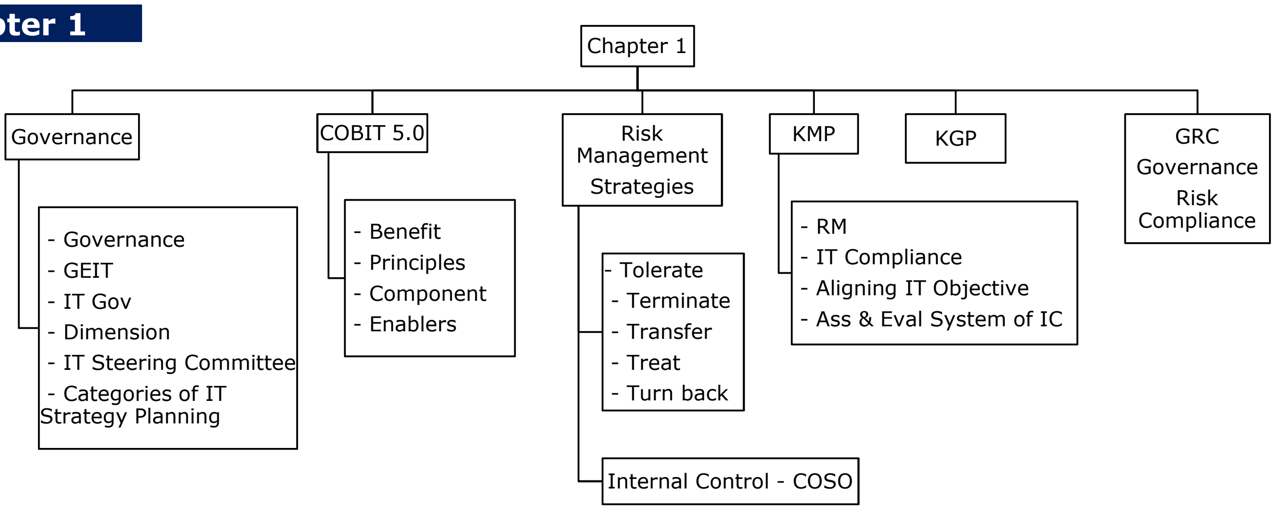
PAPER 6 - INFORMATION SYSTEMS CONTROL AND AUDIT

Chapter 1



Governance - Major Benefits of Governance [SIM-BPO] [May 19]

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

- **GEIT Governance - Benefits** [Legal MPDC]

GEIT is subset of Corp Govn. and facilitate implementation of framework of IS control within enterprises as relevant & encompassing all key areas

Legal	It confirms compliance with **legal** and regulatory requirements.
M	It ensure that the governance requirement for boards members are **met**.
P	It ensure that IT related **processes** are overseen effectively and transparently.
D	It ensure that IT related **decision** are made in line with the enterprises strategic & objectives.
C	It provides a **consistent** approach integrated & aligned with the enterprises governance approach.

- **KGP of GEIT** [EDM]

Evaluate the Governance System:	Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements;
Direct the Governance System:	Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT; and
Monitor the Governance System:	Monitor the effectiveness and performance of the enterprise’s governance of IT.

- **IT Governance - Benefits** [N14] [Memory - User Value Of TECBAM]

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

User	Increased **User** satisfaction with IT Services
Value	Increased **Value** delivered through ent IT
Of	More **optimal** utilization of IT resources
T	Improved **transparency** & understanding of IT's contribution to d business
E	IT becoming an **enabler** for change rather than an inhibitor
C	Improved **Compliance** with relevant laws, regulation and policies
B	**Better** Cost performance of IT
A	Improved **agility** in supporting business needs
M	Improved **mitigation** of IT related risks

IT Govn.	is -->	Subset of GEIT
GEIT	is -->	Subset of corporate governance

GEIT

GEIT me IT Gov hai

IT Governance

Enterprise Governance has two dimensions:

Particular	Business / Performance Governance	Conformance / Corporate governance
Provide	Forward Looking view, Proactive approach	Historic view
Focus	Its Business oriented, Focuses on strategy & value creation	Regulatory requirement
Monitored by	Board	Audit Committee
Objective	Helping board to make strategic decision, understand its risk appetite and its key performance	Increase shareholder value by enhancing eco. Performance

Some of Best practices of corporate governance: [RIM SEA]

R - Clear assignment of **responsibilities** & decision-making authorities;
I - Financial & managerial **incentives** to senior management & employees offered in an appropriate manner;
M - Establishment of a **mechanism** for interaction & cooperation among board of directors, senior management & the auditors
S - Implementing **strong** Internal Control systems;
E - Monitoring risk **Exposures** where conflicts of interest are likely to be particularly great. (E.g. Related party transactions);
A - **Appropriate information flows** internally (e.g. I.A. Report to BOD) & externally (e.g. XBRL to MCA).

- **IT Steering Committee - Key Functions** [Memory-SSC exam EDIT karke RDI me dalo] [RTP N19]

S	To Review & Approve **Standards**, policies and procedure
S	To Review the **Status** of IS plans & budget & overall IT performance
C	To Resolve **Conflict** in deployment of IT
E	To Establish size & scope of IT function & sets **priorities** within the scope
D	To Make **decision** on all key aspects of IT deployment & Implementation
I	To Facilitate **Implementation** of IT Security within Ent

T	To Ensure that long & short range plans of the IT dept are in **Tune** with ent objectives
R	To **Report** to the BOD on IT activities on a regular basis
D	To Review and approve major IT **deployment** projects in all their stages
I	To Approve & Monitor key projects by measuring result of IT projects in terms of **return on invst. etc**

- **Classification of Strategic Planning & Categories of IS Plans** [EIRA]

Ent. Strategic Plan Determine overall plan of enterprises It is Primary plan by top management.

IS Strategic Plan Should align with enterprises strategic plan enablers are;

1. Enterprises business strategy 2. How IT Support Business 3.Feasibility Study
4. Risk Assessment 5. Need for Senior management

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

IS Application Plan The information systems mgmt. can develop an information systems applications & facilities plan.

COBIT 5.0

Control Objectives for Information and Related Technology (COBIT) is a set of best practices for Information Technology management developed by Information Systems Audit & Control Association (ISACA) and IT Governance Institute. It Aligns IT objective with business objectives. Allows bridge the gap between control requirement technical issue & Business risks Enable clear policy development & goods practice of IT Control & Help org to increase value from IT

- **COBIT 5.0 - Benefits** [M18] [SOO PIC HER]

S	Provide generic framework which can be used by ent. of **all sizes**, whether commercial, not for profit or public sector
O	COBIT 5 help enterprises to create **optimal value from IT** by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
O	Comprehensive framework such as COBIT 5 enables enterprises in achieving their **objective** for governance & management of enterprise IT
PI	COBIT 5 enables clear **policy development** and good practice for IT management including **increased business user satisfaction.**
C	COBIT 5 supports **Compliance** with law, regulations & contractual requirements
H	COBIT 5 enables IT to be governed and managed in a **holistic manner** for the entire enterprise, taking full IT functional areas of responsibility, considering the IT related interests of stakeholders.
ER	COBIT 5 help to manage IT related **Risk** and **ensures** compliance, continuity, security and privacy.

- **COBIT 5 - Five Principle** [ME IAS]

M	Meeting stakeholders needs	Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits & d optimization of risk & use of resources
E	Covering enterprise end to end	COBIT 5 integrates governance of ent. IT into ent. governance. It covers all functions & processes within the enterprise; COBIT 5 does not focus only on the 'IT function'.
I	Applying Single Integrated frm.wrk	There are many IT related standards & best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single & integrated framework.
A	Enabling Holistic Approach	Efficient & effective governance & management of ent. IT require a holistic approach. It defines a set of enablers to support the implementation for GEIT. Enablers are anything that can help to achieve the objectives of the enterprise.
S	Separating governance from management	The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

• COBIT 5.0 - Component	[Nov 19] [CFPMM]
Control Objective	Provide a complete set of high level req considered by mgmt for effective control
Framework	Organize IT gov objectives & Good practices by IT domain
Process Descriptions	The process map to responsibility areas of plan, build, run and monitor
Mgmt Guidelines	Help assign responsibility, agree on objectives measures performance
Maturity Models	Assess maturity and capability per process and helps to address gaps

• COBIT 5.0 - Seven Enablers [M14] [IPS is COPS]

I Information is pervasive throught any org & include all info. produced & used by the ent.

P Principles, Policies and Framework are the vehicle to translate desired behaviour into practical guidance for day to day management

S People, Skills & Competencies r linked to people & r required for successful completion of all activities

C Culture, Eth. & Behaviour of Ind. & of ent very often understanding as success factor in governance

O Organisational Structure Are the key decision making entities in an enterprises

P Processes Describe an organised set of practices and activities to achieve certain objective

S Service Infrastructure and Applications includes infrastructure technology & application that provide the ent. with IT processing & Service.

Risk Management Strategies

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

• Internal Control as per COSO [N14] [Memory - EACCM]

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

Key Management Practices

• KMP for Risk Management

[Memory - CAMDAR]

C	Collect Data	Identify and collect relevant data to enable effective IT related risk
A	Analyse Risk	Develop useful info. to support risk decisions that take into account risk factors.
M	Maintain a Risk Profile	Maintain an inventory of known risks and risk attributes, including expected frequency and current control activities.
A	Articulate Risk	Provide info. on the current state of IT-related exposures & opportunities in a timely manner to all required stakeholders for appropriate response.
D	Define Risk mgmt action portfolio	Manage opportunities and reduce risk to an acceptable level as a portfolio.
R	Respond to Risk	Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

• KMP for IT Compliances

[May 19]

C	Identify External Compliance Requirement	On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
O	Optimize Response to External Requirement	Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.
C	Confirm External Compliance	Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements
A	Obtain Assurance of External Compliance	Obtain & report assurance of compliance & adherence with policies, principles,standards,procedures & methodologies.

[N18, Nov 19]

• KMP for Aligning IT Strategy with Enterprise Strategy [N19]

[DAD Conduct Strategic Communication]

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

[N14, N18]

• KMP for Assessing & Evaluating the system of Internal control in an enterprises

[Nov 19]

M	Monitor Internal Control	Continuously monitor the IT control environment and control to meet organizational objectives
R	Review Business Process Control Effectiveness	Review the operation of controls, including monitoring and test evidence. This provides the business with the assurance of control effectiveness.
P	Perform Control Self-assessment	Encourage management and process owners to take positive ownership of control improvement through self – assessment.
D	Identify & report control deficiencies	Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.

E	Ensure that assurance providers are independent & qualified	Ensure that the entities performing assurance are independent from the function, groups or organizations.
PAI	Plan Assurance Initiative	Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and sufficient knowledge of the enterprise.
SAI	Scope Assurance Initiative	Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
EAI	Execute Assurance Initiative	Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions and recommendations for improvement relating to external compliance and internal control system residual risks.

Key Metrics for Assessing Compliance Process

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

Raw

IT Strategy Planning	Strategic Planning	Mgmt Control	Operational Control

Exposure	Loss of Business	Violation of Privacy
	Loss of Reputation	Failure to perform the systems mission
	Loss of Resources	

• IS Audit

C	Confidentiality	Unauthorised access	
I	Integrity	Unauthorised modification	
A	Availability	Unauthorised withholding	(Sanket ki salary payslip, PAN Diya)
E	Effectiveness	Desired output aana chaiye as required	ISCA paper ke din ISCA yad aana chahiye
E	Efficiency	Desired output in response time	3 hrs me hi yaad aana chaiye,
C	Compliance	All policies and procedures should comply	Kisika paper dekhe bina yad aana chaiye

• Access Control Mechanism

Identification	ATM me amit tated
Authentication	PIN dalna
Authorisation	Rs. 20k daily limit

• Risk and Related Terms

Asset	Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees.
Vulnerability	Vulnerability is the weakness in d system safeguards that exposes the system to threats.
Threat	A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.
Risk	Risk is where threat and vulnerability overlap. at is, we get a risk when our systems have a vulnerability that a given threat can attack.

Counter Measure	An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure.
Attack	An attack is an attempt to gain unauthorized access to the system’s services or to compromise the system’s dependability.
Exploit	An exploit is the way or tool by which an attacker uses a vulnerability to cause damage to the target system.
Likelihood of the threat	It is the estimation of the probability that threat will succeed in achieving an undesirable event.
Exposure	An exposure is the extent of loss the enterprise has to face when a risk materializes.

- **GRC - Sample areas review by Internal Auditor** [SIR GEEEP]

S	Scope	G	Governance
I	Interpretation	E	Evaluate Risk Exposures
R	Risk Management	E	Evaluate Fraud and Fraud Risk
		E	Evaluate Enterprise Ethics
		P	Risk Management Process

- **GRC program implementation requires the following:**

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

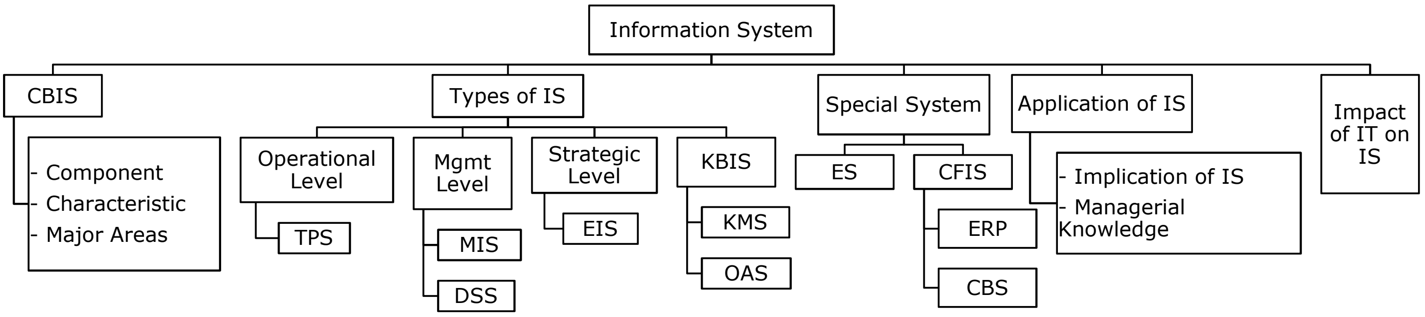
[N18]

- **GRC - Success of GRC can be measured by using following goals and metrics** [DIL toh TCF hai]

D Dashboard of overall compliance status & key issues to senior mgmt on real time basis as required
I Improvement in timely reporting of regular compliance issues & remediation measures
L The reduction of expenditure relating to legal, regulatory and review ares
T Reduction in overall time req for audit of key business area
C The reduction of redundant control and related time to execute
F The reduction in control failure in all key areas

- **Sample Areas of Review of Assessing and Managing Risks** [DROP QT Methodology]

D Different kinds of IT risks (technology, security, continuity, regulatory, etc.);
R Root cause analyses and risk mitigation measures;
O Risk management ownership and accountability;
P Defined and communicated risk tolerance profile;
Q Quantitative and/or qualitative risk measurement;
T Risk action plan and Timely reassessment.
Risk assessment methodology; and



• System **<u>Types / Classification</u>** HOBE

<u>Human Intervention</u>

Manual	Where data collection, manipulation, final reporting and maintenance are carried out obsoletely by human efforts, its called manual system
Auto-mated	Where computer, micro processor or micro cheap are used to carry out all the task mentioned above it is called automated system. No system is completely automated.

