS TESTING: This testing is used to determine the STABILITY of a given system or entity. It involves test beyond the NORMAL OPERATIONAL CAPACITY.</p>				
FINAL ACCEPTANCE TESTING	<p>When the system is just ready for implementation, final acceptance testing is done. here it is ensured that new system satisfies the quality standards adopted by the business & system satisfies the users. 2 major parts of final acceptance:</p> <p>Quality Assurance Testing: Ensures that new system satisfy the prescribed quality standard.</p> <p>User Acceptance Testing: Ensure that functional aspects expected by the users have been well addressed in the NEW SYSTEM. The following are the 2 types of user acceptance testing.</p> <table border="1" data-bbox="507 1588 1544 1912"> <thead> <tr> <th data-bbox="507 1588 1050 1659"><u>ALPHA TESTING</u></th> <th data-bbox="1050 1588 1544 1659"><u>BETA TESTING</u></th> </tr> </thead> <tbody> <tr> <td data-bbox="507 1659 1050 1912">This is performed by the user within organization by the developers to improve and ensure the functionalities as per user satisfaction.</td> <td data-bbox="1050 1659 1544 1912">This is second stage performed after deployment of the system. It is performed by the external users. This involves sending product outside for real world exposure and receive back feedback for analysis and modifications.</td> </tr> </tbody> </table>	<u>ALPHA TESTING</u>	<u>BETA TESTING</u>	This is performed by the user within organization by the developers to improve and ensure the functionalities as per user satisfaction.	This is second stage performed after deployment of the system. It is performed by the external users. This involves sending product outside for real world exposure and receive back feedback for analysis and modifications.
<u>ALPHA TESTING</u>	<u>BETA TESTING</u>				
This is performed by the user within organization by the developers to improve and ensure the functionalities as per user satisfaction.	This is second stage performed after deployment of the system. It is performed by the external users. This involves sending product outside for real world exposure and receive back feedback for analysis and modifications.				

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.		
	<u>Site Preparation</u>	Appropriate location must be found to provide an operating environment for the equipment that will meet the vendor's TEMPERATURE, HUMIDITY & DUST CONTROL SPECIFICATIONS.	
	<u>Installation of new hardware</u>	Installation to be done by the MANUFACTURER. If the installation needs interface of the new system with the other system, then some TESTS of the production environment is to be performed.	
	<u>Equipment check out</u>	Equipment must be turned on for TESTING under normal operating conditions.	
TRAINING PERSONNEL	A system can succeed or fail depending on the way it is operated and used. as such the quality of training has serious impact on the system. thus training is major component of system implementation. such training can be imparted through classes, hands-on learning techniques.		
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	Under this strategy, the changeover is done in one operation completely replacing the old system. This conversion takes place often after a break in production.
		Phased Changeover	Under this strategy, the changeover is done by DEGREES. Some new files may be converted & used by the employees while other files continue to be used in OLD SYSTEM. If that phase is successful
		Pilot Changeover	With this strategy, the new system replaces the old one in one operation but only on a small scale.
		Parallel Changeover	Under this strategy, old system remains fully OPERATIONAL while the new system comes ONLINE. Both the system operates independently. If all goes well then the old system is STOPPED & new system carries on as the ONLY SYSTEM.
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	<ol style="list-style-type: none"> 1. Operating procedure to be documented completely for the new system. 2. Before any conversion activities take place, operating procedures must be clearly spelled out. 3. Written operating procedures must be supplemented by oral communication during the training session. 4. Information on inputs, data files, methods, procedure etc. must be presented in a way that is understood by the reader easily. 	

	FILE CONVERSION	<ol style="list-style-type: none"> Here the large information files are to be converted from one medium to another. This phase has to start before programming & testing phase. The major consideration is the cost involved in the file conversion. i.e. OFF-LINE OR ON-LINE conversion. The existing computer files should be kept for a period of time until sufficient files are accumulated for the back-up.
	SYSTEM CONVERSION	<ol style="list-style-type: none"> When the files are converted & reliability of the new system is confirmed, Daily processing can be shifted from existing to NEW system. All the transaction after this phase is carried on the new system. Proper development team must be there to assist the QUERIES that might develop.
	SCHEDULING PERSONNEL & EQUIPMENT	<ol style="list-style-type: none"> Scheduling data processing operations of a new system is a difficult task When the users are familiar with the new system, it becomes the routine job.

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	System Maintenance
<p>Post implementation review ascertains the degree of success from the project. Post implementation review should be scheduled some time after the solution has been implemented.</p> <p>Code to Remember: I - D . O .</p> <p>1. INFORMATION EVALUATION:</p> <ol style="list-style-type: none"> It must be evaluated in terms of information it provides. The objective of the information system is to provide information for the decision making. <p>2. DEVELOPMENT EVALUATION:</p> <ol style="list-style-type: none"> It is primarily concerned with the whether the system was developed on SCHEDULE & within BUDGET. It requires schedule & budgets to be established in advance and that records of actual performance & cost can be maintained. <p>3. OPERATIONAL EVALUATION:</p> <ol style="list-style-type: none"> This evaluation helps in determining whether the HARDWARE, SOFTWARE and PERSONNEL are capable of performing their duties. 	<p>It is an important aspect of the SDL. Most of the information system requires some sorts of modifications after development. Various types of modifications:</p> <p>Code to Remember: P - S . C . R . A . P .</p> <p>1. Preventive maintenance:</p> <ol style="list-style-type: none"> Aimed at increasing system's maintainability. As large program is continuously changed, its complexity increases unless work is done to maintain it <p>2. Scheduled maintenance:</p> <ol style="list-style-type: none"> It is anticipated & can be planned for. <p>3. Corrective Maintenance:</p> <ol style="list-style-type: none"> It is anticipated & can be planned for. Example – Design, logic, data processing, errors etc. <p>4. Rescue Maintenance:</p> <ol style="list-style-type: none"> Refer to previous undetected malfunctions that require immediate solution. <p>5. Adaptive Maintenance:</p> <ol style="list-style-type: none"> Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. <p>6. Perfective Maintenance:</p> <ol style="list-style-type: none"> 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.

Chapter 6: Auditing of Information System

6.1 Introduction:

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.

6.2 Need for Audit of information system:

CODE TO REMEMBER: C.V.A.A.S. - - D.E.E. - - Mc.D.
(Chaminda Vas Sister (Dee) in McDonald)

NEED OF AUDIT	An installation checklist should be developed now with operating advice from the vendor and system development team.	
	C ost of data loss	(a) Data is critical resources for an organisation, (b) For its processes & ability to adapt in the changing environment.
	V alue of Computer hardware, Software & Personnel:	Installation to be done by the MANUFACTURER. If the installation needs interface of the new system with the other system, then some TESTS of the production environment is to be performed.
	Computer A buse	Equipment must be turned on for TESTING under normal operating condition.
	A uditing of info. system	It is the process of focusing on the asset safeguard & data integrity.
	S afeguard of assets	The information system assets must be protected by a system of INTERNAL CONTROLS from unauthorized access.
	D ata Integrity objectives	(a) Integrity of data depends on the value of the information. (b) Importance to maintain data integrity depends on value, extent of access & value of information to the business.
	E fficiency / effectiveness of system	(a) Evaluated by Auditing the characteristics & objective of system. (b) To optimize the use of various information system resources.
	E rror by computer	(a) In this technological environment, one error during the process/ entry, (b) Can cause great damage since it relates to critical business processes.
	M aintenance of Privacy	(a) Data collected in respect of an individual on medical, educational etc. (b) With the use of computers it might be possible that a person may access to these information without proper channel.
	C ontrolled evaluation of computer use	(a) Excess use & dependency on the computers may be destructive. (b) It is not possible to guarantee the success of the process with the use of the technology
	D ecision making (faulty)	(a) Management & operational controls taken by the managers involves detection, investigation & correction of out-of-control processes. (b) For effective & successful decisions it is imperative that management uses correct data.