<u>Working / Output</u>

Deterministic:	It operates in predictable manner. The interaction among the parts is known with certainty. If input & Process is known, the next state of system can be given exactly without error. Eg. Computer program
Probabilistic:	It can be defined in terms of probable behaviour but certain degree of error is always attached to the Prediction of what system will do. Input & Output will be uncertain. Eg. Inventory System

<u>Interactive Behaviour</u>

Open	Open syst. Actively interact with their env. Such syst. regularly get input & give output to its env. These systems are also subject unknown inputs and outputs. Open systems are adaptable.
Closed	Close system doesn't interact with its environment. Close system don't get feedback from ext. envt. Such system are not adaptable

<u>Element</u>

Abstract	Orderly arrangement of interdependent ideas eg. Gods relationship with human.
Physical	Set of Interrelated elements which operate collectively to accomplish common goal eg. Business.

• Information

Mere collection of data is not information & mere collection of information is not knowledge

Data is processed and put into meaningful & useful context

Data consists of facts, values or results and information is result of relation between data

Information is d substances on which business decision are taken so quality of information determines quality of action. Information graphic, video, audio me bhi present kar sakte hai

• Attributes / Characteristics of Information [Memory - OMCAR ko TV pe FQCR hai]

Objective / Purpose	Information must have purpose / objectives at the time it is transmitted to a person / machine otherwise it is simple data.
Mode & Format	The mode of communication information to humans should be in such way that it can be easily understandable by the people and may be in the form of voice, text and combination of these two.
Current / updated	The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match

Availability	Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
Rate	The rate of transmission/reception of information may be represented by the time required to understand a particular situation. For example- the information available from internet site should be available at a click of mouse.
Transparency	It is essential in decision and policy making. For eg. total amount of advance does not give true picture of utilization of fund, deposit-advance ratio is more transparent information in this matter
Validity	It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
Frequency	The frequency with which information is transmitted or received affects its value. For example- the weekly reports of sales show little change as compared to the quarterly and contribute less for accessing salesman capability.
Quality	It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
Completeness & Adequacy	Should be complete & adequate in itself because only complete information can be used in policy making. (adequate refers to quantity of Information).
Reliability	It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
Value of Information	It is defined as difference between the value of the change in decision behaviour caused by the information and the cost of the information.

1. Computer Based Information System (CBIS)

When computer plays major role in decision making it is called CBIS

1. Component of CBIS --> Hardware Data Network
Software People

2. Characteristics of CBIS

All system works for **Pre-determined set of objectives** and system is designed accordingly.

All system will have Inter-related and Interdependent components. **No system works in isolation**

If one subsystem fails in most cases **complete system may fail.**

Sub-system works with another subsystem is called interaction

All sub-system work to **achieve common goal**. Goal of Individual subsystem is of lower priority than entire sys.

3. Major Areas of CBIS or Business application areas of Expert Systems

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

2. Type of Information System

Operational Level	Management Level	Strategic Level	Knowledge Level
TPS Operational Manager	MIS, DSS Middle Manager	EIS Senior Manager	KMS, OAS Knowledge & Data Workers

Transaction Processing System (TPS)

At the lowest level of management TPS is an Information system that manipulate data from business trans.

TPS will thus record & manipulate transaction data into usable information

Usually people using TPS are not in position to make decisions.

Basic Activities

C	Capturing data to obtain in files and database
P	Processing / Manipulating database using application software
G	Generating Information in tabular and detail format
P	Processing of queries from various quarters of the organisation

Component of TPS

Input	It involves the basic activities of capturing data, facilitating operations and authorising another operations. Eg. PO, Sales Invoice are physical evidence in TPS
Process	It involves use of journals & registers to provide permanent & chronological record of inputs.
Output	Any documents generated by system is output. Sum documents are both output and input. TPS generate tabular reports on daily basis.
Storage	Ledgers and files provide storage of data. Storage can be manual / computerised. Trail bal. and ledger stored for generating P&L, BS.

Features of TPS [Memory - LABS]

L	Large Volume of Data	As TPS is transaction oriented it generally consist of large volume of data and thus req greater storage capacity.
A	Automation of Basic operation	TPS aims at automating basic operation of enterprises. Since TPS plays critical role in day to day functioning, with the help of automation it can be effective and efficient.
B	Benefits are tangible	TPS is deterministic system. It reduces workload of the people associated with operations. Most of the benefits of TPS are tangible and easily measurable.
S	Source for other document	The output of TPS becomes input for MIS, DIS etc. Indirectly TPS also assist strategic decision making.

Management Information System (MIS)

MIS is computer based system that provide flexible & speedy access to accurate data

Integrated system designed for providing information to support management in decision making

MIS Support manger at different level to take strategic / tactical management decision to fulfil org. goals

Characteristics of Effective MIS [MM ka ac ICC-HS bank me hai]

M	Management Oriented	It means the efforts for development of MIS should start by understanding overall busi. objectives & involvement of management
M	Management Directed	Management should actively direct system development efforts. Mere one time involvement is not enough.
I	Integrated	Development of Information system should be an integrated one. Integrated system has capability of generating more meaningful information to management

C	Common Database	Common database can be accessed by management & thus elements the necessity of duplication in data storage, updating, deletion and protection. (har system ko a.virus dalne ki jarurat nahi)
C	Computerised	MIS can work without computer but use of computers increases effectiveness and efficiently of the system
H	Heavy Planning Element	MIS usually takes 1-3 years to get establish firmly within company. Therefor a HPE must be present in MIS development.
S	Concept of Subsystem	Which department to be included to what extent should be clear while developing an MIS.

Ye chaiye

<u>Myths/ Misconception</u>

Any CBIS is MIS
MIS is Study of Computer
MIS is Bunch of Technology
More data generation means more info.
Accuracy plays vital role in reporting
Any reporting is MIS
It is management techniques
It is file structure

<u>Pre-requisites of MIS</u> [Evolution MIS requires STD]

Evoln should be done [M14]
Control and Maintenance of MIS
Qualified System and Mgmt Staff
Support of Top Mgmt
Database is required

<u>Constraints in Operating MIS</u> Kyun nai mila

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

Limitations of MIS Superior DSS aaya tabhi MIS ke limitation mile [TURANT Quality Substitute]

T	MIS effectiveness decreases due to frequent changes in **top management**, organizational structure and operational team
U	MIS may not have requisite flexibility to quickly **update** itself with the changing needs of time, especially in fast changing and complex environment
R	The effectiveness of MIS is **reduced** in enterprise, where the Culture of Hoarding Information and not sharing with other holds
A	MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and **attitude** of members of organisations.
N	MIS is less useful for making **non-programmed decision**
T	MIS cannot provide **tailor-made** information packages suitable for the purpose of every type of decision made by executives
Quality	**Quality** output depends on quality of Input and Processing (Guj MP Tobacco launch)
Substitute	MIS is not **substitute** for effective management, which means that it cannot replace managerial judgement in making decision in different functional areas

Decision Support System (DSS)

DSS is type of computerised information system that supports business and organisational decision making activities. A properly designed DSS is an interactive based system intend to help decision makers to make decision. Ultimately Decision are taken by management in their somewhat personalised way.

Characteristics

DSS Support decision making at all level of mgmt
It should be Flexible and Adaptable
DSS Should be User friendly
DSS can be used for solving structured problems
It should be easy to use

It should be able to help Group in decision making
Focus on decision rather than data info
Should not be used for training purpose
Should be extensible and evolve over time
Used 4 decision making rather than 4 training purp.

Examples of DSS in Accounting

Cap Budgeting System	Companies require new tools to evaluate high technology investment decisions. Decision makers can use DSS to perform analytical techniques such as NPV /IRR. DSS can be used for financial analysis purpose.
Budgeting & variance analysis	Financial Institutions rely heavily on their budgeting system for controlling cost and evaluating managerial performance. DSS can generate monthly variance report for individual division to control cost.
Cost Accounting System	The health care industry is well known for its cost complexity. Managing cost in this industry require controlling of cost supplies, expensive machinery and technology. DSS application can help in such activities.
General DSS	GPPL can be used for analysing difference types of problem. DSS can be used to solve variety of problems such as cash flow, fund flow, small investment decisions.

Components: User; Database - Physical Level - Logical Level - External Level; Planning Lang - GPPL (Excel) (Structured + Unstr.) - SPPL (SAS,SPSS) (Unstructed Only); Model Base - Brain of DSS

Components	User	Database	Planning Lang	Model Base
		- Physical Level - Logical Level - External Level	- GPPL (Excel) (Structured + Unstr.) - SPPL (SAS,SPSS) (Unstructed Only)	- Brain of DSS

- **Difference**

Dimensions	DSS	Traditional MIS
	More useful for Unstructured problems	More useful for Structured problems
Orientation	Internal + External	Internal Information only
	Doesn't incl TPS limitations	Includes TPS limitation
Flexibility	Flexible	Less Flexible
Analytical capability	More analytical capability	Less analytical capability

Dimensions	EIS - Executive Information System	TPS - Transaction Processing System
Level of Management	For top	For lower staff
Nature of info	Online tools and analysis	Offline status reporting
Drill down facility	Available	Not available
Information format	Text with graphics	Tabular
Information source	More External less Internal	Internal

Executive Information System [EIS]

IT is tool that is designed to meet the special needs of top level managers. It provide direct online access to relevant information in useful and navigable format. It is DSS having online facility

DSS + CBIS

Characteristic of EIS

Top Executive ko decision lena tha uske pass **Time** bht kum tha isiliye vo DSS ke pass gya vaha pe usne **Internal & External** data ka **summarised** form mein **online analysis** kiya

Its CBIS that serves information need of top executives

EIS provides Rapid access to timely information and direct access to mgmt reports

EIS helps in decision making

EIS capable accessing both internal and external data

EIS enables users to Extract summary data without the need to learn query language

EIS provides extensive Online analysis tool like trend analysis, market conditions etc.

Characteristic of Types of Information used in Executive Decision making [FILL HIGH] [May 19]

Future Orientation	Strategic planning decision are made in order to made shape future events. As condition changes organisation and plan must also change. It is the executives responsibility to make sure that org. keep pointed towards future.
Informal Sources	Executives relies heavily on informal sources for key information. Eg. Lunch with the colleague may disclose sensitive information or competitors strategy.
Low level of details	Most important executive decisions are based on Broad Trends. Therefore executive decision contains low level of details information for making decisions
Lack of Structure (Unstructure)	Many of the decision made by executives are relatively unstructured. Eg. What should be the adv campaign ? How should we promote the product ?
High degree of Uncertainty	Executives work in decision space that is often characterised by Lack of precedent. The results are not scientifically predictable therefore high degree of uncertainty is always attached.

Principles [Nov 19] [BAEMAN]

B	It should be based on **Balanced view** of organisations objective
A	It should be **Adaptable** to changes in organisation needs
E	It should be **Easy to use,** understand and collect data
M	It should encourage mgmt and staff to **share Ownership** of org objectives
A	It should be **Available to everyone** in org^n. Confidential info should not form part of EIS in this case.
N	It should reflect everyone's contribution in **Fair and consistent** way.

Content

Purpose served by EIS

• KMS - Types of Knowledge [Nov 19]

Explicit Knowledge	Tacit Knowledge
It the knowledge which formalised easily and as a consequence it is easily available across organisation. Explicit knowledge is represented as spoken word, compile data, written material.	This knowledge is not available within organisation as it resides with individuals. It can be faith, value, believe and intuition based on individual experience. Its personnel, experimental, difficult to document and communicate.

Office Automation System

The application of computers to handle office activities is terms as office automation.

Types

TPS - Text Processing System	EDMS - Electronic Document Management Systems	EMCS - Electronic Messages Communication System Type: E-Mail, FAX Voice Mail	Teleconferencing / Video Conferencing System

Basic Activities [DDR office FC Road]

Document Capture	Documents originating from outside sources keep to be preserved like notes, handouts, charts etc.
Document Creation	This consist of preparation of document, detection, editing text etc.
Receipts & Distribution	This basically includes correspondence related activities
Filing, Search, retrieval	This is related to filing, indexing, searching which takes up significant time
Calculation	This include usual calculation function Eg. %, interest calculation etc.
Recording utilisation of recourses	It includes record keeping in respect to specific resource utilised by personal (prabhu roj likhega)

Benefits OAS [AIR^2]

Ensures **Accuracy** of information and smooth flow of communication
Improve communication within an organisation & between ent
Reduce cost of office communication both in term of time spent by executives & cost of comm. links
Reduce cycle time between preparation of messages and receipt of messages at the recipients end.

Feature of Email [Memory - ERP Online Economical] ***** [RTP N19]

Electronic Transmission	The transmission of messages with email is electronic and message delivery is very quick almost instant. The confirmation of transmission is also very quick.
Broadcasting & Rerouting	Email permits sending a message to large no. of target users Eg. Circulation of message across all branches, Lots of paper saving.
Portability	Physical location of sender and receiver is irrelevant. Email can be accessed by computer / smart phones / tablet equipped with the relevant communication hardware, software and link facilities
Online Develop. & Editing	Email message can be developed and edited online before the transmission. It eliminates the need for use of paper in communication
Economical	Email is most economical mode for sending messages. Email can be used not only for formal communication but also for informal communication with business enterprise.

Special System - 1. Expert System

Expert System is highly developed special DSS that utilise knowledge generally processed by an expert. Expert systems are software systems that imitate the reasoning process of human experts and provide decision makers with the type of advise they would normally receive from such expert systems

Benefit of Expert System

Expert system Preserve Knowledge that might be lost due to death, resignation, retirement of an expert
Expert system puts information in Active form
Expert System assist in Novice (Unique) Thinking the way experienced professional do.
Expert System are not subject to human fallings.
Expert systems can be effectively used as Strategic Tool in the area of marketing product etc. (Cancer Mch)

Need of Expert System

Expert labour is expensive and scarce

Handling only few factors at a time

Limitation of human information processing capability

[SAED.COM]

Potential Qualities/Properties/Qualification that appln should posses to qualify for Expert. Sys. dev.