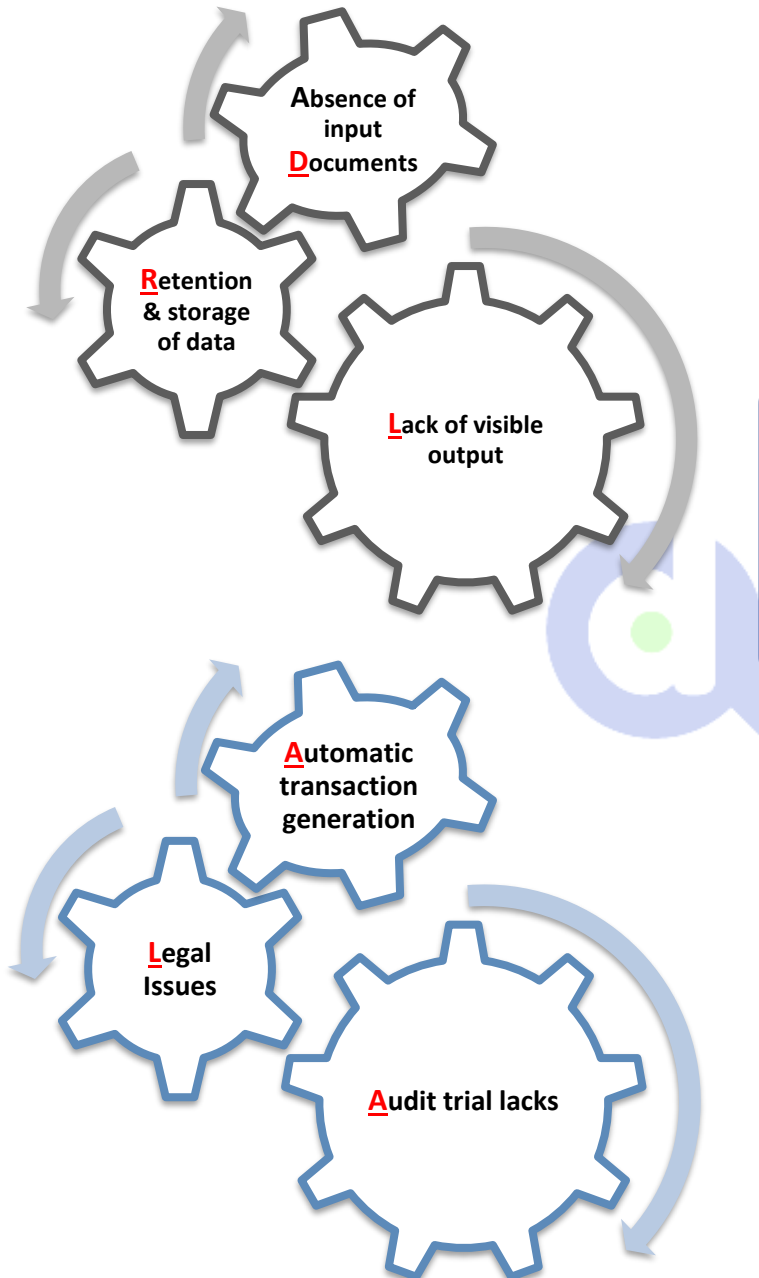
6.3 Effect of Computers On Audit:

Auditor must be competent to provide independent evaluation whether or not the business process activities are reordered and reported as per standards. To do the same, 2 basic functions carried out to examine these changes are:

EFFECT OF COMPUTERS ON AUDIT

Changes to Evidence Collection

**CODE TO REMEMBER:
D.R. - L.A.L.A.**



Changes to Evidence Evaluation

SYSTEM GENERATED TRANSACTIONS

- Financial systems have the ability to initiate, approve & record financial transactions.
- EDI system helps the organisation to provide faster processing without the manual intervention.

SYSTEMATIC ERRORS

- Computers are designed to carry out processing on continuous basis.
- It may not possible that with same inputs, every time same output is obtained.

AUTOMATED

- This system is frequently used in JIT inventory and stock control system.
- This indeed causes problems to auditor in respect of gaining assurance about transaction authorization.
- E.g.: system automatically create a Purchase order if stock drop below minimum level.

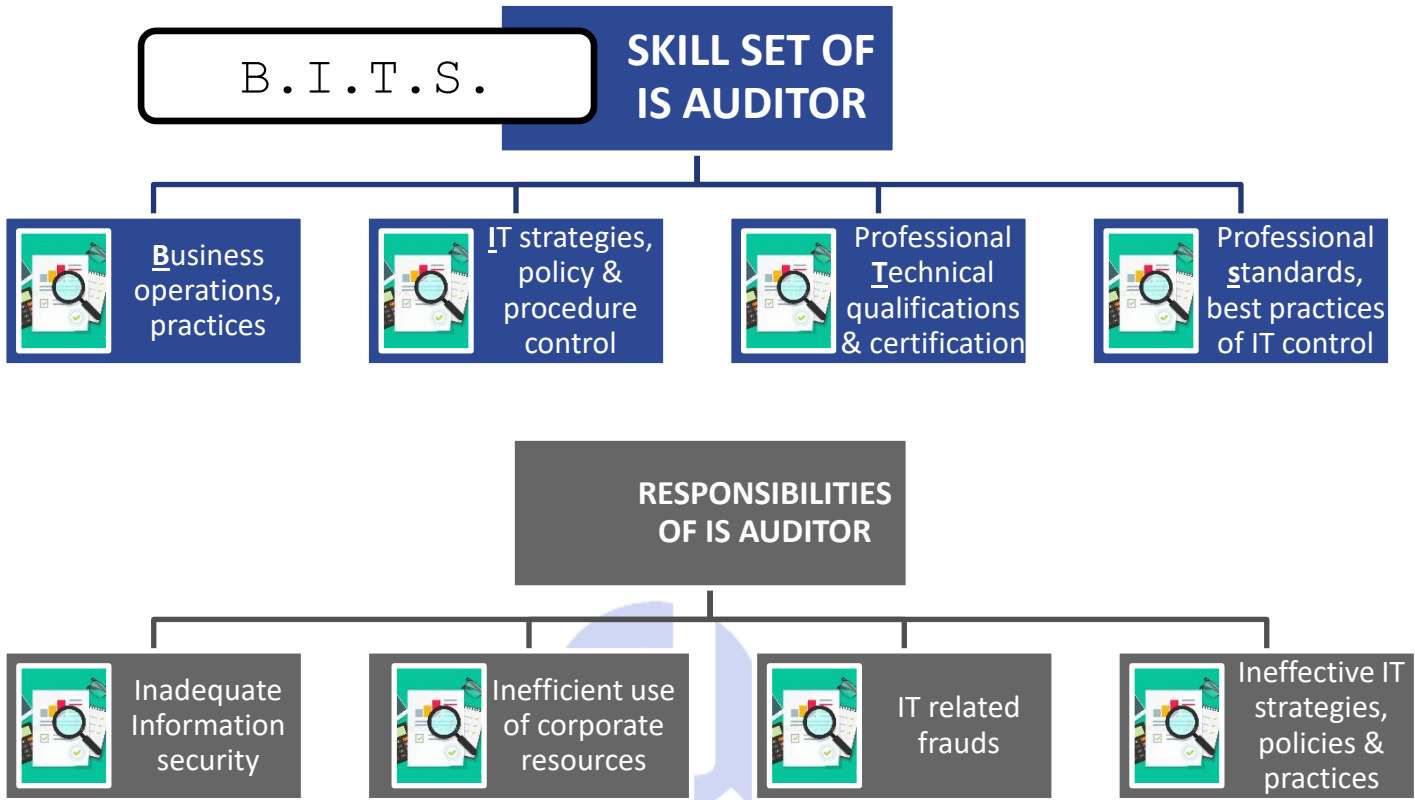
6.4 Responsibilities for controls:

- (a) Management is responsible for establishing & maintaining controls.
- (b) Management should consistently apply the internal controls standards to meet the organizational objectives.
- (c) Senior management is responsible for strategic planning and objectives.
- (d) Middle management develops tactical plans, activities to achieve strategic goals.
- (e) Supervisory management oversees and controls daily activities & functions.

6.5 IS Audit:

Audit of IS environment includes the assessment of internal controls within IS environment to assure, validity, reliability & security information, efficiency & effectiveness of the IS environment in economic terms.

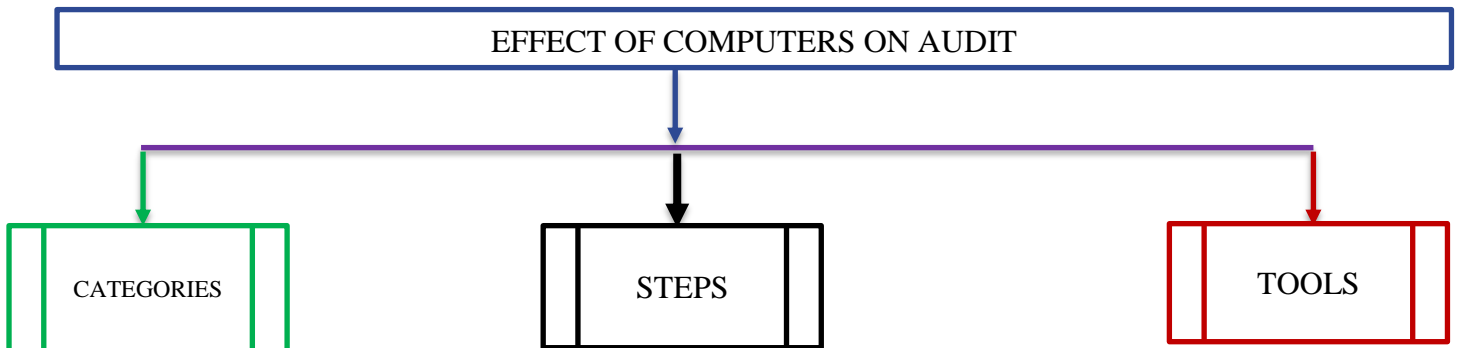
IS audit is done to evaluate the adequacy of the internal controls in respect of both specific computer program and data processing environment.