Structure	Solution for unstructured problem will be structured.
Availability	One or more experts are capable of communicating how to solve the problem based on past experience for which expert system is applied
Expertise	Solution to problem the require efforts of expert. Only few poses knowledge, experience, techniques and intuition (aabhas).
Domain	The subject area of expert system relatively small and limited.
Complexity	Problem for which expert system available is complex which would not be easily handled by conventional information processing system.

Business Applications of Expert systems [Same as CBIS major areas]

Accounting and Finance Manufacturing Personnel General Business

Marketing

Special System - 2. Cross Functional Information System (CFIS)

It is an integrated information system which integrate various departments. It converts data into information as well as support management decision making process;

a. ERP - Enterprises Resource Planning

It is process management that allows organisation to use integrated systems and automate many back office functions. It integrate various departments such as accounts, finance, hr, etc.

Component of ERP - SPCM

Software component	This is most Visible components which consist of several module such as finance, hr, crm etc.
Process flow	This component illustrate the information flow from different module within ERP system. It make easier to understand how ERP work
Customer mind-set	Major components involves to make end user comfortable ERP system. User are always resistant to change. To adapt the changes is big challenge for any org.
Change management	In ERP implementation changes needs to be managed at several levels. It must be ensured that change should be authorised

Benefits of ERP

Process Standard & streamline business process into single integrated system.

Establish Uniform Process for sharing information

Improve Customer satisfaction by improving delivery time and quality

Faster collection based on better visibility of accounts

Reduce duplication in data entry Improves work flow and efficiency

Reduce inventory cost from better planning(Flipcart) Prepare Consolidated picture for organisation

• **Core Banking System**

Core represent Centralised Online Real Time Environment. CBS is banking services provided by network bank which has branches where customer may access their bank accounts & perform basis transactions from any branch

Que - Elements of CBIS

Opening a new account
Processing payments and cheques
Calculating Interest
Managing CRM activities
Process cash deposit and withdrawals
Servicing Loans
Establish criteria for min. balance, cash withdrawal etc
Maintaining record of all activities

• **Different managerial level in IT** [SMO]

Strategic Planning
Mgmt Control
Operational Control

• **Importance of Implication of Info System** [M15] [ICU me AAM]

I Innovative idea generation for solving critical problem
C Org is able to survive in competitive environment
U Past knowledge in unusual situation me utilize kar sakte hai
A It helps in decision making to achieve org goals
A IS is viewed as process, formulate a strategy of action
M IS helps in making right decision at right time ie just on time

• **To Operate IS effectively & efficiently, busi. mngr should have following knowledge;** [BID-FM]

B	Business Application	It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.
I	Information Technology	It includes operation, development and management of hardware, software, data management, networks and other technologies.
D	Development Process	It comprises how end users and Information Systems specialists develop and execute business/IT solutions to problems.
F	Foundation concept	It includes fundamental business & managerial concepts eg. 'what r components of system & their functions', or 'what competitive strategies are req.'.
M	Management challenges	It includes 'how the function and IT resources are maintained' and utilized to attain top performance and build the business strategies.

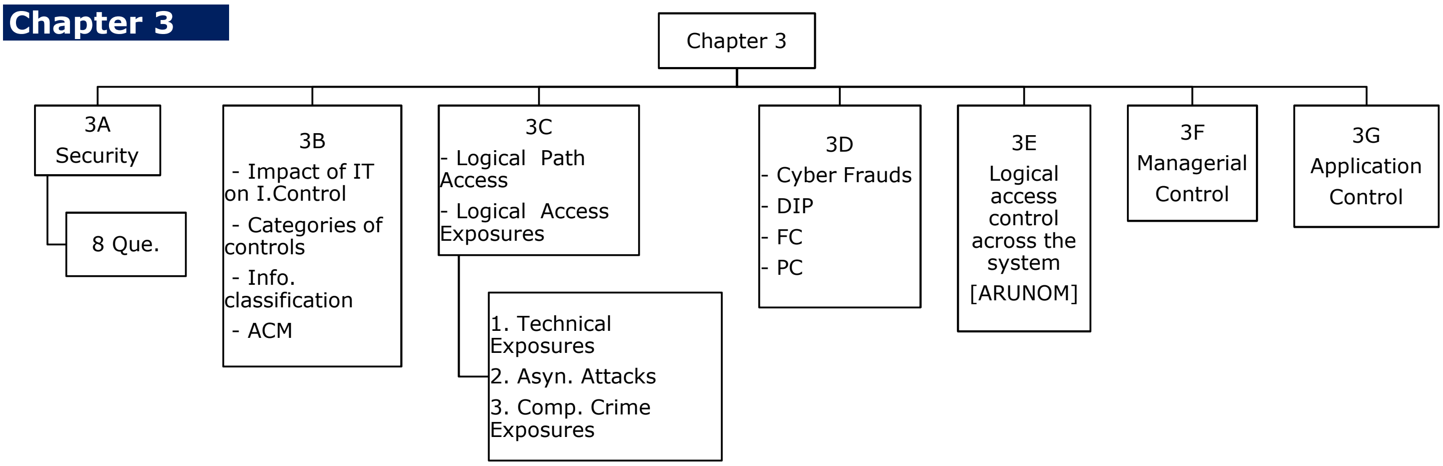
• **IT Tool - Critical for business growth** [Nov 19] [SBCB]

Software	DBMS, data mining, data warehousing ERP JIT
Business Website	CRM, advt cost
Computer system, scanner, lappy, printer	Video conference, time saving
Business Intelligence	EIS, HR, Budgeting tool
Internet and Intranet	No geographical boundary

• **Impact / Effect of IT** ***** [RTP N19]

On Info. System Chpt 2	On Internal Control Chpt 3	On Audit Chpt 6
E-Business Public Sector Financial Service Sector Wholesaling & Retailing Other	RAMDIP ki Dulhan	DOSA EDLI

Chapter 3



3A - Security

1. Degree of protection applied & required, reason for gap

These risks have led to a gap between the need to protect systems and the degree of protection applied.

a Widespread of technology
b Interconnectivity of Systems
c Devolution of management
d Elimination of distance, time, space as a constraints
e Unevenness of technological changes
f Electronic attacks are preferred over conventional physical attacks
g Attractiveness of conducting unconventional external factors

2. What Information is sensitive ?

Strategic Plan	Most of the organizations readily acknowledge that **strategic plans are crucial to the success of a company. But many of them fail to really make an effort to protect these plans.** For example: **a competitor learns that a company is testing a new product line in a specific geographic location.** The competitor removes its product from that location, creating an illusionary demand for the product.
Business Operations	**Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary.** This is the case when one company can provide a service profitably at a lower price than the competitor. A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor.
Finance	**Financial information, such as salaries and wages, are very sensitive and should not be made public.** While general salary ranges are known within industry, precise salary information can provide a competitive edge. This information if available can help competitive enterprises to understand and re-configure their salary structure accordingly.

3. Information Security Policy

An ISP is formal statement of the rules which give access to people to an orgs technology & information asset. It is statement of intent by management. Should be in written form & communication to everyone. It provide guidance to the people who build install and maintain information system. High level document. How organisation asset including information will be protected, managed & used will be defined by policy. **ISP should be flexible**

4. Tools to Implement Policy Standard Guidelines Procedures

5. Issues to be addressed [Memory - DRESS]

D	Definition of Information Security
R	Reasons why information security is important to the organization, and its goals and principles
E	Brief explanation of the security policies, principles, standards and compliance requirements,
S	Reference to supporting documentation
S	Definition of all relevant information security responsibilities

6. Members of Security Policy [Nov 19] [MTL]

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

7. Type of Information Security Policy

User Security Policies	These include User Security Policy and Acceptable Usage Policy.
1. User security policy 2. Acceptable usage policy	Policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers & System Owners. This sets out the policy for acceptable use of email, Internet & other IT resources.
Organisation Policy	These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.
1. Organisational Information Security Policy 2. Network & System Security Policy 3. Information Classification Policy	Policy sets out d Group policy for the security of its information assets & Info. Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it's the main IT security policy document. This policy sets out detailed policy for system and network security and applies to IT department users. This policy sets out the policy for the classification of information.
Condition of Connections	This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

8. Components of the Security Policy

Purpose and Scope of the Document and the intended audience;
The Security Infrastructure;
Security policy document maintenance and compliance requirements;
Incident response mechanism and incident reporting;
Security organization Structure
Inventory and Classification of assets;
Description of technologies and computing structure;
Physical and Environmental Security;
Identity Management and access control;
IT Operations management;
IT Communications;
System Development and Maintenance Controls;
Business Continuity Planning;
Legal Compliances;
Monitoring and Auditing Requirements.

3B - 4 Questions

Critical control lacking in a computerized environment are as follows:

Lack of management understanding of IS risks and related controls;
Absence or inadequate IS control framework;
Absence of weak general controls and IS controls;
Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;
Complexity of implementation of controls in distributed computing environments and extended enterprises;
Lack of control features or their implementation in highly technology driven environments;
Inappropriate technology implementations or inadequate security functionality in technologies implemented.

1. Impact of IT on Information Control

[RAMDIP ki Dulhan]

R	Physical Control over Assets and Records	Physical control over access and records is **critical in both manual systems and computer systems. In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets.** Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site - namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.
A	Authorisation Procedures	In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
M	Adequate Mgmt Supervision	This refers to **review of specific work by a supervisor** but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location.
D	Segregation of Duty	Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. Examples of Segregation of Duties are as follows: • Systems software programming group from the application programming group; • Database administration group from other data processing activities; • Computer hardware operations from the other groups; • Systems analyst function from the programming function; • Physical, data, and online security group(s) from the other IS functions;
I	Independent Checks on Performance	In manual systems, **independent checks are carried out because employees are likely to forget procedures, make genuine mistakes,** become careless, or intentionally fail to follow prescribed procedures. **If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures** in the absence of some other type of failure like hardware or systems software failure.
P	Competent & Trustworthy Personnel	Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.
D	Delegation of Authority and Responsibility	A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

2. Categories of Information System Control

a) Based on Objectives

	Purpose	Characteristics [VPN]	Examples
Preventive	Designed to prevent errors, bug, Omission or Fraud Both manual & computerised	V- Clear understanding of Vulnerability of assets P- Understanding probable threats N- Provision for necessary Control for probable threat from materializing	Employing Qualified Persons Segregation of Duties Access Control Vaccination against deseases Documentation Training & retaining of staff Edit Check in an Application Firewall
	Purpose	Characteristics [MIS U]	Examples
Detective	Designed to detect error, omission or malicious Report on Occurrence	M - Establish Mechanism to refer reported unlawful activity I - Interaction with preventive control S - Surprise check by supervisor U - Clear understanding of lawful activities	Hash totals Past due accounts report Instrusion detection system Check point in production job Echo control in telecommu. Cash count and Bank Reco Error massage over tape Duplicate checking
	Purpose	Characteristics [Identify M2RF Error]	Examples
Corrective	Designed to reduce the impact & correct the error once detected BCP is Corrective Control	I- Identify cause of the problem M- Minimizing impact of threat M- Modifying the processing system to minimize future occurrence R- Providing remedy to the problem discovered by detective controls F- Getting feedbk from det and prev E- Correcting error arising from problem	1. Backup procedure 2. Change Input Value to an application system 3. Re-run Procedure 4. Contingency Planning

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

b) Based on Nature of IS Resources

Physical Access Control Logical Access Control Environmental Control

c) Based on Audit Function

Managerial Controls System Controls

3. Information Classification [May 19] [Memory - High TIPP]

Top Secret	Highest	Highly sensitive internal information e.g. pending mergers/ acquisitions; investment strategies; that could seriously damage the organization if such information were lost / made public. Information classified as Top Secret information has very restricted distribution & must be protected at all times.
Highly Confidential	Very High	Information that, if made public or even shared around the organization, could seriously impede the organization’s operations & is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc., patient's medical records and similar highly sensitive data. Such information should not be copied / removed from the organization’s operational control without specific authority.
Proprietary	High	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only.

Internal Use only	Moderate	Information not approved for general circulation outside the org. where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports.
Public Documents	Minimum	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should minimal.

4. Access Control Management

An Access Control Mechanism is associated with identified, authorized users the resources they are allowed to access and action privileges. The mechanism processes the users request for Real time Memory and Virtual Memory resources in three steps:

Identification	First and foremost, the users have to identify themselves
Authentication	Secondly, the users must authenticate themselves and the mechanism must authenticate itself. The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request.
Authorisation	Third, the users request for specific resources, their need for those resources and their areas of usage of these resources. There are two approaches • In a **ticket-oriented approach** to authorization, the access control mechanism assigns users, a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user. • In a **list-oriented approach**, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource. This mechanism operates via a column in the matrix.

3C - Logical Access Issues and Exposures

• Logical Path Access [Do2T]

a. Dial up Paths	**Using a dial up port, user at one location can connect remotely to another computer present at an unknown location via a telecommunication media.** A modem is a device, which can convert the digital data transmitted to analog data. **Thus, the modem can act as an interface between remote terminal and the telephone line.** Security is achieved by providing a means of identifying the remote user to determine authorization to access.
b. Online Terminal	To access an online terminal, a user has to provide a valid login-ID and password. If additional authentication mechanisms are added along with the password, it will strengthen the security.
Operator Console	The operator console is one of the crucial places where any intruders can play havoc. Hence, access to operator console must be restricted. This can be done by: o Keeping the operator console at a place, which is visible, to all? o By keeping op. console in a protected room accessible to selected personnel.
c. Telecommunication Network	In a Telecommunication network, **a number of computer terminals, Personal Computers etc. are linked to the host computer through network / telecommunication lines.** Whether the telecommunication lines could be private or public, security is provided in the same manner as it is applied to online terminals. **Each of these routes has to be subjected to appropriate means of security in order to secure it from the possible logical access exposures.**

- **Logical Access Exposures**

Technical Exposures	Asynchronous Attacks	Computer Crime Exposures
[Worm ne ghode pe baithke round round karke Data ko salami di & Door pe Bomb feka]		Impact of Cyber Frauds on Organisation [SLSL ka BF]
Worm Trojan Horse Rounding Down Data Diddling Salami Techniques Trap Doors Bomb	Data Leakage Wire tapping Subversive Threats - Invasive - Read & Modify data - Inductive - Read only Piggybacking Denial of Service	Sabotage Legal Repercussions Spoofing Loss of Credibility Blackmail Financial Loss

a. Technical Exposures

Worm	A worm does not require a host program like a Trojan to relocate itself. Thus, **Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses.** Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.
Trojan Horse	These are malicious programs that are hidden under any authorized program. The concept of Trojan is similar to bombs but a computer clock / particular circumstances do not necessarily activate it. A Trojan may: o Change or steal the password or May modify records in protected files or o May allow illicit users to use the systems.
Rounding Down	This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.
Data Diddling	Data diddling involves the change of data before or after they are entered into the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.
Salami Techniques	This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, 456.39 becomes 456.40, while in the Salami technique the transaction amount 456.39 is truncated to either 456.30 or 456.00, depending on the logic.
Trap Doors	Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.
Bomb	Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. Since, these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.

b. Asynchronous Attacks [N18]

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

Data Leakage	Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

Subversive Threats:	An intruder attempts to violate the integrity of some components in the sub-system. Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways. An intruder attempts to violate the integrity of some components in the sub-system by: **o Invasive tap:** By installing it on communication line, s/he may **read and modify data.** **o Inductive tap:** monitors electromagnetic transmissions & allows data to **be read only.**
Wire-tapping	This involves **spying on information being transmitted over telecommunication network**
Piggybacking	This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and he user and modifying them or substituting new messages.
Denial of Service	This is initiated through terminals/ microcomputers that are **directly/ indirectly connected to the computer.** Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACK to complete the connection.

c. Computer Crime Exposures [Nov 19]

Computers can be utilized both constructively and destructively. Computer systems are used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made.