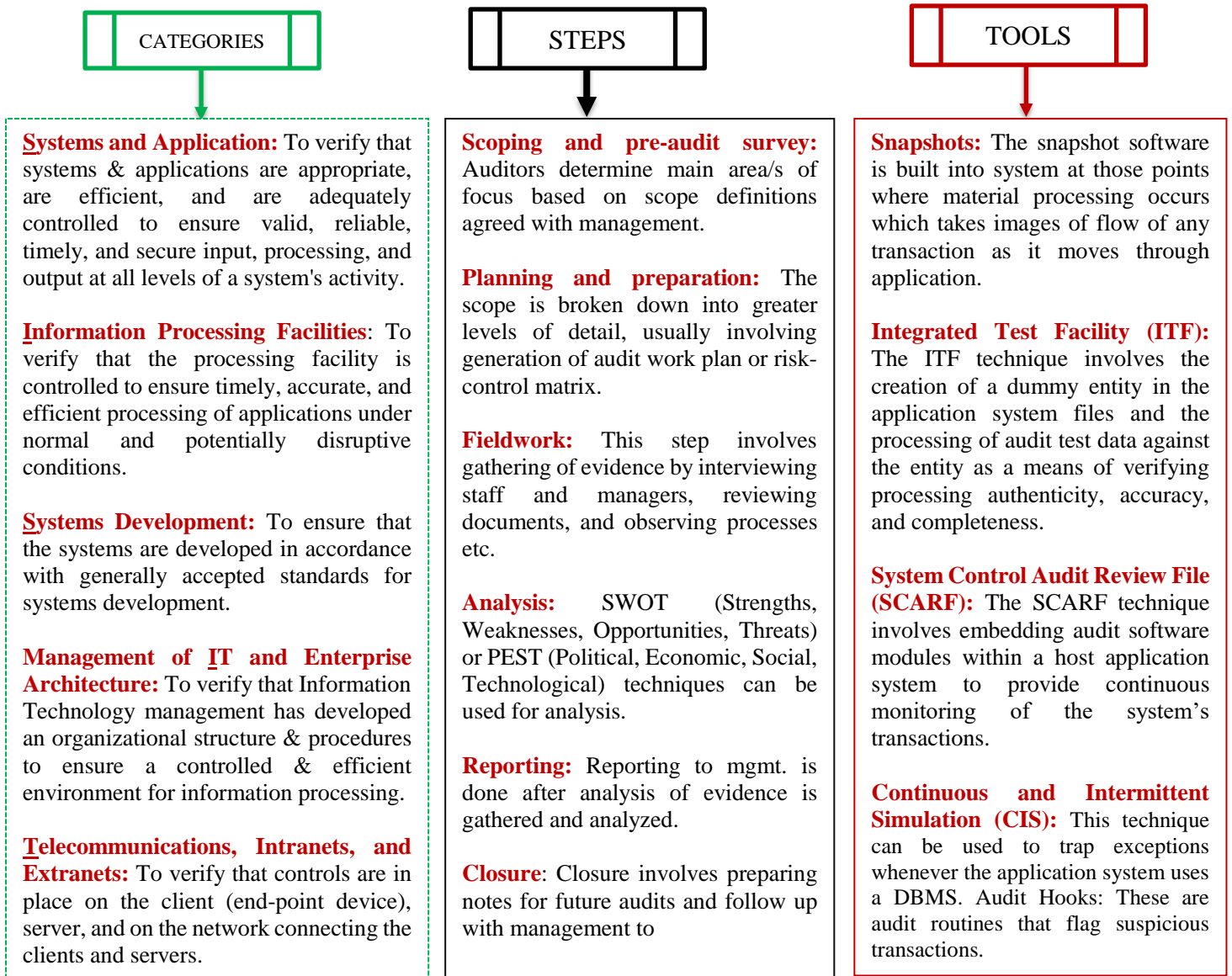


6.6 Information System Audit:

It is the 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.





6.7 Audit standards and best practices:

ICAI has issued various standards on auditing. Though these standards are primarily concerned with the financial information, but they can be used for IS audit depending on its scope and objectives. Some of the well-known organization(s) are present to provide useful information on IS audit:



6.8 Performing Information system audit:

IS auditor uses the concept of materiality and significance to plan audit procedures. Both the elements are being used by the auditor to determine the planned nature, timing and extent of audit procedure.

Auditors perform necessary testing by using **documentary evidences, interviews and personal observations**. Intensive program allows auditor to become informed about the operations. The audit team selects one of the **GAS (Generalized Audit Software)** to determine what changes are necessary to run the software at the installation.

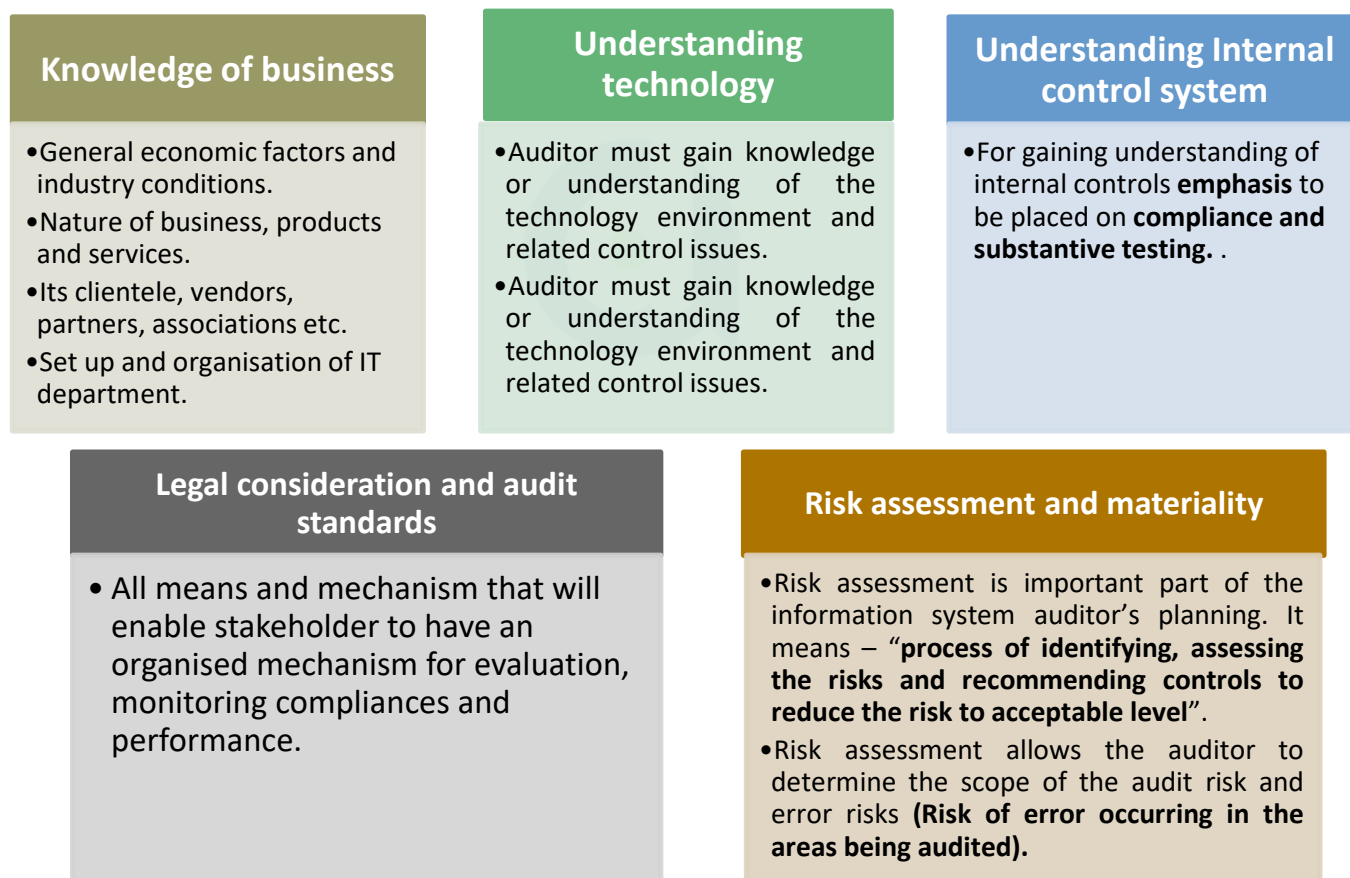
Steps involved which help in conducting effective audit:

1. Basic Plan:

Planning is one of the important phases in information system audit. To make ensure that audit is successful, **a good audit plan** is critical success factor. Planning develops the **annual audit** schedule to perform individual audit.

2. Preliminary Review:

Preliminary review of audit environment enables the auditor to gain understanding of business, technology and control environment.



Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR), and can be calculated thus:

$$AR = IR \times CR \times DR$$

(i) INHERENT RISK:

It means that resources (includes information resources) are open to material theft, destruction, disclosure, unauthorized modification assuming that there is no INTERNAL CONTORLS.

For example, the inherent risk in the audit of a newly formed financial institution which has a significant trade and exposure in complex derivative instruments may be considered to be significantly higher as compared to the audit of a well-established manufacturing concern operating in a relatively stable competitive environment.

Internal controls are ignored in inherent risks since they are considered separately in the control risks.

(ii) CONTROL RISK:

It is the risk that are not prevented or detected and corrected on a timely basis by the internal control system.

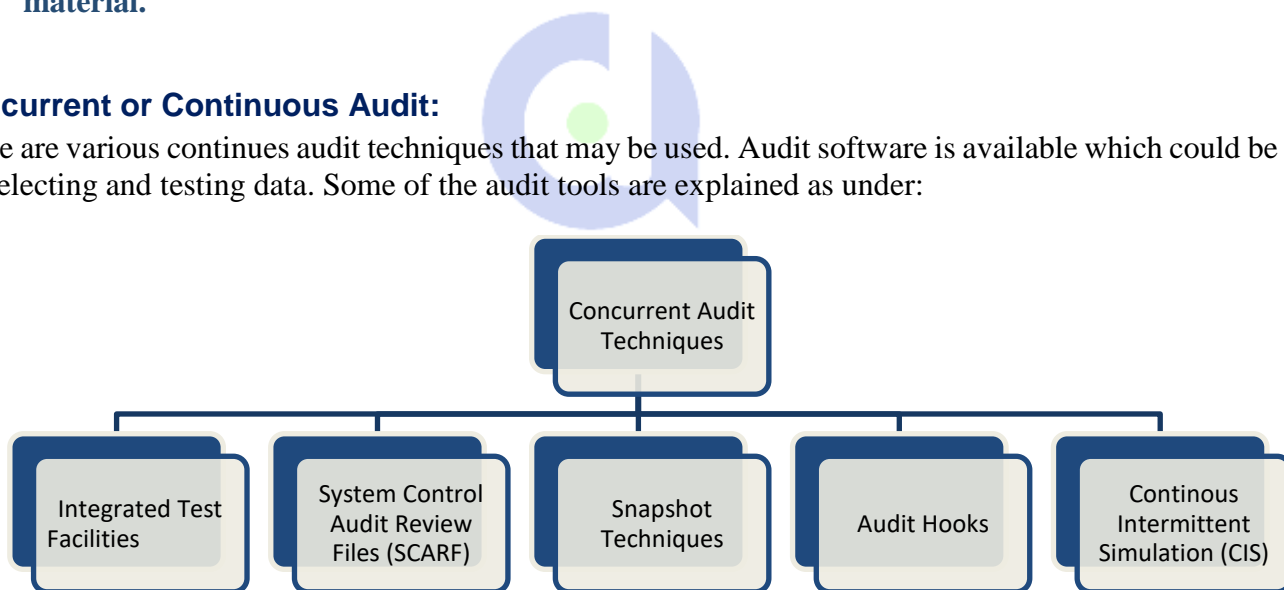
This assessment encompasses assessment of client’s internal control system. This means to ascertain whether or not internal controls are effective for preventing or detecting the gaps in the internal control system.

(iii) DETECTION RISK:

It is the risk that the IT auditor’s substantive procedures will not detect any error which could be material.

6.9 Concurrent or Continuous Audit:

There are various continues audit techniques that may be used. Audit software is available which could be used for selecting and testing data. Some of the audit tools are explained as under:



Integrated Test Facility	<ul style="list-style-type: none">(a) It involves creation of a dummy entry in the application system files.(b) The dummy records entered by the auditor don’t affect the actual records in the system.(c) Auditor after entering dummy records evaluate the processing and output of these transactions with the expected processing & output verifies whether the system and its controls are operating correctly or not.(d) Here the auditor has to decide what would be the method to be used to enter the data and the methodology for removal of the effects of the ITF transactions. (Use ITF module).
---------------------------------	--

System control audit review files (SCARF)	<p>(a) It involves embedding audit software module within a HOST application system.</p> <p>(b) The data are recorded in the SCARF files. Auditor then examines the information contained in this file and see if some aspect of the application system needs follows up.</p>
--	---

TYPES OF INFORMATION	ROLE OF SCARF
Application system Errors	SCARF audit provide independent check on the system processing quality.
Policy and procedure Variances	SCARF audit can be used to check whether entity has adhered to policies, procedures and the standards.
System Exceptions	SCARF can be used for system exception. I.e. if salesperson might be given some authority to charge its customers. SCARF can be used to see the frequency of over-riding the standard price.
Statistical Sample	SCARF provides convenient way of collecting data together on one file & use analytical tools for review.
Snapshots and extended Records	Snapshots and extended Records can be written into SCARF files and printed when required.
Profiling Data	SCARF can be used to collect data to build profiles of the system users. Deviations are being analyzed.
Performance Measurement	SCARF method can be used to collect data for measuring & improving application system performance.

Snapshot Techniques	<p>(a) The snapshot is built into the system at those points where material processing occurs which takes image of the flow of the transactions as it moves through applications.</p> <p>(b) These images then used to access the accuracy, authenticity and completeness of the processing carried out on the transactions.</p> <p>(c) All the snapshot data related to transaction can be collected at one place facilitating audit work.</p>
Continuous Intermittent Simulation	<p>(a) This is a variation of the SCARF continuous audit techniques.</p> <p>(b) It is used to trap exceptions wherever the application system uses database management system.</p>

CODE	ADVANTAGE OF CIS	CODE	DISADVANTAGE OF CIS
I	Information system whether capable of meeting the set goals i.e. Data integrity.	K	Knowledge of experts is needed by the auditor about the information system working.
T	Test (Surprise) can be done by the auditor without the system staff and users being aware that evidence is collected.	A	Audit trail is less visible under this and costs of the errors and irregularities are very high.
A	Audit is conducted in time and in very comprehensive manner. Entire process can be evaluated.	U	In Unstable environment system CIS is not effective.
T	Training for new users.	R	All Resources has to be obtained by the auditor form the organization to support audit techniques.

Audit Hook	<p>(a) These are audit routines that flag suspicious transactions.</p> <p>(b) Auditor must devise a system of audit hook to tag records with name/address change</p>
-------------------	---

6.10 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:

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

Audit Trail Objectives:-	
Detecting Unauthorized Access	<ul style="list-style-type: none"> (a) Involves real time detection. (b) Objective is to protect the system from outsider who is attempting to breach security controls. (c) REAL TIME AUDIT is used to report on changes in system performance that in certain case may indicate any sort of virus infestation.
Reconstruction of Events	Audit analysis can be used to reconstruct the steps that led to system failures, security violations etc.
Personal Accountability	<ul style="list-style-type: none"> (a) Audit trail can be used to monitor user activity at the lowest level of details. (b) This is rather preventive control that can be used to influence behavior.

6.11 Managerial Controls - Audit Trails:

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

Top Management & Information Systems Management Control	<ol style="list-style-type: none"> 1. 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. 2. Organizing: Auditors should be concerned about how well top management acquires and manages staff resources. 3. Leading: Auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. 4. 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	<ol style="list-style-type: none"> 1. Concurrent Audit: Auditors assist the team in improving the quality of systems development for the specific system they are building and implementing. 2. Post -implementation Audit: Auditors seek to help an organization learn from its experiences in the development of a specific application system. 3. 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	<ol style="list-style-type: none"> 1. Planning: Auditors must evaluate how well the planning work is being undertaken. 2. 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. 3. Design: Auditors should find out whether programmers use some type of systematic approach to design. 4. Coding: Auditors should seek evidence to check whether programmers employ automated facilities to assist them with their coding work. 5. Testing: Auditor's primary concern is to see that unit testing; integration testing of the system testing has been undertaken appropriately. 6. 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.