Sabotage	People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization or for their intemperance.
Legal Repercussions	An organization has to adhere to many laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures. The IS auditor should take legal counsel while reviewing the issues associated with computer security.
Spoofing	A spoofing attack involves forging one's source address. Spoofing occurs only after a particular machine has been identified as vulnerable. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.
Loss of Credibility	In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
Blackmail	By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
Financial Loss	Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

[MR. LAL ka Data Transmission]

- **Remote and distributed data processing application can be controlled in many ways;** [M15]

M To prevent the unauthorized user's access to the system, **there should be proper control mechanisms** over system documentation and manuals.

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

L Terminal & computer operations **at remote locations should be monitored** carefully & frequently for violations.

A Applications that can be remotely accessed via modems & other devices should be **controlled appropriately.**

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

Data **Data transmission over remote location should be controlled**

3D - Cyber Frauds, DIP, Financial Control, Personal Control

• Type of Cyber Frauds	**Pure Cyber Frauds:** Frauds, which exists only in cyber world. They are borne out of use of technology. For example: Website hacking.
	Cyber Enabled Frauds: Frauds, which can be committed in physical world also but with use of technology; the size, scale & location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

• Techniques to commit Cyber frauds

Data Diddling
Piggybacking
Data Leakage
Denial of Service (DoS) Attack
Round Down
Trap Door
Internet Terrorism
Hacking

• Impact of cyber frauds on Enterprises [N14]

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.
Loss of credibility	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.
Sabotage	The above situation may lead to misuse of such information by enemy country.

• Major Cyber Attacks - Types [N18]

Phishing	It is the act of attempting to acquire information such as usernames, passwords, & credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors / 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.
Spam	E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as spam.
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 threat	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.

• Data Integrity Policy [M18] [DD SV - B]

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

• Financial Control [M14] [ABCD-IM-Safe]

Authorisation	This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.
Budget	These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
Cancellation of documents	This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid"/ "processed" stamp/ punching a hole in the document.
Dual Control	This entails having two people simultaneously access an asset. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
Input / Output verification	This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
Safekeeping	This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
Sequentially numbered documents	These are working documents with pre-printed sequential numbers, which enables the detection of missing documents.

• Personal Computer Control

Related Risk

Personal computers are **small in size and easy to connect and disconnect**, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.
PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
Segregation of duty is not possible, owing to limited number of staff.
Due to vast number of installations, Staff mobility is higher & it becomes source of leakage of information.
The operating staff may not be adequately trained.

Remedy

Physically locking the system

Uses of antimalware software

Proper logging of equipment shifting must be done

Centralised purchase of hardware and Software

Standards set for developing, testing and documenting

The use of personal computer and their peripheral must have controls

3E - Logical Access Control across the System

[Memory - ARUNOM]

A	R	U	N	O	M
Application & Monitoring System Access Control	User Responsibility	User Access Mgmt Control	Network Access Control	Operating System Access Control	Mobile Computing
MECSI		RUPA	FERSaN	LAL DUPATTA	

Application and Monitoring System Access Control [MECSI]

M	Monitor System Use	Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. **The log files are to be reviewed periodically and attention should be given to any gaps in these logs.**
E	Event Logging	In Computer systems, **it is easy & viable to maintain extensive logs for all types of events. An intruder may penetrate the system by trying different passwords and user ID combinations.** The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
C	Clock Synchronisation	Event logs maintained across an enterprise network plays a significant role in correlating an event & generating report on it. Hence, need for synchronizing clock time across the network as per a standard time is mandatory.
S	Sensitive System Isolation	Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. (German Client with Indian CA firm, their timing)
I	Information Access Restriction	The access to information is prevented by application specific menu interfaces, which limit access to system function. **A user is allowed to access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users, For example, read, write, delete, & execute.**

User Responsibilities

Password Use	Mandatory use of strong passwords to maintain confidentiality.
Unattended user equipment's	Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password, and should not leave it accessible to others.

User Access Management Control [RUPA]

User Registration	**Information about every user is documented.** The following questions are to be answered: Why is the user granted the access?, Has the data owner approved the access?, and Has the user accepted the responsibility? etc.
User Password Management	Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, & reissue of password are password management functions. Educating users is a critical component about passwords, & making them responsible for their password.
Privilege Management	Access privileges are to be **aligned with job requirements and responsibilities**. For example, an operator at the order counter shall have direct access to order processing activity of the application system. **However, misuse of such privileges could endanger the organization's information security.** These privileges are to be minimal with respect to their job functions.
Review of User access rights	A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.

Network Access Control [FERSaN]

F	Firewall	Organizations **connected to the Internet and Intranet** often implements an electronic firewall to insulate their network from intrude. **A Firewall is a system that enforces access control between two networks.** Only authorized traffic between the organization & the outside is allowed to pass through the firewall.
E	Enforced path	Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g., **internet access by employees will be routed through a firewall and proxy.**

R	Recording Transaction Log	An intruder may penetrate the system by trying different passwords & user ID combinations. All incoming & outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, Time of the access & the terminal location.
S	Segregation of Network	Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office, this network is to be isolated from the internet usage service
N	Policy on use of Network Service	An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.

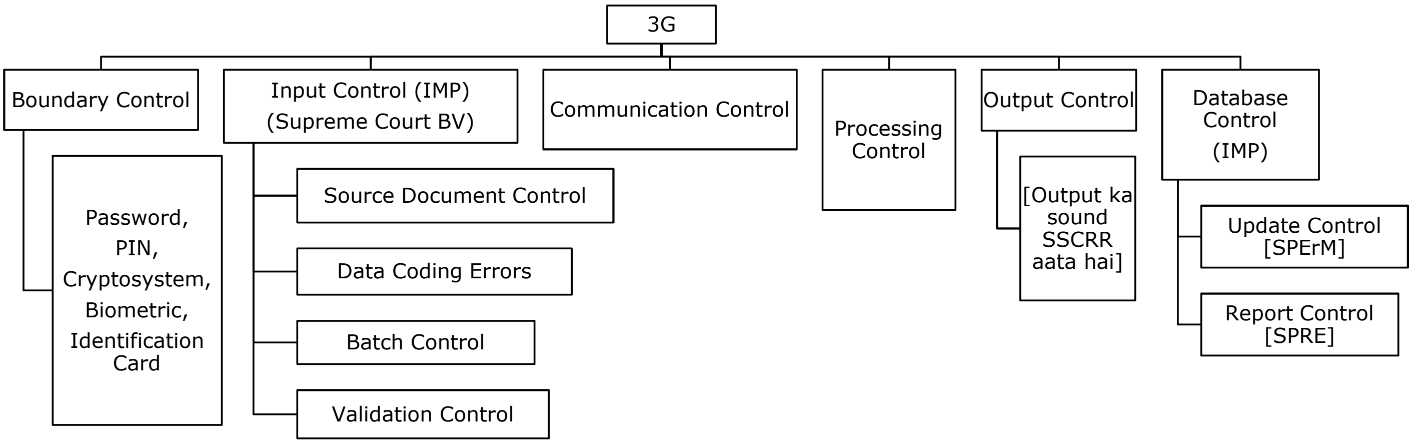
Operating System Access Control [Nov 19] [LAL DUPATA]

L	Limitation of connection time	**Define the available time slot. Do not allow any transaction beyond this time period.** For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.
A	Automated terminal identification	This will help to ensure that a **particular session** could only be **initiated from a particular location or computer terminal.**
L	Terminal log-in procedures	**A log-in procedure is the first line of defence against unauthorized access.** When the user initiates the log-on process by entering user-id and pass., the system compares the ID and pass. to a database of valid users. If the system finds a match, then log-on attempt is authorized.
D	Duress alarm to safeguard users	If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
U	User Identification and Authentication	The users must be identified & authenticated in a fool proof manner. Depending on risk assessment, more stringent methods like Biometric Authentication / Cryptographic means like Digital Certificates should be employed.
P	Password Management System	An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
A	Access Token	If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
T	Terminal time out	Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
A	Access Control List	When a user attempts to access a resource, the system compasses his/ her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

3F - Managerial Control

1	Top Managerial Control	Planning Organizing Leading Controlling
2	System Development Management Control	Concurrent Post implementation Audit General Audit
3	Programming Management Control	Planning Control Design Coding Testing O&M
4	Data Resource Management Control Definition Control--> Backup Control -->	Access Control Update Control Quality Control Dual Recording of Data Logging Input transactions Periodic dumping of data Logging Changes to data
5	Quality Assurance Control	
6	Security Administration Control	
7	Operational Management Control	

3G - Application Control



1	Boundary Control	Comprises the components that establish interface between the user & the system.

Password	PIN	Biometric	Cryptosystem	Identification Card

[Supreme court ke judge ki BV]

2	Input Control	Comprises the components that capture, prepare, and enter commands and data into the system.

Source Document Control	Use pre-numbered source documents:	Source documents should come pre-numbered from the printer with a unique sequential number on each document. Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.	
	Use source documents in sequence	Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site.	
	Periodically audit source documents	Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.	
Data Coding Errors	Transcription Errors	Addition Error	occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
		Truncation Error	occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
		Substation Error	are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.
	Transposition Error	Single Transposition	occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.
		Multiple Transposition	occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.
Batch Control	Physical Control	These controls are groups of transactions that constitute a physical unit. For example - source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.	
	Logical Control	These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.	

Validation Control	Field Interrogation	Limit Check Check Digit	Picture Checks Arithmetic Checks Valid Code Checks
	Record Interrogation	Reasonableness Check	Whether the value specified in a field is reasonable for that particular field?
		Sequence Check	If physical records follow a required order matching with logical records.
		Valid Sign	The contents of one field may determine which sign is valid for a numeric field.
	File Interrogation [VID ka IFC code]	Version usage	Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
		Internal & External Labelling	abeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labelling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labelling is more important.
		Data File Security	Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.
		Before & After Image Logging	The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.
		File updating & maint. authorisation	Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.
		Parity check	When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

3	Communication Control

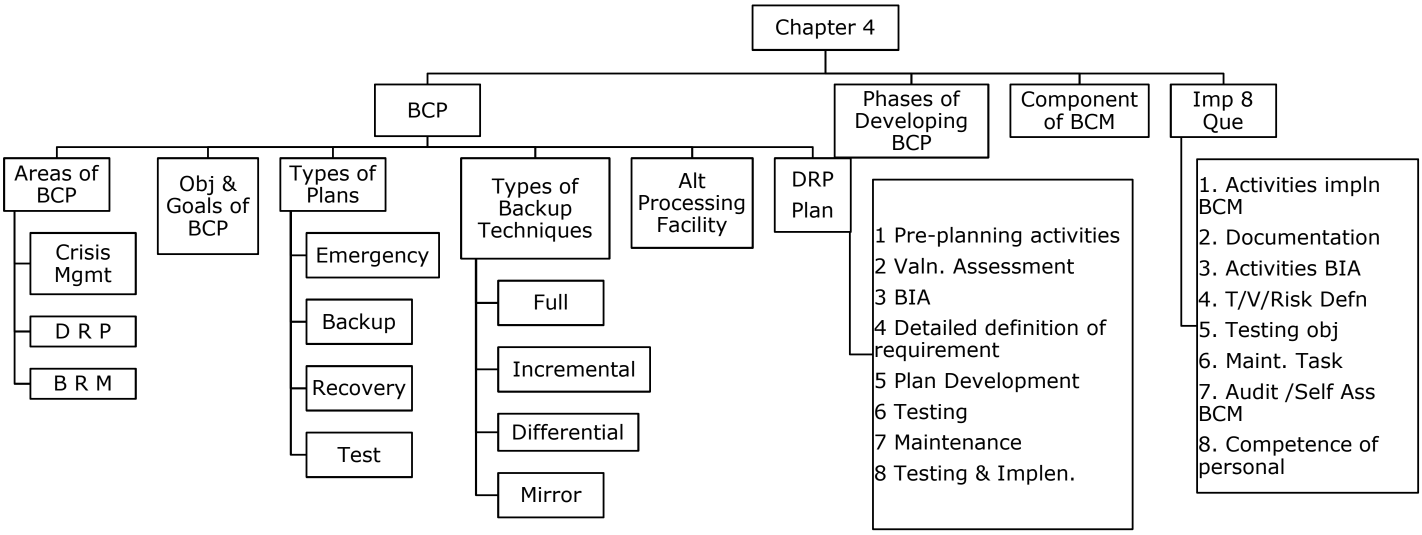
4	Processing Control

[Output ka sound SSCRR aata hai]

5	Output Control	
S	Storing & Logging of Sensitive & Critical Forms	Pre-printed stationery should be stored securely to prevent unauthorized destruction/ removal & usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.
S	Spooling	Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to continue working, while the print operation is getting completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk.
C	Control Over Printing	Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
R	Report Distribution & Collection Control	Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced.
R	Retention Control	Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored.

6	Database Control	[Database ka SPErM update karke Report pe SPRE maro]
Update Control [SPErM]	Seq. check between Trans & master files	Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records. If errors, in this stage are overlooked, it leads to corruption of the critical data.
	Process multiple trans for a single record in correct order	Multiple transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centres). Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.
	Ensure all records on files are processed	While processing, the transaction file records mapped to the respective master file, and the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.
	Maintain a suspense account	When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account. A non-zero balance of the suspense accounts reflects the errors to be corrected.
Report Control [SPRE]	Standing Data	Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Any changes or errors in these tables would have an adverse effect on the organizations basic functions. Periodic monitoring of these internal tables by means of manual check / by calculating a control total is mandatory.
	Print Run to Run Control Total	Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.
	Print Suspense A/c entries	Similar to the update controls, the suspense account entries are to be periodically monitors with the respective error file and action taken on time.
	Existence Control	The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup strategies are implemented using prior version and logs of transactions or changes to the database. Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

Chapter 4



Business Continuity Planning

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

• BCP - Area

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

• Objective of BCP

[Complexity Provide Success watch DDLj]

Complexity	Reduce the **complexity** of the recovery effort
Provide	**Provide the safety** and well being of people on the premises at the time of disaster
Success	**Establish Mgmt Succession** and emergency powers
D	**Minimize Duration of serious disruption** to operation and resource
D	**Minimize immediate Damage** and Losses
L	**Identify Critical Lines** of business process
	Continue critical business operations

• Goals of BCP

[Weak CCD]

Weak	**Identify weakness** and implement a disaster prevention program
C	Facilitate effective **co-ordination** of recovery task
C	**Reduce the complexity** of the recovery effort
D	**Minimize duration** of Serious disruption to business operation

Business Continuity Life Cycles:

Risk Assessment

Determination of Recovery Alternatives

Recovery Plan Implementation

Recover Plan Validation

Parameter considered in Business Categorization :

Loss of Revenue

Loss of Reputation

Loss of Productivity

Types of Plan

[EBRT]

Emergency Plan	The emergency plan specifies the **actions to be undertaken immediately when a disaster occurs.** Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. 1. The plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'. 2. The plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. 3. Any evacuation procedures required must be specified. 4. Return procedures (e.g., conditions that must be met before the site is considered safe)
Backup Plan	The backup plan specifies the **type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources,** site where these resources can be assembled and operations restarted, **personnel who are responsible for gathering backup resources and restarting operations,** and a time frame for recovery of each system. **The backup plan needs continuous updating as changes occur.**
Recovery Plan	The backup plan is intended to **restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities.** Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken.
Test Plan	The purpose of the test plan is to **identify deficiencies in the emergency, backup, or recovery plans** or in the preparedness of an organization and its personnel for facing a disaster. Periodically, test plans must be invoked.

Type of Backup Techniques

[N14]

1. Full Backup

A Full Backup **captures all files on the disk** or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed.	
Advantages	1. Restores are fast & easy to manage as d entire list of files & folders r in one backup set. 2. Easy to maintain and restore different versions.
Disadvantages	1. Backups can take very long as each file is backed up again every time d full backup is run. 2. Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

2. Incremental Backup

An Incremental Backup **captures files that were created or changed since the last backup**, regardless of backup type. **The last backup can be a full backup or simply the last incremental backup.** With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.	
Advantages	1. Much faster backups. 2. Efficient uses of storage space as files are not duplicated. Much less storage space used compared to running full backups and even differential backups.
Disadvantages	1. Restores are slower than with a full backup and differential backups. 2. Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore .

3. Differential Backup

Differential backups **fall in the middle between full backups and incremental backup.** A Differential Backup stores files that have **changed since the last full backup.** With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.

Advantages	1. Much faster backups then full backups. 2. More efficient use of storage space then full backups since only files changed since the last full backup will be copied on each differential backup run. 3. Faster restores than incremental backups.
Disadvantages	1. Backups are slower then incremental backups. 2. Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup. 3. Restores are slower than with full backups. 4. Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.

4. Mirror back-up

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

Advantages	1. The backup is clean and does not contain old and obsolete files.
Disadvantages	1. There is a chance that files in the source deleted accidentally, by sabotage or through a virus may also be deleted from the backup mirror.

***** [RTP N19]

Particular	Full	Incremental	Differential
Tasks	Capture all files	Capture file that created or Changed since last back -up	Stores file that have Changed since last full backup
Speed (Stage 1)	Slower 3	Faster 1	Faster than Full Slower than Incre. 2
Storage (Stage 2)	High. High 3	Less than F/D dono se kam 1	Efficient use than F Not Eff. use than I 2
Restore (Stage 3)	Sabse Fast. Fast.. 1	Slower than F/D, Complicated 3	Faster than Incre. Slower than Full 2
Example			
Jan	01 Jan to 31 Jan	01 Jan to 31 Jan	01 Jan to 31 Jan (Last Full)
Feb	01 Jan to 28 Feb	01 Feb to 28 Feb	01 Feb to 28 Feb
Mar	01 Jan to 31 Mar	01 Mar to 31 Mar	01 Feb to 31 Mar
Apr	01 Jan to 30 Apr	01 Apr to 30 Apr	01 Feb to 30 Apr

Type of Backup Site / Alternative Processing Facility

* Based on Recovery Time *

Hot site	Cold site	Warm Site
1. If **Fast recovery is critical** for organisation	1. If organisation can **tolerate some downtime**, then its appropriate	1. **Intermediate level** of backup
2. All hardware and operational **facilities are available**	2. All facilities need to install main-fram system eg. Raised flooring, AC, Power consm. Line	2. Its **cold site having addn. facility** of hardware
3. **Software also be installed**	3. Its **low cost** option	3. **Moderate recovery time** & moderate cost
4. Its **expensive** option to maintain.		

* Based on Agreement *

Reciprocal agreement	Third Party Site
i) Two or more org might agree to provide backup facility to each other in the event of one suffering disaster	i) It is used for backup & recovery purpose, security administrator must ensure that contract cover following issues;
ii) This backup option is cheap but both parties should have additional facility	[Nov 19] [SNPP CD nahi mil rahi ? What?] S - How soon site will be available subseq to disaster N - No. of org that can use site concurrently P - Priority to be given to concurrent users in the event of common disaster P - The period during which site can be used C - Condition under which site can be used D - Procedure to ensure security of companies data being accessed by others What - What control & Addn facility will be in place and working at off-site facility.

Disaster Recovery Plan

1 Resumption procedures, which describe the actions to be taken to return to normal busi. operations.

2 A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.

3 Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.

4 The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

5 Contingency plan document distribution list.

6 Detailed description of the purpose and scope of the plan.

7 Contingency plan testing and recovery procedure.

8 List of vendors doing business with the org, their contact numbers & address for emergency purposes.

9 Checklist for inventory taking and updating the contingency plan on a regular basis.

10 List of phone numbers of employees in the event of an emergency.

11 Emergency phone list for fire, police, hardware, software, suppliers, customers, back -up location, etc.

12 Medical procedure to be followed in case of injury.

13 Back-up location contractual agreement, correspondences. · Insurance papers and claim forms.

14 Primary computer centre hardware, software, peripheral equipment and software configuration.

15 Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.

16 Alternate manual procedures to be followed such as preparation of invoices.

17 Names of employees trained for emergency situation, first aid and life saving techniques.

18 Details of airlines, hotels and transport arrangements.

Phases of Developing BCP

1	**Pre-planning activities**
	• Methodology for Developing BCP [SAAS-FOUR]
S	Development of a policy to **support** recovery programs.
A	Obtaining committement from approp mgmt to support and participate
A	Conduct **user awareness session** to educate management
S	**Senior mgmt to participate** in business continuity program
F	**Focusing appropriately** on disaster prevention and impact minimization
O	Policy should define scope and out of scope. **Obtain an understanding** of existing and projected system environment of an organisation.
U	Developing a Business continuity plan that is **understandable, easy to use & maintain**
R	**Defining recovery requirement** from the perspective of business functions
2	**Vulnerability Assessment and General Definition of Requirements**
	This phase will include the following key tasks: [SIR ki DRP Develop Team]
S	A **thorough Security Assessment of System** need to be conducted. It should be continuos activity.
I	The Security Assessment will enable the project team to **improve any existing emergency plans** and to implement required emergency plans where none exists.
R	**Report findings** and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be taken in a timely manner.
D	**Define the scope of the planning effort.**
RP	Analyze, recommend and purchase **recovery planning** and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
Dev	**Develop a Plan Framework.**
Team	**Assemble Project Team** and conduct awareness sessions.
	Identify vulnerability in following areas- Physical security; systems development & maintenance; database security; data & voice communications security; software security; insurance; application controls; and personal computers.
3	**Business Impact Analysis** BIA of all busi. units enable project team to identify critical system, assess the impact & recovery time
4	**Detailed Definition of Requirements** During this phase, a profile of recovery requirements is developed.
5	**Plan Development** During this phase, recovery plans components are defined and plans are documented. Recovery standards are also developed during this phase.
6	**Testing Program** The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established & alternative strategies are evaluated. On-going testing program should be established.
7	**Maintenance Program** Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environment. Existing change management processes are revised. Where change management doent exist, change management procedures will be recommended & implemented.
8	**Initial Plan Testing and Plan Implementation** Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made.

BCM

It is high level policy which guide to make systematic approach for disaster recovery, to bring awareness to test & review BCM

• BCM Policy - Advantages [PATI]

P Has **planned response to disruptions** which can contain the damage

A Is able to **proactively assess** the threat scenario and potential risks;

T Is able to demonstrate a response through a process of **regular testing and trainings.**

I Minimize the **impact** on the enterprise;

• BCM Policy - Objectives [AKIRA]

A	**Identify critical services & activities** including key products, Develop plan to ensure continuity of critical services following business disruption, may arise due to loss of facility, system failure etc.
K	Plans will be developed to **ensure continuity of Key services** delivery following business
I	Development / **Innovation of IMP** & BCP can be managed
R	IMP & BCP are subject to **on-going testing, revision & updating**
A	Planning & Management responsibility are **assigned to member of senior management team**

Component in Details: [Nov 19]

BCM – Process	The management process enables the business continuity, capacity & capability to be established and maintained. The capacity & capability are established in accordance to the requirements of the enterprise.
1. BCM - Information Collection Process	The activities of assessment process do the prioritization of an ent's products & services and the urgency of the activities that are required to deliver them.
2. BCM - Strategy Process	Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level within an acceptable timeframe for each product or service.
3. BCM – Development & Implementation Process	Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
4. BCM – Testing and Maintenance Process	BCM testing, maintenance and audit testify the enterprise BCM to prove its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.
5. BCM – Training Process	Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders to cope with minimum disruptions and loss of service.

• Component of BCM [May 19] [Memory ISDTT]

BCM Process	Major Activities [CID Trump]		Documentation
BCM - Information collection process	BIA [CITLRI]		
BCM - Strategy process			
BCM - Development and Implementation			
BCM - Testing and maintenance process	Testing objective [BMCC Backup]	Maintenance of BCP [I ki Responsibility]	Audit of BCM [RASMI]
BCM - Training process	Comp of Program		

BCM - Process

• Activities in Implementation of BCP [CID arrested TRUMP]

C **Managing costs** and benefits associated

I Engaging and **involving all stakeholders**

D Define scope and content

T **Testing of program** on regular basis

R Define **roles** and response

U **Review & update** Business continuity & capability

M **Maintenance of BCP** to ensure its appropriateness

P **Convert policies** & strategies **into action**

• **BCM Documentation** BCM records should be retained for a minimum period of 1 year.

1 The business continuity policy;
2 The business impact analysis report;
3 The business continuity management system;
4 The risk assessment report;
5 The aims and objectives of each function;
6 The activities undertaken by each function;
7 The business continuity strategies;
8 The overall & specific incident mgmt plans;
9 The business continuity plans;
10 Local Authority Risk Register;
11 Exercise schedule and results; ·
12 Incident log;
13 Training program.

1. BCM - Information Collection Process

• **Task or Activities involved in BIA** [M15] [CITLRI]

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

4. BCM Testing and Maintenance Process

• **BCM Capability**

Practicing the enterprise's ability to recover from an incident;
Verifying that the BCP incorporates all activities and their priorities;
Highlighting assumptions, which need to be questioned;
Instilling confidence amongst exercise participants;
Raising awareness of business continuity throughout the enterprise by publicizing the exercise;
Validating the effectiveness and timeliness of restoration of critical activities;
Demonstrating competence of the primary response teams and their alternatives.

• **Testing Objectives of BCP** [M18] [Memory - BMCC Backup]

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

• **Maintenance Task of BCP** [Version up-to-date update rakha "I" ki responsibility hai]

Version **Implement version control procedure** to ensure that plan is maint up to date
Up-to-date Maintenance regime to ensure **plan remain up-to-date**
Update Maintenance process to **update the plan**
I **Identify BCP maint triggers** to ensure who are accountable
Responsibility **Determine ownership & responsibility** for maintaining various BCP strategies within ent.

• **Audit / Self Assessment of BCM or Review of BCM** [Key Priority & Capability of RASMI Changed]

Key	All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
Priority	The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements;

Capability	The enterprise' BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
R	BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities;
A	The enterprise has an ongoing program for BCM training and awareness;
S	The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
M	The enterprise's BCM maintenance & exercising programs have been effectively implemented;
I	BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
Changed	Change control processes are in place and operate effectively.