Security Management Controls	Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; and check whether organizations 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.

6.12 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.

6.13 Audit of Application Security Controls:

One of the approaches followed for the application security audit is layered approach. This approach is based on the activities undertaken at various level of management i.e. supervisory, tactical and strategic. Now explaining the layers and related audit issues:

Strategic Layer

- Activities Under this layer
1. Drawing up security policy.
 2. Security guidelines formation
 3. Security training.

IT risk Promote ongoing security awareness to the organisation users. Auditor role is to verify whether aforesaid guidelines have been properly farmed and are capable of achieving for the purpose for which they are formulated.

Tactical Layer

- Activities Under this layer
1. Timely updating the users. Auditor must verify that any changes in user account are by formal ways.
 2. Regular monitoring the audit log is required.
 3. There is need of interface security.

Operational Layer

- Activities Under this layer
- Duty segregation**
It is basic internal control that prevents or detects errors and irregularities by assigning individual responsibilities, for initiating and recording the transactions.
- User account and access right**
This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities. Auditor must ensure that these User ID and password are traceable.
- Password Controls**
Auditor has to ascertain whether such password controls are weak or strong. If controls are found to be ineffective, he must take necessary step to compensate loss from such weak controls.

Chapter 7: Information Technology Regulatory Issues

7.1 Introduction:

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

7.2 IT Act 2000 and its objectives:

This act provides legal recognition for transactions carried out by means of electronic data interchange. Objective of this act:

CODE	ADVANTAGE OF CIS
Storage of Data	Facilitate electronic storage of the data
Amendment in other laws	This act results in simultaneous amendment following laws. Indian Penal Code, The Indian Evidence Act, 1872, The Banker's book Evidence Act, 1891, Reserve Bank of India, 1934.
Legal Recognition	To grant legal recognition for transaction carried out by means of EDI to digital signatures for authentication, for keeping banking BOA* in electronic form.
E-Filing Facilitation	Facilitate e-filing of documents with government departments.

7.3 Definitions:

Sections/Name	Description
Access	Getting entry into logical, arithmetical or memory function resources of computer or computer network.
Addressee	Means a person who is intended by the originator to receive the electronic records not including any intermediary.
Adjudicating officer	Means officer appointed under section 46(1).
Affixing Electronic signature	Means adoption of any methodology or procedure by a person for the purpose of authenticating ELECTRONIC RECORDS by means of electronic signature.
Appropriate Government	Enumerated in LIST II of seventh Schedule to constitution relating to any state law enacted under LIST III of seventh Schedule to constitution.
Asymmetric crypto system	Means a system of a secure key pair consisting of a PRIVATE KEY for creating digital signature & a public key to verify the digital signature.
Certifying authority	Means a person who has been granted a LICENSE to issue an ELECTRONIC SIGNATURE CERTIFICATE under SECTION 24.
Certificate practice statement	Means a statement issued by a CERTIFYING AUTHORITY to specify the practices that certifying authority employs in issuing electronic signature certificate
Computer	Means Electronic, magnetic, optical & high speed data processing machine that Performs logical, arithmetic & memory functions by manipulating of electronic, magnetic & includes all inputs, output, processing facilities which are connected in a computer system.




Computer Network	Means interaction of ONE or MORE computers/ computers system/ communication device through use of satellite, microwave, wire/ wireless terminals.
Computer System	It means a device or a collection of the devices , including input & output devices capable for being used in conjunction with the external files containing computer programs, electronic instructions, input data, that performs logic, arithmetic; data storage & retrieval , communication control & other functions.
Communication Device	Means cell phone, personal digital assistance or combination of both used to communicate, send or transmit text, audio, video or images.
Controller	Means controller Of Certifying Authorities appointed under section 17(7).
Data	Representation of facts, knowledge, concepts, information, instructions which are being prepared in a formalized manner & is intended to be processed in a computer system/ network & may be in any form or stored internally in the memory of the computer
Cyber café	Means any facility from where access to internet is offered by a person in ordinary course of business.
Cyber security	Means protecting information, equipment, devices, computer, computer resources, communication device & information stored therein from UNAUTHORISED ACCESS, USE, DISCLOSURE etc.
Digital signature	Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the section 3.
Digital signature certificate	Means protecting information, equipment, devices, computer, computer resources, communication device & information stored therein from UNAUTHORISED ACCESS, USE, and DISCLOSURE etc.
Electronic Form	With the reference to information means information generated, received, stored in any media, magnetic tape, optical devices, computer memory and micro films.
Electronic records	Means data, records, images, sound (R.I.D.S.) sent, received and stored in an electronic from.
Electronic signature	Authentication of any records by a subscriber by means of electronic technique as in 2 nd schedule & include digital signature
Function	In relation to computer includes Logical, control, communication, arithmetic, retrieval, deletion, storage from or within computers.
Intermediary	Intermediary with respect to any particular electronic records, means person who on behalf of other receives, stores or transmits those records with respect to that records etc.
Key pair	<ol style="list-style-type: none"> 1. It is asymmetric crypto system, means 2. Private key & its related public key which are so related that public key can verify a digital signature created by the private key.
License	<ol style="list-style-type: none"> 1. It means license granted to certifying authority under section 24. Here originator means who Send generates, stores or transmit any electronic, or cause any electronic message to be sent, generated, stored to any person. Prescribed: means prescribed by rules made under this act Private key: Key used to create a digital signature Public key: Key used to verify a digital signature & listed in DSC.



Secure System	Means computer hardware, software & procedure that:-	
	P	P erforming the intended functions
	U	Security from U nauthorized access & misuse.
	R	Reasonable level of R eliability & correct operation.
	A	A dhere to general accepted security procedures.
Security Procedure	Security procedure prescribed under section 16 by central government	
Subscriber	Means a person in whose name the electronic signature certificate is issued.	
Verify	In relation to a digital signature, electronic records or public key, to determine whether → a. Initial electronic records were affixed with the digital signature by use of private key corresponding to the public key of the subscriber. b. Initial electronic records are retained intact or have been altered since such electronic record was so affixed with the digital signature	

7.4 Digital Signature & Electronic Signature:

CHAPTER II	Creation of digital Signature	<p>(a) Electronic records are converted into message digest by using mathematical functions called hash.</p> <p>(b) Identity of the person affixing the digital signature is authenticated through the use of private key which can be verified by the receiver by using public key corresponding to that private key.</p>
	Section 3 Authentication Of Electronic Records	<p>a) Subject to provisions of this section, any subscriber may authenticate electronic records affixing his digital signature.</p> <p>b) Authentication is effected by use of asymmetric crypto system & hash function which transforms the electronic record in another ELECTRONIC RECORD.</p> <p>c) Any person by use of public key of the subscriber can verify electronic records.</p> <p>d) Private and Public key are unique to subscriber & constitute a functioning key pair.</p>
	Section 3A Electronic Signature	<p>a) Notwithstanding anything contained in section 3, a subscriber may authenticate any electronic records by such electronic signature/ authentication technique which is considered reliable & may be specified in 2nd schedule.</p> <p>b) Electronic signature/ authentication technique will be considered reliable If:</p> <ul style="list-style-type: none"> • Any alteration to information made after authentication is detectable. • Any alteration to electronic signature made after affixing is detectable. • Signature creation/authentication data are linked to authenticator & no other person • Signature creation/authentication data at time of signing are under control of the authenticator & no other person. • Other conditions as prescribed <p>c) Central government may prescribe the procedure of ascertaining whether electronic signature is that of person by whom it is supposed to be affixed.</p> <p>d) Central government (Notification in OZ) may add or omit any electronic signature/ authentication.</p> <p>e) Such notification in OZ shall be laid before each house of parliament.</p>