5. BCM Training Process

- **Competence of Personnel Providing Training** [April me NRI ko promote karna Hai]

A	Actively listens to other, their ideas & opinions	Promote the culture of health and safety
P	Provide support in difficult circumstance	
R	Respond constructively in difficult circumstances	
I	Ack the contribution done by other, Involve team members	
L	Adopt Leadership style appropriately to match circumstance	
N	Encourages and actively listen / respond to new ideas.	
R	Encourage to take calculated risk	
I	Demonstrates personal integrity	

- **Steps to be taken by IS Auditor with respect to IT in the process of BCP**

a Determine if the plan reflects the current IT Environment

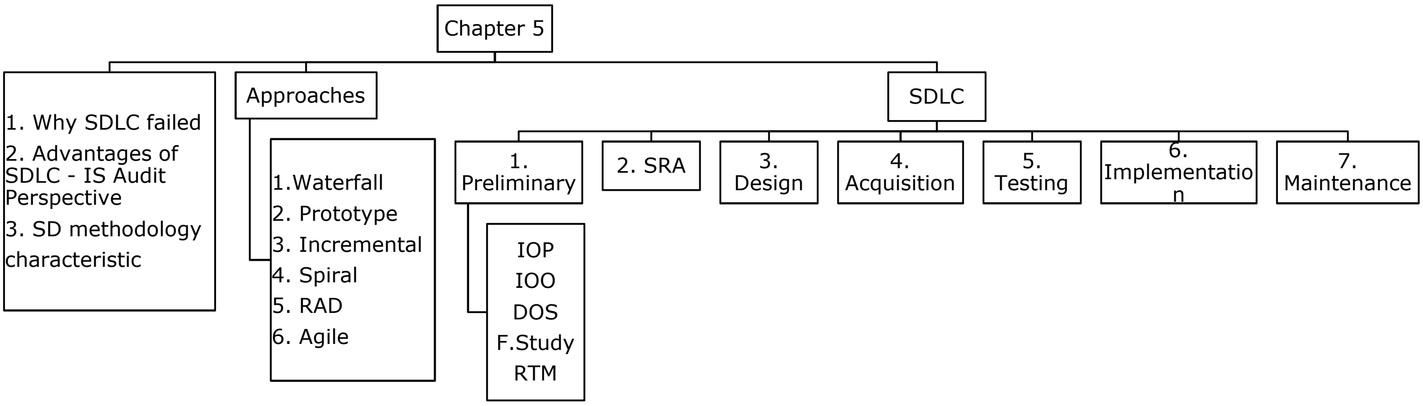
b Determine if the plan includes prioritation of critical application & systems

c Determine if the plan includes time req for recovery of each critical system

d Does DRP includes arrangement for emergency telecommunications ?

e Is there plan for alternate means of data transmission if computer network is interrupted

Chapter 5



Why Org Fail to achieve objective ? [RTP N19] [Inadequate PNR]

(i)	**User related issues**	It refers to those issues where user is reckoned as the primary agent.
	Inadequate testing and user training	New systems must be tested before installation. **Users must be trained** to effectively utilize the new system.
P	Lack of user participation	**Users must participate in the development** efforts to resolve development problems. User participation also helps to reduce user resistance to change.
N	Shifting user needs	User requirements for IT are constantly changing. When these changes occur during a development process, the development team faces the challenge of developing systems.
R	Resistance to changes	People have a natural tendency to resist change, changes- often radical - in the Workplace. Development project is doomed to failure.
(ii)	**Management related issues**	[SD]
S	Lack of Senior Mgmt support and involvement	Developers and users of information systems watch senior management to determine 'which systems development projects are important'.
D	Development of strategic systems	Because strategic decision making is unstructured, objectives are difficult to define.
(iii)	**Developers related issues**	[US]
U	Overworked staff or Under-trained development staff	System developers often **lack sufficient educational background and skills.** Furthermore, training plan and training budget do not exist.
S	Lack of Std Project Mgmt & sys. dev. methodologies	Some organizations do not formalize their project management and system development methodologies, making it very difficult to complete projects on time or within budget.
(iv)	**New technologies**	When an organization tries to create a competitive advantage by applying advance technologies, attaining system development objectives is more difficult because personnel are not as familiar with the technology. (GST, AI)

• Advantages of SDLC from IS Audit perspective (Auditor) [PERT]

IS Auditor can have clear understanding of **various Phases** of SDLC on the basis of document created during each phases

IS Auditor can provide an **Evaluation** of methods & technique used through various development phases

IS Auditor on examination can state in its **Report** about the compliance by IS Mgmt

IS Auditor, if has **Technical knowledge** & ability of different areas of SDLC can be a guide during various phases

System Development Methodologies

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

The methodology is characterized by the following:

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

1. Waterfall / Traditional

The waterfall approach is a **traditional development approach** in which each phase is **carried** in **sequence or linear fashion**. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release. Emphasis of this approach will be on 1. Full Proof 2. Control 3. Documented 4. Secured System

Features: [DO Document]

1. Project is **divided** into seq phases with some overlap and splash back acceptable between phases
2. Emphasis is on planning, time schedules, target dates, budget & implement of an entire sys. at **one time**
3. Tight control is maintained over the life project through use of extensive written **documentation**

2. Prototyping

The **goal** of prototyping approach is to **develop a small / pilot version** called a prototype of a Part / All a system. prototype is a **usable system** / system component that is **built quickly** & **at a lesser cost**, and with the intention of modifying or even replacing it by a full -scale and fully operational system. If it is scrapped, the **knowledge gained** from building the prototype **is used to develop the real system.**

- **Phases :** [IDT - Sign off]

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

3. Incremental

Incremental model is a method of soft. development where the **model is designed, implemented & tested incrementally** Develop Software in part **using elements of waterfall model & iterative philosophy of prototyping model**

Features: [RIM]

1. Overall **requirements are defined** before proceeding to evolutionary, mini–Waterfall development of individual increments of the system.

2. The **initial soft. concept & system core are defined** using the Waterfall approach, followed by iterative Prototyping.

3. **A series of mini-waterfalls are performed**, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.

4. Spiral

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

Features: [Preliminary FNS]

A preliminary design is created for the new system. This phase is the most important part of "Spiral Model" in which all possible alternatives are analyzed. This phase has been added specially in order to identify and resolve all the possible risks in the project development.

A first prototype of the new sys. in constructed from d preliminary design. This is usually scaled-down sys.

The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users.

A second prototype is evolved by a fourfold procedure by evaluating the first prototype in terms of its strengths, weaknesses, and risks.

5. Rapid Application Development

Rapid Application Development (RAD) uses **minimal planning** in favour of rapid prototyping. The planning of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements. **Also called 'Joint Application Development'**

Features : [JD BANTA]

J Generally includes Joint Application Development (JAD).
D Produces documentation necessary to facilitate future development and maintenance.
B Attempts to reduce inherent project risk by Breaking a project into smaller segment
A Aims to provide high quality system quickly
N Key emphasis is on fulfilling the business need.
T Project control involves prioritizing development and defining delivery deadlines or "time boxes."
A Active user involvement is imperative.

6. Agile Features

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

Agile Manifesto is based on following 12 features: [MSD is always CORRECT]

M Working software is the principal **measure of progress**;
S **Simplicity;** D Working software is **delivered frequently** (weeks rather than months);
C **Customer satisfaction** by rapid delivery of useful software; O **Self-organizing teams;**
R **Regular adaptation** to changing circumstances.
R **Welcome changing requirements**, even late in development;
E Continuous attention to **technical excellence** and good design; 10
C **Face-to-face conversation** is the best form of communication (co-location);
T Projects are built around motivated individuals, who should be **trusted**;

Type	Strengths [Support OPC]	Weakness [GEET IRS]
Waterfall	1. Fresh programmer can work on this project Support less experience project team 2. Ensure order sequence needs to quality, reliability, security maintainability in d system. 3. Project progress is measurable 4. Enablers to conserve resources.	1. Promote GAP between users and developers 2. It leads to excessive documentation 3. There is a little to iterate, which may be essential in situations. 4. Sys Performance cant be tested until sys. full ok 5. It is criticized to be inflexible, slow, costly, & cumbersome (frausted, bore) 6. Difficult to respond changes occur in life cycle 7. Written specifications r difficult for users to read

Type	Strengths [Improve Unclear DEFENCE]	Weakness [Nadan RIA ka Behaviour & STD Call]
Prototype	1. **Improve both user participation** in System dev 2. It's especially useful 4 resolving **unclear objective** 3. It typically results in a better **definition of these users' needs & requirements** than does the traditional systems development approach. 4. **Potential exists 4 exploiting knwdg** gained in an early iteration as later iterations r developed. 5. Encourage Innovation & **flexible design** 6. **Help easily** to identify difficult & confusing functio 7. A very short time period is normally required to develop and start experimenting with a prototype. 8. Errors are hopefully detected & eliminated early in the developmental process. Information system should be more reliable & less costly to develop. 9. It **enables to generate** specifications for a production application. 10. It provides for **quick implementation** of an incomplete, but functional, application.	1. **Identification of non-functional elements** is difficult to document. 2. Requirements may frequently change significantly. 3. Incomplete/ inadequate prob. analysis may occur. 4. Approval process and control are not strict. 5. Prototyping may cause **behavioural problems with system users.** These problems include dissatisfaction by users if sys. developers are unable to meet all user demands. 6. Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype. 7. Inadequate testing can make the approved system error-prone, & **inadequate documentation** makes this system difficult to maintain. 8. Designers may prototype too quickly resulting in an inflexible design. 9. Prototype may not have **sufficient checks** and balances incorporated.

Type	Strengths [Sasti Dairy GEMS ka CDR]	Weakness [RUDE]
Incremental	1. It is more flexible and less costly to change scope and requirements. 2. Moderate control is maintained over the life of d project through d use of written documentation. 3. Gradual implementation provides the ability to monitor d effect of incremental changes & make adj's before d organization is negatively impacted. 4. Potential exists for exploiting knowledge gained in an early increment as later increments are dev. 5. Stakeholders can be given concrete evidence of project status throughout the life cycle. 6. It allows d delivery of series of implementations that are gradually more complete. 7. It helps to mitigate integration & architectural risks earlier in the project.	1. Each phase of an iteration is rigid and do not overlap each other. 2. When utilizing a series of mini-waterfalls, there is usually a lack of overall consideration of the business problem for the overall system. 4. It is difficult to demonstrate early success to management. 3. Since some modules will be completed much earlier than others, well-defined interfaces are required.

Type	Strengths [ROI] --> Nov 19	Weakness [DEER]

Spiral	1. Enhances risk avoidance 2. Useful in helping 4 optimal best dev methodology 3. It can incorporate W+P+I model provide guidn. which combination of these models best fits	1. No firm Deadline / No clear termination 2. No establish control exists, 1 cycle se dusre cycle 3. Skilled experienced project manger req 4. Highly customize hota hai so reuse nahi kar sakte

Type	Strengths [SOLAR TV]	Weakness [Difficult AIMS Attention Fast]
RAD	1. It holds a great level of commitment from stakeholders than W, I, Spiral frameworks. 2. It concentrates on essential system elements from user viewpoint. 3. RAD tends to produce systems at lower cost. 4. It provides for the ability to rapidly change system design as demanded by users. 5. Quick initial reviews are possible. 6. It leads to a tighter fit between user requirements and system specifications. 7. Operational version of an application is available much earlier than with W, I, Spiral frameworks. ·	1. Formal reviews and audits are more difficult to implement than for a complete system. 2. It may lead to inconsistent designs within & across systems. 3. Since sm modules will b completed much earlier than others, well–defined interfaces r required. 4. The project may end up with more requirements than needed (gold-plating). 5. It may call for violation of programming standards related to inconsistent documentation. 6. It may call for lack of attention to later system administration needs. 7. Fast speed & lower cost may affect adversely the system quality.

Type	Strengths [CEAT-High]	Weakness [ALERT-Track]
Agile	1. Face to face communication from customer representative leaves little space for guesswork. 2. The team does not have to invest time and efforts and finally find that by the time. 3. Has a concept of adaptive team, respond quick 4. The documentation is crisp and to the point to save time. 5. The end result is the high quality software in least possible time duration & satisfied customer.	1. Agile lacks the attention to outside integration. 2. In case of some software deliverables, especially the large ones, it's difficult to assess the efforts Required at the beginning of the SDLC. 3. There is lack of emphasis on necessary designing and documentation. 4. Agile requires more re-work & due to the lack of long-term planning & the lightweight approach to architecture. 5. Agile increases potential threats to business continuity and knowledge transfer. 6. The project can easily get taken off track if d customer is not clear about the final outcome.

System Development Life Cycle (SDLC)

1. Preliminary Investigations

Delineation of Scope - **Factors to be considered** Q9 CLEAR IDIOt

Clear While presenting d proposed solution for a problem, d development organization has to **clearly quantify d economic benefits to d user organization.** For eg, when system is proposed for Road tax collection.

I While the **initiator** of the project may be a member of the senior management, the actual users may be from the operating levels in an organization.

D **Different users** may represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project.

I It is also necessary to understand the **impact of the solution** on the organization. Wide impact met with greater resistance. ERP implementation is a classic example.

Ot While economic benefit is a critical consideration when deciding on a solution, there are several **other factors** that have to be given weightage too.

- **Two Primary Methods**

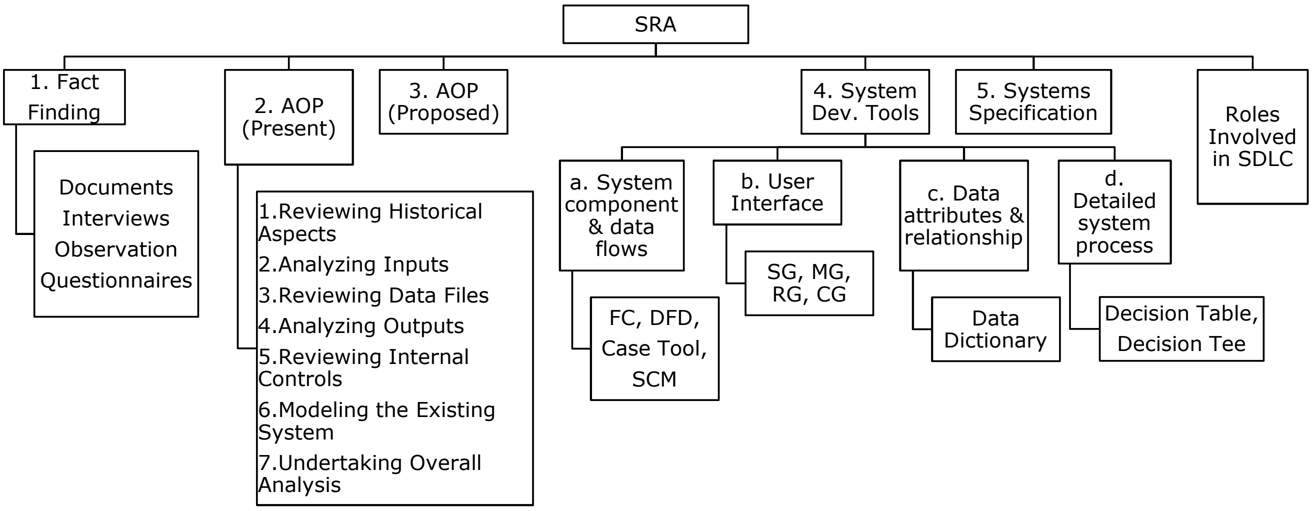
Review Internal doc	The analysts conducting the investigation first try to learn about the org. For example, to review an inventory system proposal. Analysts can usually learn these details by examining org. charts.
Conducting Interviews	Written doc's tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made. To learn these details, analysts use interviews. **Interviews allow analysts to know more about the nature of the project** request and the reasons for submitting it. Usually, preliminary investigation interviews involve **only management and supervisory personnel.**

- **Feasibility Study** [LOBSTER Fry]

A feasibility study is carried out by the system analysts, which refers to a process of evaluating alternative sys. through cost/benefit analysis so that the most feasible & desirable sys. can be selected for dev.

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

2. System Requirement Analysis (SRS)



- **Fact Finding Technique** [DIOQ]

Every sys. is built to meet some set of needs, for eg., the need of organization for lower operational costs, better information for managers, smooth operations for users/ better levels of services to customers.

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

- **Analysis of Present System** [DIDI ko HOME Overall Analysis]

Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates.