<p>Section 4 Legal recognition of Electronic Records</p>	<p>Where the law provides that information is to be in written form, and then such requirement shall deemed to be satisfied if such information is:</p> <p>(a) Made available in an electronic form. (b) Accessible So As To Be Usable For A Subsequent Reference</p>	
<p>Section 5 Legal recognition of digital Signature</p>	<p>Where the law provides that information should be authenticated by affixing the signature of any person then such requirement shall deemed to be satisfied if it is authenticated by means of DIGITAL SIGNATURE affixed in such way as CG prescribed.</p>	
<p>Section 6 Use Of Electronic Records & Signature In Government & Its Agencies</p>	<p>Where any law provides for:</p> <p>(a) Filing of any form, application etc. with office, authority, government agencies in particular manner, (b) Issue/grant of any license, sanction, approvals in a particular manner. (c) Receipt/payment of money in a particular manner.</p> <p>Such requirement shall be deemed to be satisfied if such Filing of any form, Issue/grant of any license, receipt/payment of money is affected by means of electronic form.</p>	
<p>Section 7 Retention of Electronic Records</p>	<p>Where law provides that documents, records etc. to be retained for specific period, then such requirement shall be deemed to be satisfied if such records are in electronic form:</p> <p>(a) Information contained remains accessible so as to be usable for subsequent reference (b) Electronic records are maintained in the FROMAT IT IS ORIGINAL GENERATED, sent or received. (c) The details which will FACILITATE the identification of the origin, destination, date & time of dispatch of such electronic records are available in ELECTRONIC RECORD.</p>	
<p>Section 7A Audit of documents etc. in electronic form</p>	<p>Where law provides, there is provision for audit of documents, records & information, then same rule will applicable in respect of electronic form.</p>	
<p>Section 8 Publication Of Rules, Regulations etc. In Electronic Gazette</p>	<p>Where law provides, that any rules, regulations, order, bye laws have to publish in Official Gazette, then such requirement deemed to be satisfied if such rules, regulations, order, bye laws published in the ELECTRONIC GAZETTE.</p>	
<p>Section 10 Power To Make Rules By Central Govt.</p>	<p>M.</p>	<p>Manner & format in which electronic signature shall be affixed.</p>
	<p>C.</p>	<p>Control processes / procedures to ensure adequate integrity, security & confidentiality of electronic records/payments.</p>
	<p>P.</p>	<p>Procedure which facilitate identification of person affixing electronic signature</p>
	<p>T.</p>	<p>Type of Electronic Signature.</p>
<p>Section 10 Audit of documents</p>	<p>Where in contract formation, the communication of proposal, acceptance of proposal, revocation of proposal and rejection is being expressed in electronic form or by means of an electronic record. So, validity of the contract cannot be questioned only on the ground that electronic form is being used.</p>	

CHAPTER V	Section 14 Secure Electronic Records	Where any security procedure is applied to an electric record at a specific point of time, then such records shall deemed to be secure electronic record from such point of time to time of verification.
	Section 15 Secure Electronic Signature	An electronic signature shall be deemed to be secured if: (a) Signature creation data, at time of fixing signature was under the exclusive control of signatory & no other person. (b) Signature creation data was stored in such manner as prescribed.
	Section 16 Secure procedures & practices	Central government may prescribe the security procedures & practices. It may take into consideration the commercial circumstances, nature of transaction & other related factors.

7.5 Various authorities for system control and audit:

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.

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.

(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.

7.6 Security Standards:

Information security is essential in the day-to-day operations of enterprises. Any breach of information security might result in adverse effect on the entity. COBIT 5 published by ISACA highlight the need for enterprises to ensure required level of security is implemented. There are many security standards which may ensure protection of vital information of the business. Some of them are:

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 aims to provide a methodology for the implementation of information security in an organizati

SA 402

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

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.

SERVICE STRATEGY

SERVICE DESIGN

SERVICE TRANSITION

SERVICE OPERATION

CONTINUAL SERVICE IMPROVEMENT

PENALTIES CHART

PENALTIES & ADJUDICATIONS	Section 43 Penalties & Compensation For Damage To Computers, Computer System, etc. Code to Remember A.M.C. – D.V.D	If any person without permission of the owner / any other person who is in-charge of computer, computer resources--	
	A	<u>A</u>ccess to computers: Accesses or secure access to such computer, computer resources, computer network.	
	M	<u>M</u>anipulation of information: Destroys, deletes or alters any information in the computer resources, or use it in such a manner that it diminishes/reduces the value of the information.	
	C	<u>C</u>oncealment of computer resource: Steals, conceals, destroy / or cause any person to steals, conceals, destroy any computer source code with an intention to cause damage	
	D	<u>D</u>ownload of information: Downloads copies or extracts any data, database from such computer, computer resources or computer network.	
	V	<u>V</u>irus in computer system: Introduces, or cause to introduce any computer virus/any computer contaminant into any computer system or computer network.	
	D	<u>D</u>isruption in computer network: Disrupts or cause disruption of any computer, computer system or computer network.	
	Section 44 Penalty For Failure To Furnish Information, Return Etc.	Reason of penalty imposition	Amount of penalty
		Furnish any documents, return or report to the controller or certifying authority, FAILS to furnish the information,	Not exceeding Rs. 1,50,000.00 ≤ 1,50,000.00 [for each failure]
		Return / information not furnished within the time as specified in the regulations	Not exceeding Rs. 50,000.00 ≤ 50,000.00 [For every day during which such failure continues]
	Book of accounts are not maintained	Not exceeding Rs. 10,000.00 ≤ 10,000.00 [For every day during which such failure continues]	
Section 45 Residual Penalty	For which no penalty is separately provided separately.	Not exceeding Rs. 25,000.00 ≤ 25,000.00	

3. COMPUTER CONTAMINANT:

It means set of computer instructions that are designed:

- To modify, destroy, record data/program in computer OR
- By any mean to usurp (seize or hold) normal operations of computer.

4. DAMAGE:

- Means destroy, alter, delete, add, and modify **[MADAD]** re-arrange any computer resources.

1. COMPUTER DATABASE:

It means representation of Information, knowledge, facts, concepts in image, video, audio, text that is being **prepared in formalized manner** or has been produced, by computer, computer resources, and computer network.

2. COMPUTER VIRUS:

It means computer instruction, information, data or program that **destroys, damage, degrades & adversely affect performance of computer** or which attach itself with other computer resources & operates when a program is executed.

OFFENCES CHART

Section Number	Nature of Offence	Penalties for offences
CODE TO REMEMBER : CD-SR [CD of SIR]		
65	Intentionally Concealment, destroy, alteration any source code, computer program, computer system, network, resources etc.	Imprisonment / fine 3 years or 2,00,000 OR BOTH
66	Damage to computer, computer resources, by doing acts defined in section 43	Imprisonment / Fine 3 YEARS OR 5,00,000 OR BOTH
66A	Sending offensive messages through communication services etc. 1. Info. Having threat character 2. Info which is false & is being communicated to cause danger. 3. Email send to deceive to mislead the recipient about message origin point	Imprisonment 3 YEARS and Fine
66B	Receiving dishonestly any stolen computer resources or communication devices	Imprisonment / Fine 3 years or 1,00,000 Or Both
CODE TO REMEMBER : I. -C.V.C.		
66C	Identification theft fraudulently by making use of the ELECTRONIC SIGNATURE, PASSWORD	Imprisonment / Fine 3 years or 1,00,000
66D	Cheating by personation by using computer resources.	Imprisonment / Fine 3 years or 1,00,000
66E	Violation of the privacy of any person	Imprisonment / fine 3 years or 2,00,000 OR BOTH
66F	Cyber Terrorism done with: (a) Intent to threaten integrity of India. (b) Intentionally penetrates a computer resources result in damage to property	<u>IMPRISONMENT</u> LIFETIME
67	Punishment for publishing or transmitting OBSCENE MATERIAL in electronic form	CONVICTION IMPRISONMENT FINE 1 st 3 YEARS 5,00,000 Subsequent 3 YEARS 10,00,000
67A	Punishment for publishing or transmitting of MATERIAL contain sexually explicit act etc. in electronic form	CONVICTION IMPRISONMENT FINE 1st 5 YEARS 5,00,000 Subsequent 7 YEARS 10,00,000
67B	Punishment for publishing or transmitting of MATERIAL depicting children in sexually explicit act etc. in electronic form.	CONVICTION IMPRISONMENT FINE 1st 5 YEARS 5,00,000 Subsequent 7 YEARS 10,00,000
73	No person shall publish the electronic signature certificate to any other person knowing that: (a) Certifying authority listed in the certificate, has not issued it. (b) Subscriber listed in the certificate has not accepted. (c) Certificate has been revoked or suspended	Imprisonment (Extend up to 2years) and fine may extend to INR 1,00,000 or both.

OFFENCES

MISCELLANEOUS PROVISIONS

SECTION NUMBER	DESCRIPTION
<p>Section 70 Protected system</p>	<ol style="list-style-type: none"> 1. Appropriate government, by notification in official gazette, declares any computer resources which directly or indirectly affects the facility of critical information infrastructure. 2. The appropriate government, by order in writing, authorizes the person who is authorized to access the protected system. 3. If any person tries to access the protected system in contravention of the provisions shall be punishable with imprisonment (Extend up to 10 years) and fine.
<p>Section 80 Power of police officer and other officer to enter, search etc.</p>	<p>Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act</p>
<p>Section 81A Application of The Act to Electronic Cheque and truncated Cheque</p>	<p>The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.</p>
<p>Section 84C Punishment for attempt to commit offences</p>	<p>Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.</p>
<p>Section 85 Offences By Companies</p>	<p>Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.</p>

Chapter 8: Emerging Technologies

8.1 Introduction:

Emerging Technologies are contemporary advances and innovation in various fields of technology. Various converging technologies have emerged in the technological convergence of different systems evolving towards similar goals. Emerging technologies are those technical innovations which represent progressive developments within a field for competitive advantage.

8.2 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 V- P.M. – M.A.R.S.	ADVANTAGES I. - C.A.R.D.S.
<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • VIRTUALISATION • PERFORMANCE • MAINTENANCE • MULTI-SHARING • AGILITY • REALIBILITY AND AVAILABILITY • SCALABILITY 	<ul style="list-style-type: none"> • INTEGRATION OF SOFTWARE • COST EFFICIENT • ACCESS TO INFORMATION • RECOVERY • DEPLOYMENT • STORAGE

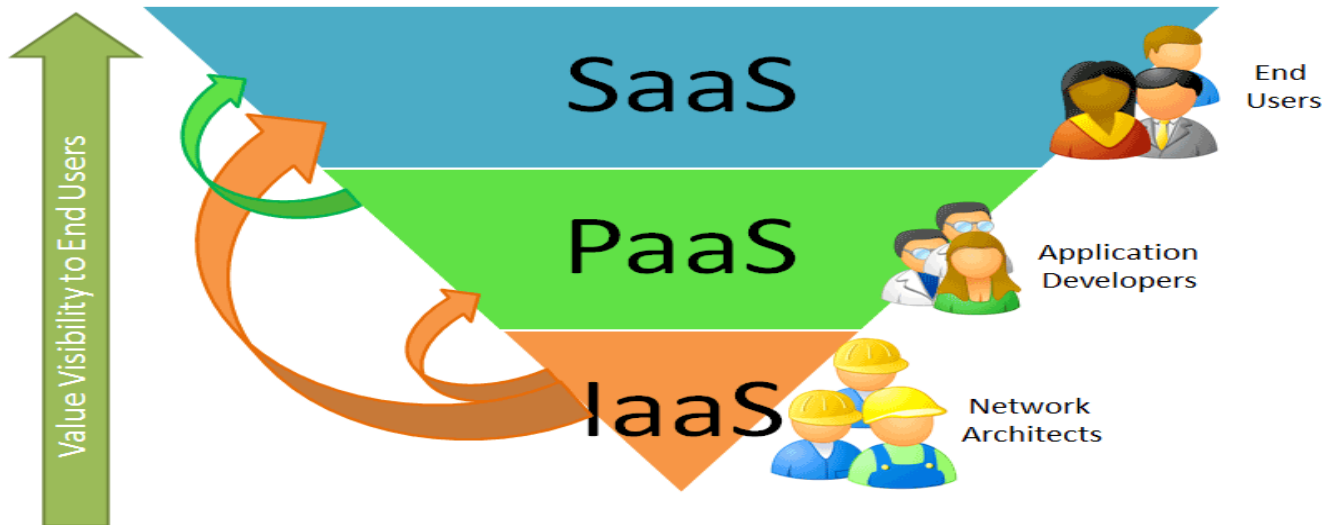
8.3 Cloud computing environment / Types of Cloud:

Cloud computing environment			
PUBLIC CLOUD	PRIVATE CLOUD	COMMUNIUNITY CLOUD	HYBRID CLOUD
<p>A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider). Public cloud services may be free or offered on a pay-per-usage model. This environment can be used by general public.</p>	<p>A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. These are typically deployed within an organization's own internal ecosystem, often leveraging the organization's own private data center. Private clouds typically rely on the organization having trained IT staff onsite to manage the private cloud ecosystem.</p>	<p>Here the cloud is being shared by person(s) of one community and hence the name. In this type of cloud infrastructure is provisioned by a specific community</p>	<p>A hybrid storage cloud uses a combination of public and private storage clouds. Hybrid storage clouds are often useful for archiving and backup functions, allowing local data to be replicated to a public cloud.</p>

8.4 Advantages & Characteristics of type of cloud:

ADVANTAGES	THE MAIN BENEFITS OF USING A PUBLIC CLOUD:
	<ul style="list-style-type: none"> (a) Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider. (b) Scalability to meet needs. (c) No wasted resources because you pay for what you use.
CHARACTERISTICS	THE MAIN BENEFITS OF USING A PRIVATE CLOUD:
	<ul style="list-style-type: none"> (a) Improves the average server utilization, usage of low cost servers & hardware. (b) Small in size...Controlled and maintained by the organization. (c) Provides high level of security and privacy to the users.
CHARACTERISTICS	CHARACTERISTICS OF PUBLIC CLOUD: (S.A.L.S.A.)
	<ul style="list-style-type: none"> (a) Scalable: Resources and the users in the public code are large and service provider has to grant all the requests. Hence public clouds are considered to be scalable. (Able to be changed in size or scale.) (b) Affordable: In this case, user pays for that only for what he or she is using and this don't involve any cost related to the deployment Less Secure: Since it is offered by third party and they have full control over the cloud, as such it is less secured as compared to on-premises public cloud. (c) Stringent SLAs: Since there is Service level agreement between the service provider and users, and reputation of the service provider is dependent on that, they follow the SLA very strictly. (d) Available: It is highly available since anyone can link to the public cloud with the proper permission.
	CHARACTERISTICS OF PRIVATE CLOUD:
	<ul style="list-style-type: none"> (a) Secure: Private cloud is being managed by organization itself, hence less chance of data being stolen and leaked out. (b) Central Control: Private cloud is managed by organization itself so there is no need of relying on the outside agency hence results in central control by the entity. (c) Weak Service-level Agreement: SLAs are agreement between user and the service provider. However, in case of private cloud the SLA is weak since this type of networking is between the organizations & user of the same organization.
	CHARACTERISTICS OF HYBRID CLOUD:
	<ul style="list-style-type: none"> (a) Scalable: Hybrid has the property of public cloud hence scalable. (b) Partly Secure: Public cloud is more vulnerable and is subject to high risk of security breach. AS such hybrid is not fully secure, hence partly. (c) Stringent SLAs: Since there is Service level agreement between the service provider and users, and reputation of the service provider is dependent on that, they follow the SLA very strictly. (d) Complex Cloud Management: Since hybrid model comprises of one or more deployment models & users are also very large.
	CHARACTERISTICS OF COMMUNITY CLOUD:
	<ul style="list-style-type: none"> (a) Cost effective: Since community cloud is shared by several organizations, the community cloud is cost effective too. (b) Collaborative & Distributive Maintenance: Since there is sharing of the cloud among various organization, as such the control is distribute and hence better cooperation provides better results.

8.5 Cloud computing service models:



Now explaining each of the services in detail:

INFRASTRUCTURE AS A SERVICE (IaaS)	MEANING OF IaaS:	
	<p>Infrastructure-as-a-Service providers provide an alternative to buy and install the software and the equipment which are needed to support the business operations. The servers and the networks that are required to provide the storage, server functions and networks are provided by this IaaS vendor. Example of IaaS provider includes Amazon, EC2, Dyn DNS, Google chrome engine etc.</p> <p>IaaS provides you the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc.</p>	
	CHARACTERISTICS OF IaaS: (M. - W.I.S.E.)	
	M	Management is centralized: Resources distributed across different places to be controlled from any management console that ensure effective resource management
	W	Web access to the resources: IaaS enables the users to access the infrastructure resources over the internet.
	I	Infrastructure Sharing: In IaaS, different users share same physical infrastructure and thus ensure high resource utilization.
S	Metered Services: IaaS allows the user not to buy the computing resources but to rent them. The user will be charged as per the usage.	
E	Elasticity & dynamic Scaling: IaaS service provider can increase or decrease the usage of the resources depending on the load.	
DIFFERENT INSTANCE OF IaaS:		
<ul style="list-style-type: none"> • Network-As-A-Service (NaaS) • Storage as a Service (STaaS) • Database as a Service (DBaaS) • Backend as a Service (BaaS) • Desktop as a Service (DTaaS) 		

PLATFORM AS A SERVICE (PaaS)	MEANING OF PaaS:	
	(a) PaaS is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet.	
	(b) Platform as a Service allows users to create software applications using tools supplied by the provider.	
	(c) PaaS services can consist of preconfigured features that customers can subscribe to; they can choose to include the features that meet their requirements while discarding those that do not.	
	CHARACTERISTICS OF PaaS:	
	W	Web access to development platform: PaaS provides helps the developer to create, modify, test & deploy different applications.
	S	Scalability: PaaS ensure that applications built are capable of handling the varied loads efficiently.
C	Collaborative Platform: To enable collaboration among developers, most of PaaS provider provides tools for project planning and communication.	
O	Metered Services: IaaS allows the user not to buy the computing resources but to rent them. The user will be charged as per the usage.	
E	Elasticity & dynamic Scaling: IaaS service provider can increase or decrease the usage of the resources depending on the load.	

SOFTWARE AS A SERVICE (SaaS)	MEANING OF SaaS:	
	Software-as-a-Service is cloud service where consumers are able to access software applications over the internet. The programs which are developed by the software developers are accessed by the customers through the browser and pay the fees for their usage. Users don't have to worry about the installation, setup and running of the application. Service provider will do that.	
	CHARACTERISTICS OF SaaS: (W.O. – C.A.M)	
	W	Web access: User can use application from any location of device is connected to internet.
	O	One to many: Single application can be used by multiple users.
	C	Centralized Management: SaaS services are managed from a single location as such there is centralized control.
	A	Availability: SaaS ensures almost 100% availability of data..
M	Multi-device Support: SaaS can be accessed from any devices e.g. desktop, mobile, laptop etc.	

8.6 Challenges to cloud computing: (D. – L.A.S.T. – I.C.A.I. – G.A.A.P)

D	Data Stealing: In cloud computing, data is accessible by everyone and from anywhere. There may be the chances where the cloud provider uses infrastructure of some other service provider. As such, data is less secured and is prone to concept of “data stealing”.
L	Legal Issues And Compliances There are various data, security laws that to be complied with by the entity. There is need to understand various types of rules and laws that imposes security and privacy duties on the organization.

A	Audit: It emphasis on “What is happening in the cloud environment”. It is being hosted on the virtual machine to watch “what is happening in the system”. The context of use of clouds, time consuming audits seriously detains the key gain of cloud agility.
S	Software Isolation: Software isolation is a way to understand virtualization and other techniques that the cloud owner employs in software architecture and evaluate the risks required for the organization.
T	Trust: Deployment model provide a trust to cloud environment. An entity has direct control over its security issue. Trust is an important issue in the cloud. Trust ensures that service arrangements are sufficient to allow visibility into security and privacy controls.
I	Incident Response: It ensures to meet the organization’s requirement during an incident. It ensures that cloud provider has a transparent response process in proper place. Affected network, applications, exposed intrusion helps to understand an incident response.
C	Confidentiality: Prevention of data access from unauthorized disclosure referred to as confidentiality. Cloud works on public network therefore it is imperative to keep the data confidential. This can be done through encryption of data or by way of physically secure at separate location.
A	Architecture: In cloud computing model, there should be control over security and privacy of the system. Its reliable and scalable infrastructure depends on design and implementation to support the overall framework.
I	INTEGRITY: Integrity means prevention of data from unauthorized modification of data and ensures that data is of high quality, correct, accessible and correct. On cloud network it should be ensured that data is not changed. Redundant Array of Independent Risks (RAID) is one of the way to preserve integrity on the cloud computing.
G	Governance: Since on cloud computing there is no control over the employees and services, it creates problems like design, implementation, testing etc. So there is need to put up governance model that will control the standards, policies and procedures of the entity.
A	Application security: It applies when application moves to cloud platform. Service provider should have complete access to server with all rights to ensure protection of the application. Infected application need to be monitored and recovered by the cloud security drivers.
A	Availability: The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. It ensures back up of data through BCP, DRP. Cloud computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems.
P	Privacy: It is one of the important issue in the cloud computing. The privacy issues are embedded in each phase of cloud design. The cloud should be designed in such a way that it decreases the privacy risks.

8.7 Mobile Computing:

A technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link.

Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution to the biggest problem of business people on the move – mobility.

CODE	Issue in Mobile Computing	CODE	Limitations of Mobile Computing
C	Challenges of Business This is due to lack of trained professionals to bring mobile technology to general people.	B	Bandwidth insufficient: It is slower than direct cable connections
S	Security Issues: Wireless networks have more security requirement than that of wired networks	S	Security standards: When mobile connects, one is dependent on public network
B	Bandwidth: The same can be improved by logging and compression of data before transmission	P	Power consumption: a mobile is dependent on the battery inbuilt in it. expensive batteries are used.
P	Power consumption: In case of mobile, without power a mobile is dependent on the battery inbuilt in it.	H	Health Hazards: Use of phone while driving which is a major cause of accidents.
P	Performance: Since mobile computing involves multiple networks and applications, end-to-end technical compatibility, server capacity and network response time are difficult to achieve.	H	Human interface with the device: input device in mobile such as keyboard is small in size and as such hard to use
L	Integration with Legacy mainframe: IT focuses on mainframes, a huge inventory of applications using communication interface that are basically incompatible with mobile connectivity have been accumulated.	T	Transmission Interface: Any geographical conditions may hinder the good transmission for e.g. hilly areas, tunnel etc.
R	Revising technical architecture: Mobile users are demanding. So in order to provide complete connectivity among the users; the current communication must be revised to incorporate mobile connectivity.		

Components of Mobile Computing

- 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 program that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications.

8.8 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. Below are the best practices of green computing →

(a) Develop a sustainable green Computing plan

1. Involve stakeholders to include checklist, recycling policies for disposal of used components & equipment.
2. Involve power usage, reduction of consumption of papers, recycling old machines & equipment.
3. Use cloud computing so that multiple organizations share same computing resources.

(b) Recycle:

1. Dispose e-waste as per regulations.
2. Discard unwanted equipment in environmentally responsible manner.
3. Manufacturers must provide option how to dispose equipment when become unusable.

(c) Environment Sound Decisions:

1. Purchase of laptops, desktops based on environmental attributes.
2. Clear policy in respect of designing of the product.

(d) Reduced Paper Consumption:

1. More use of emails resulting in saving of papers.
2. For marketing, advertising on-line marketing is best and will reduce paper wastage.
3. Use both side of paper while printing any document.

8.9 BYOD:

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	Threats
<ol style="list-style-type: none">1. Happy employees: Employees use their own devices at work. It lowers the burden since they have to take only their device not the organizational device.2. Lower IT budget: Since employee bring their own device, this result in decrease in outlay of the organization. (Organizations need not to purchase the devices for their employee).3. IT reduces support requirement: Since, devices are of employee there is cost saving since IT doesn't have to provide and user support and maintenance activities.4. Increased employee efficiency: In case of self-device, user is efficient in working on its own device. In case it works on other devices some learning phase is included.	<ol style="list-style-type: none">1. Application risks: Employee's phone or smart devices that are connected to corporate network are not protected by security software.2. Device risks: Lost or stolen computer device or mobile phones can result adverse impact on the company as these devices contains vital information about the company.3. Implementation risks: A weak BYOD policy may result in failure of communication of employee expectations; thereby increase the chances of device misuse.4. Network risks: As BYOD involves use of personal devices, IT is unaware of number of devices connected to the company network. For instance, any virus is detected in the network as such it is imperative to scan all connected devices. Since complete visibility is not there, it may be possible that some devices may not get covered under scanning program. This is hazardous for the company.

8.10 Web 2.0 & 3.0:

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.

Web 2.0	Web 3.0
<ol style="list-style-type: none"> 1. 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. 2. 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. 3. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. 	<ol style="list-style-type: none"> 1. Known as the Semantic Web, this describes sites where computers will generate raw data on their own without user interaction 2. 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. 3. 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. 4. Two major components of Web 3.0 are as follows: <ul style="list-style-type: none"> ■ Semantic Web ■ Web Services.

BENEFITS

2. Provide platform where users of the network need not to worry about the implementation or underlying technology at a very affordable cost and a very easy pickup time.
3. Concepts of Web 2.0 like blogging are some things that people do on a day to day basis and no new knowledge skills are required.
4. People are coming much closer to another and all social and geographical boundaries are being reduced at intense speed.
5. Increases the social collaboration to a very high degree and this in turn helps in

CHALLENGES

1. Provide platform Chances are there where there may be huge chance of data leak and confidentiality loss because there are usually no centrally mandated administrative services to take care of such things.
2. Malicious users somehow manage to perpetrate the social networks resulting in to penetration in privacy of individual users.

Student Feedback Questionnaire

The purpose of this questionnaire is to identify, using student feedback, about the quality of notes provided and also ways to improve:

Kindly encircle the numbers to be given for the notes:

	Poor	Average	Good	Excellent	Out-standing
Coverage of the syllabus	1	2	3	4	5
Presentation of topics	1	2	3	4	5
Coverage of modern/advanced topics	1	2	3	4	5
Usefulness of notes	1	2	3	4	5
Overall rating of the Notes	1	2	3	4	5

Please add any other comments you wish to make with regard to summary notes (The Catalyst) & bulk notes (Alchemist Series):

.....

.....

.....

.....

.....



Thank you for your assistance