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

- **System Development Tools- categories** [SUDD]

a. System component and data flows

Flowcharts	Flowcharting is a pictorial representation technique that can be used by analysts to represent the inputs, outputs and processes of a business process.
DFD	A DFD uses few simple symbols to illustrate the flow of data among external entities.
Case tools	CASE refers to the automation of anything that humans do to develop systems & support virtually all phases of traditional system development process. For eg, these packages can be used to create complete & consistent requirements specifications with specifications lang.
SCM Matrix	A System Component Matrix provides a matrix framework to document the resources used and the information produced by an information system. It can be used for both systems analysis and system design.

b. User Interface

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

c. Data attributes and relationship

Data Dictionary	A data dictionary contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help to establish an audit trail.

d. Detailed system process

Decision Tree	A Decision Tree is a support tool that uses a tree-like graph/ model of decisions including chance event outcomes, resource costs, and utility. Decision tree is commonly used in operations research.
Decision Table	A Decision Table is a table, which may accompany a flowchart, defining the possible contingencies that may be considered within the program & the appropriate course of action for each contingency.

Objective/Activity to be performed [PAAVTI]
analyze req and deter. Priorities
To doc activities - interview. que. Report
To model act - ER dig, Data flow diag
To verify the req r complete consistent, traceable
Identify and consult karo stake ho. Expectation

3. System Design

Architecture Design

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

User Interface Design

Design of Data

The design of the data and information flow is a major step in the conceptual design of the new system. In designing the data / information flow for the proposed system, the inputs that are required are -existing data / information flows, problems with the present system, and objective of the new system.

Design of Database [N14] [Conceptual DPS]

Design of the database involves determining its scope ranging from local to global structure. The scope is decided on the basis of interdependence among organizational units.

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

4. System Acquisitions

Acquisition Standard [SCRET]

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

Acquiring System Component from Vendors [VLUP]

Vendor Selection:	This step is critical step for success of acquisition of systems. Vendor selection is to be done prior to sending RFP. 'RFP are sent only to selected vendors'.
Geographical Location of Vendor:	The issue to look for whether the vendor has local support persons. Otherwise, the proposals submitted by vendor not as per RFP requirements need to rejected. This stage may be referred to as 'technical validation'.
Evaluation of Users Feedback:	The best way to understand the vendor systems is to analyze the feedback from present users. Present users can provide valuable feedback.
Presentation by Selected Vendors:	All vendors, whose proposals are accepted after "technical validation", are allowed to make presentation to the System Acquisition Team.

Method of Validating Vendors Proposal [May 19] CPT Report Benchmarking]

Checklist	It is the most simple and a subjective method for validation and evaluation. The various criteria are put in check list in the form of suitable questions against which the responses are validated. For example, Support Service Checklists.
Point Scoring Analysis	Point-scoring analysis provides an objective means of selecting a final system.
Testing Problems	Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system.
Public Evaluation Reports	Several consultancy as well as independent agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports. This method is particularly useful where the buying staff has inadequate knowledge of facts.
Benchmarking Problems	Benchmarking problems related to vendors' proposals are accomplished by sample programs that represent the buyer's primary work load.

5. System Development

Good coded application characteristic [N16] [U R RARE]

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

a. Program Coding Standard d. Testing Program e. Program Documentation f. Program Maint.

b. Programming Language

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

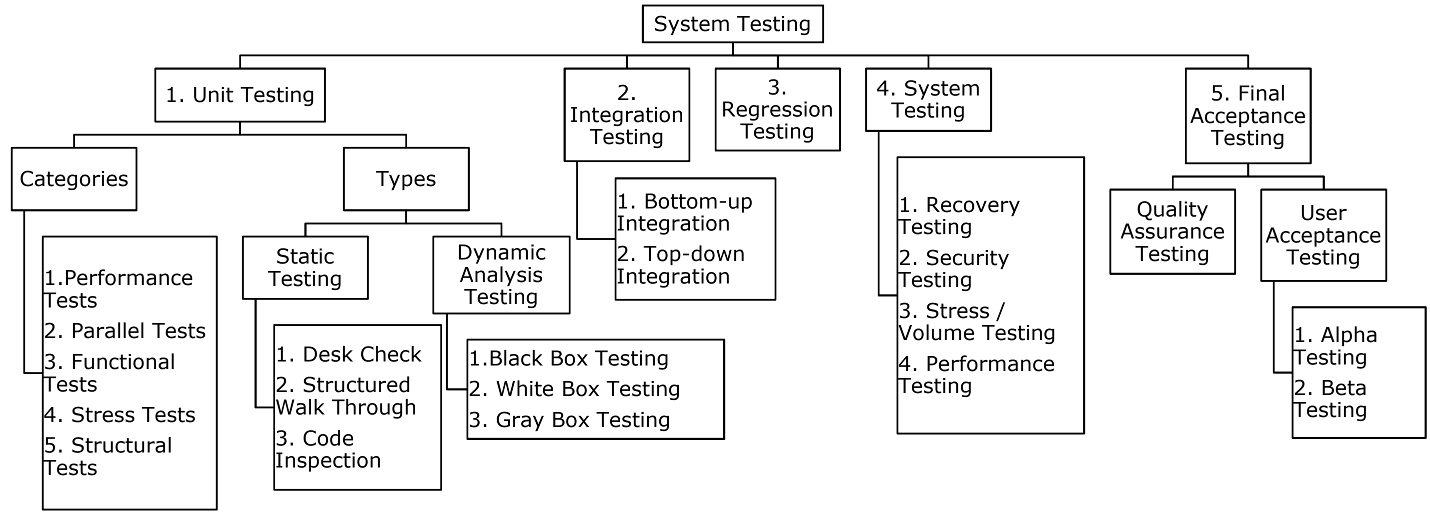
- High level general purpose programming languages such as COBOL and C;
- Object oriented languages such as C++, JAVA etc.;
- Scripting language such as JavaScript, VBScript; and
- Decision Support languages such as LISP and PROLOG.

c. Program Debugging

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

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

6. System Testing



1. Unit Testing

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

• Categories [Pooja Patel Feeds Shreyas Shah]

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

• Types

Static Testing: Static Analysis Tests are conducted on source programs and do not normally require executions in operating conditions. [DSC] a. Desk Check: This is done by the programmer him/herself. S/he checks for logical syntax errors, and deviation from coding standards. b. Structured Walk Through: The application developer leads other programmers to scan through the text of the program and explanation to uncover errors. c. Code Inspection: The program is reviewed by a formal committee. Review is done with formal checklists.	**Dynamic Analysis Testing:** Such testing is normally conducted through execution of programs in operating conditions. a. Black Box Testing: Black Box Testing takes an external perspective of the test object, to derive test cases. b. White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It c. Gray Box Testing: It is a software testing technique that uses a combination of black box testing and white box testing.

2. Integration Testing

***** [RTP N19]

Integration testing is an activity of software testing in which individual software modules are combined and tested as a group.

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

Top-down Integration: It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module.. A stub does not go into the details.

3. Regression Testing

In the context of the integration testing, the regression tests ensure that changes have not introduced new faults. The data used for the regression tests should be the same as the data used in d original test.

4. System Testing

It is a process in which software & other system elements are tested as a whole.

Recovery Testing	This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'.
Security Testing	This is the process to determine that an Information System protects data & maintains functionality as intended or not. This testing technique also ensures the existence & proper execution of access controls in the new system.
Stress & Volum Testing	Stress testing is a form of testing that is used to determine the stability of a given system or entity. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
Performance Testing	Software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device.

5. Final Acceptance Testing

It is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies d quality standards adopted by the business and the system satisfies the users.

a. Quality assurance testing	Ensures that d new sys. satisfies the prescribed quality stds & the development process is as per d org's quality assurance policy, methodology & prescriptions.
b. User Acceptance testing	It ensures that the functional aspects expected by the users have been well addressed in the new system.

Alpha Testing - This is the first stage, often performed by the users within the organization by the developers, to improve and ensure the quality/functionalities as per user's satisfaction.	**Beta Testing** - This is the second stage, generally performed after the deployment of the system. It is performed by the external users, during the real life execution of the project. It normally involves sending the product outside and receives feedback.

7. System Implementation

Equipment Installation

Training Personnel

System Change-over Strategies

Direct Implementation	With this strategy, the changeover is done in one operation, completely replacing the old system in one go.
Phased Changeover	With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and other files continue to be used on the old system i.e. the new is brought in stages (phases).
Pilot Changeover	With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption.
Parallel Changeover	This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online.

- **Various activities involved for Successful conversion**

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

8. Post Impl. Review & Maint

Post Implementation Review

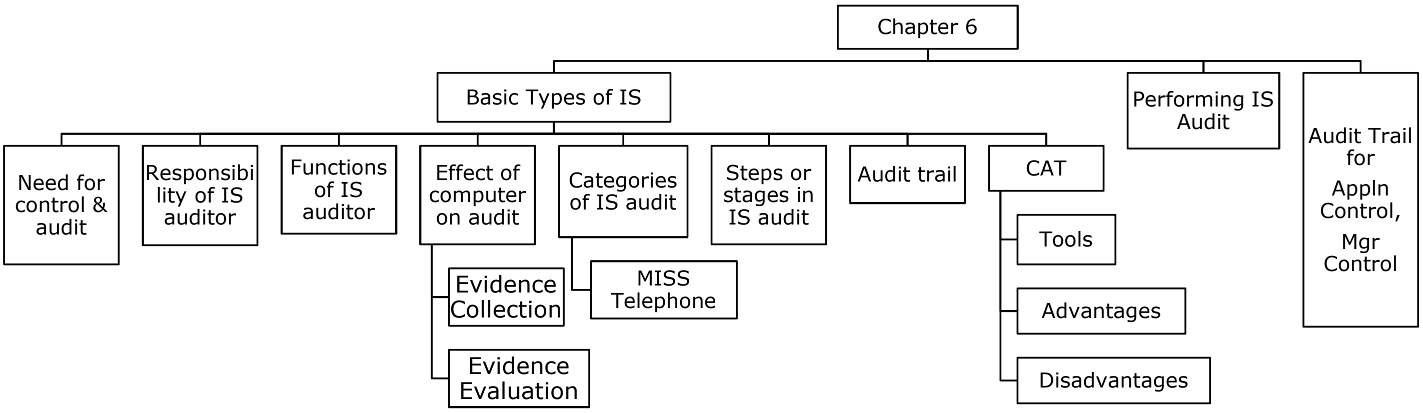
Development Evaluation	Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained.
Operational Evaluation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

System Maintenance - Categories [Memory - SCRAPP]

Schedule Maintenance	Scheduled maintenance is anticipated and can be planned for operational continuity & avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance.
Corrective Maintenance	It deals with fixing bugs in the code or defect found during the executions. Example of corrective maintenance include correcting a failure to test for all possible condition or a failure to process the last record in file
Rescue Maintenance	Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution.
Adaptive Maintenance	It consists of adapting software to changes in the environment, such as the hardware or the operating system
Perfective Maintenance	It deals with accommodating to the new / changed user requirements and concern functional enhancement to the system.
Preventive Maintenance	It concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments etc.

	Responsibility	
System Analyst	Conduct interview	Link between user and programmer
Programmer	Mason of soft ind	Convert design into prog by coding using P.lang
Database administrator		
Domain specialist		
IS auditor		Involved in design and final test
Quality assurance		Team set standard he checks on periodic basis

Chapter 6



16 IS Auditing Standard 39 Auditing Guidelines 11 IS Auditing Procedures

• Need for Audit of Information Systems

[Memory - DEPICA Value]

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

D	Organisation cost of Data loss	Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
E	Controlled Evaln. of computer use	Use of Technology and reliability of complex computer systems cannot be guaranteed & the consequences of using unreliable systems can be destructive.
P	Maintenance of privacy	Data collected contains private information about an individual too. There is a fear that privacy has eroded beyond acceptable levels.
I	Cost of Incorrect decision making	Management & operational controls taken by managers involve detection, investigations & correction of the processes. These high level decisions require accurate data to make quality decision rules.
C	High cost of computer error	In a computerised environment, a data error during entry or process would cause great damage.
A	Cost of computer abuse	Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities & unauthorised copies of sensitive data can lead to destruction of assets.
Value	Value of Computer Hardware Softwr. and Personal	These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.

• Objective of IS Audit

[AIEE]

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

• Responsibilities or Skill set of IS Auditor

Knowledge of	IT Principles & Polices, IT Strategy
Good Knowledge	Prof. Standards and **Best IT Practices** of IT Control
Sound Knowledge	**Business operations**, practice & compliance requirements
Should possess	requisite professional technical **qualification** and certifications
Good Understanding	Information Risk & Control
Ability to understand	Control for business continuity

- **Functions of IS Auditor / IS Auditor review risk relating to IT System & Process** [Memory - IFRS]

I	Review of Ineffective IT Strategies, Policies, Proc.	(Internet usage policy)
F	Review of IT Related frauds	(Phishing, hacking)
R	Review of Inefficient use of corporate resources	(Huge spending on IT budget, development)
S	Review of Inadequate Info. security control	(Password nhi, outdated antivirus)

- **Effect of Computers on Audit**

[i] Changes to Evidence Collection [N14] [DOSA EdLi]

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

[ii] Changes to Evidence Evaluation. [SAS]

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

- **Categories of IS Audit / Types of Info System Audit** [May 19] [Memory - MISS Telephone]

M	Management of IT & Ent. Architectures	An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
I	Information Processing Facilities	An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
S	System Development	An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
S	System and Applications	An audit to verify that systems & applications are appropriate, efficient, & adequately controlled to ensure valid, reliable, timely, & secure input, processing, & output at all levels of a system's activity
Tele	Telecommunication, Intranets and Extranets	An audit to verify that controls are in place on the client, server, and on the network connecting the clients and servers.

- **Steps in IS Audit** [M18] [PPF ARChi]

P	Scoping and pre-audit survey	Auditors determine the main areas of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management.
P	Planning and preparation	During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan.
F	Fieldwork	This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

A	Analysis	This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT, PEST (Political, Economic, Social and Technological) techniques can be used for analysis.
R	Reporting	Reporting to the management is done after analysis of evidence is gathered and analyzed. Analysis and reporting may involve the use of automated data analysis tools such as ACL, IDEA, Excel, Access and hand-crafted SQL queries.
C	Closure	Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

• Audit Trails & Objective of Audit Trails [Memory - DRP]

Audit trails are logs that can be designed to record activity at the system, application, and user level. Audit trails provide an important detective control to help accomplish security policy objectives.
Audit trail controls attempt to ensure that a chronological record of all events is maintained. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

Audit Trail Objectives

D	Detecting unauthorised access
R	Reconstructing Events
P	Personal Accountability

• Concurrent Audit Techniques / Types of Audit Tools [Nov 19] [SISCA]

S	Snapshot	Tracing a transaction in a computerized system can be performed with the help of snapshots. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.
I	Integrated Test Facility	The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.
S	SCARF (System Control Audit Review File) M14	The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.
C	CIS	This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way: 1. The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system. 2. CIS replicates or simulates the application system processing. 3. Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces. 4. Exceptions identified by CIS are written to an exception log file

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

[Nov 19]

- **Auditors might use SCARF to collect the following types of information** [SSAMVED]

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

- **Advantages of Concurrent Audit Techniques** [RTP N19] [CAT Objective]

C - Surprise test capability	As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
A - Timely, comprehensive & detailed auditing	Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
T - Training to new user	Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.
Objective - Info to system on meeting objective	Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

- **Disadvantages of Concurrent Audit Techniques** [May 19] [SADSE]

Auditors should be able to obtain resources required from the organization to **support development**, implementation, operation, and maintenance of continuous audit techniques.
Continuous auditing techniques are more likely to be used where the **audit trail is less visible and the costs of errors and irregularities are high.**
Continuous audit techniques are more likely to be used if auditors are involved in the **development work** associated with a new application system.

Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively **stable**.
Auditors need the knowledge & **experience** of working with computer systems to be able to use continuous audit techniques effectively and efficiently.

- **Performing IS Audit**

1 Materiality & Significance

2 Audit Testing

3 Basic Plan

4 Critical factors while Preliminary review in IS Audit [N18] [Memory - KAMTI]

K Knowledge of the business

A Legal consideration and audit standard

M Risk assessment and materiality

T Understanding the technology architecture

I Understanding Internal control system

5 Developing Risk Based Audit Plan [Nov 19] [Memory - IDA Priority]

I Inventory the Information system in use in organisation and categorize them

D Determine which of the systems impact critical function or assets

A Assess what risks affects these systems and the severity of the impact on the business

Priority Based on above assessment determine audit priorities, resources, schedule and frequency.

[BAS RAAT din Network]

Preliminary Evaluation, Major aspect should be studied to **gain a good understanding of the technology** environment and related control issues [M15]

BA Analysis of **business processes** and **level of automation;**

S **Studying ITPP** Information Technology policies, standards, guidelines and procedures.

R Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. **Role of IT in the success** and survival of business;

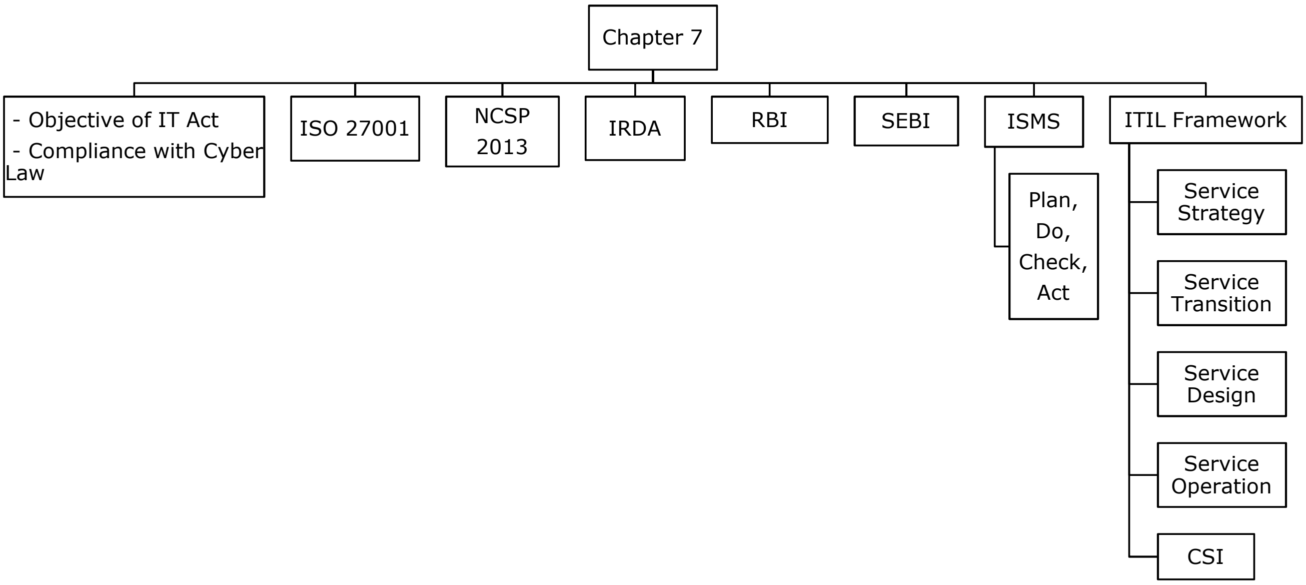
A **Understanding technology architecture** which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture;

A **Understanding extended enterprise architecture** wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government;

T **Knowledge of various technologies** and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems;

Netwo **Studying network diagrams** to understand physical and logical network connectivity;

Chapter 7



• SA 402 Audit considerations relating to an entity using service organisation

Service auditor report

Type 1 Report	Type 2 Report
Description of Control (Prabhu hai? Control hai?)	Description of Control
Whether control achieved designed objective (Door/Window)	Whether control achieved designed objective (Design Tod)
	Whether controls are operative effectively (Working)

66F Cyber Terrisom Imprisonment which may extend to imprisonment for Life

• Objective of IT Act 2000.

a To grant transaction carried out by means of electronic data i.e. 'E-commerce'

b To give legal recognition to Digital sign for authentication of any information

e To give legal recognition for keeping of books of account by Bankers in electronic form

c To facilitate electronic filing of docs with govt dept

d To facilitate electronic storage of data

f To facilitate and give legal sanction to electronic fund trf between bank and FI.

g To amend the Indian Penal Code, Indian Evidence Act,1872, The Bankers Books Evidence act, 1891 and RBI Act 1934

Private Key	Key of key pair used to create a digital signature
Public Key	Key of key pair used to verify a digital signature

• Compliance with CYBER Law

a Designate a Cyber Law Compliance Officer as required.

b Conduct regular training of relevant employees on Cyber Law Compliance.

c Implement strict procedures in HR policy for non-compliance.

d Implement authentication procedures as suggested in law.

e Implement policy and procedures for data retention as suggested.

f Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.

g Implement applicable standards of data privacy on collection, retention, access, deletion etc.

h Implement reporting mechanism for compliance with cyber laws.

ISO 270001

- **Key Benefit of ISO 27001**

a Provides confidence and assurance to trading partners and clients, act as marketing tool.
b Can act as extension of current quality system to include security.
c Independent review on Information security policy
d Opportunity to identify & manage risks to key information and systems assets.

- **A company may adopt ISO 27001 for following reasons;** [DIGRI]

a Creates market differentiation due to prestige, goodwill
b Demonstrates security status according to internationally accepted criteria
c If a company certifies once, it is accepted globally
d It Provides a holistic risk based approach to security information
e It is suitable for protecting critical & sensitive information

- **National Cyber Security Policy 2013**

IRDA

a System Audit [May 19]

1 All insurers shall have their systems and process audited at leance once in 3 years by CA firms
2 In doing so, the current internal / concurrent / statutory auditor is not eligible for appointment
3 CA firm must be having a minimum 3-4 years experience of IT system of banks or mutual funds or insurance companies

b System Control

1 **There should be Electronic transfer of Data without manual intervention.** All Systems should be seamlessly integrated. Audit Trail required at every Data entry point. Procedures for reviewing and maintaining audit trail should be implemented.

2 The auditor should comment on the audit trail maintained in the system for various activities. The auditor should review the Front Office Systems (FOS), MOS (Mid Office Systems) and BOS (Back Office Systems) and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.

3 Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.

Types of Information an auditor is expected to obtain at the audit location ? ***** [RTP N19]

1 Location(s) from where Investment activity is conducted
2 IT Application used to manage the insurers Investment Portfolio
3 Previous Audit report and Open issues from - Internal Audit, Stat Audit, IRDA Inspection Audit
4 Internal circulars & guidelines of the Insurer
5 IRDA circulars and notification issued by IRDA
6 List of new product / fund introduce during audit period
7 SOP - Standard Operating Procedures
8 BCP - Business Continuity Plans
9 IT Security Policy
10 Network Security Reports pertaining to IT Assets

RBI

a System Audit

1 Banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions.

2 Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent and exercise due professional care.

3 The IS Audit should be independent of the auditee, both in **attitude and appearance**.

4 IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training.

b System Control

1 Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design.

2 Contingence Plans to ensure continuity of critical business process & tested at periodic level.

3 An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.

4 In order to bring about uniformity of software used by various branches/offices there should be a formal method of incorporating change in standard software and it should be approved by senior management.

5 Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.

6 Annual review of IS audit policy

7 Require to **conduct Quality Assurance Testing (QAT)** at least **once every 3 years**

SEBI

a System Audit

1 Audit shall be conducted according to **Norms, TOR, guideline issued by SEBI**

2 **Stock exchange** (Auditee) may negotiate and **shall appoint auditor.** Auditor 3 successive audit hi kar sakta hai.

3 Audit schedule at least 2m advance me submit to SEBI (Scope Current + prev audit)

4 SEBI scope change kar sakta hai

5 Audit report submitted to the auditee, report contains compliance /non compliance issues

6 Non compliance ka ans 3 month me dena. The auditor should indicate if follow on audit is req to review status of NC

7 Completion audit ke 1 month ke andar report along with mgmt comment, SEBI ko dena

b System Control

1 Further, along with the audit report, Stock Exchanges/Depositories are advised to submit a declaration from the MD/CEO certifying the security and integrity of their IT Systems.

2 A proper audit trail for upload/modifications/downloads of KYC data to be maintained

c Auditor Selection - Conditions

1 Auditor must have **minimum 3 Year Experience** in eg. stock exchange, clearing houses, depositories

2 Auditor must have experience in areas covered under TOR

Shall have industry certificates ISACA se CISA (Certified Info Syst Auditor)
CISM (Cert Info Security Manager)

3 COBIT / IT Gov / framework ka knowledge chaiye

4 Jis ka audit kar rahe hai usse last 3 sal me not engaged No conflict of interest , independent chaiye

5 No case pending under SEBI Jurisdiction

ISMS

• Information Security Management Standard (ISMS) / ISO [N14]

ISO prescribe - 'How to manage Info. Security through a system of Information security management'

Phases [PDCA Cycle]

Plan	This phase serves to plan the basic org. security, setting the objectives for security and Choose appropriate security control
Do	This phase includes carrying out everything that was planned earlier
Check	Purpose of this phase to monitor the functioning of ISMS & check whether results meet objectives
Act	Purpose of this phase is improve everything that was identified as non compliance in previous phase.

• ITIL Framework - Information Technology Infrastructure Library (STD Over-Seas)

1. Service Strategy PFBG-Demand

This provides guidance on clarification and prioritization of service provider investments in services

Service Portfolio Mgmt	IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.
Financial Management	Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.
Business Relationship Management	Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.
IT Service Generation	IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.
Demand Management	It is a planning methodology used to manage and forecast the demand of products and services.

2. Service Transition

This elates to d delivery of services required by a business into live/operational use, & often encompasses the "project" side of IT rather than Business As Usual (BAU)

Service Transition Planning and Support	It ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes. The service transition planning and support process must incorporate the service design and operational requirements within the transition planning.
Service Validation & Testing	The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.
Knowledge Management	Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organisational knowledge. It refers to a multi-disciplined approach to achieving organisational objectives by making the best use of knowledge.
Change management and Evaluation	It ensure that standardized methods and procedures are used for efficient handling of all changes.
Release and Deployment Management	It is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure.

3. Service Design CCLAS

This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort

Service Catalogue Management	It maintains and produces the Service Catalogue & ensures it contains accurate details, dependencies & interfaces.
Capacity Management	Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands.
Availability Management	It allow organizations to sustain the IT service-availability to support the business at a justifiable cost. It focus on services to be provided over a period of time.
Service Level Management	Service-Level Management is the primary interface between end-user and service provider. It mention agreed level of IT services.
Supplier Management	The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements.

4. Service Operation

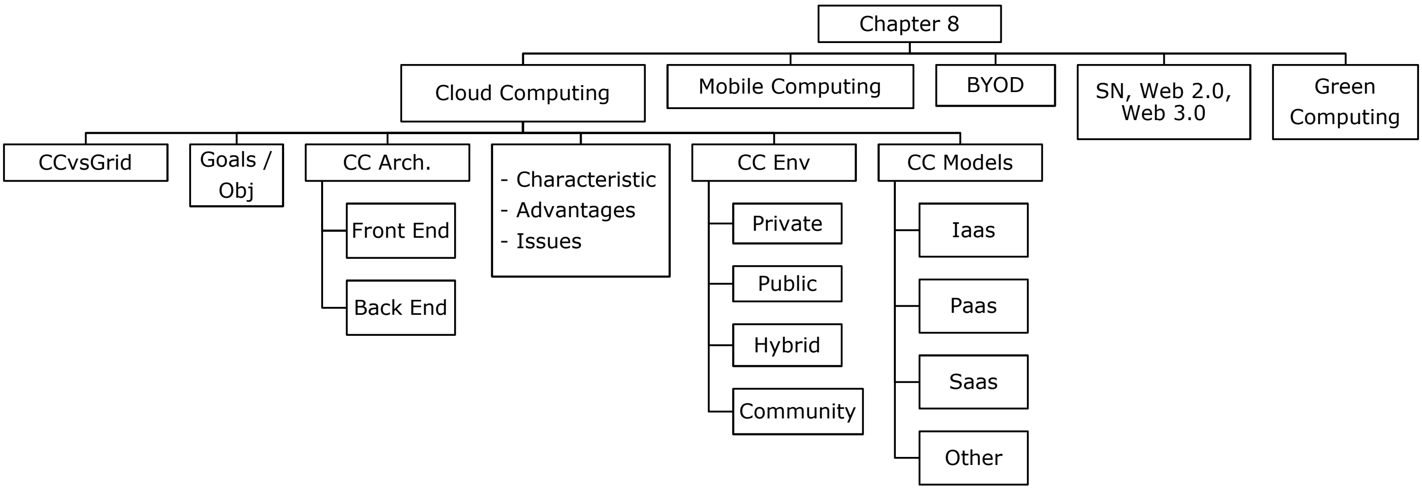
This provides best practice for achieving d delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs)

Service Desk	It is one of four ITIL functions and is associated with the Service Operation lifecycle stage. It include handling incidents and requests, and providing an interface for other ITSM processes.
Event Management	An event may indicate that something is not functioning correctly, leading to an incident being logged.
Incident Management	It aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
Application management	ITIL application management encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.
Problem Management	Problem management aims to resolve the root causes of incidents and thus to minimize the adverse impact of incidents caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.
Request fulfilment	Request fulfilment (or request management) focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.

5. Continual Service Improvement

This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.

Chapter 8



Cloud computing simply means the use of computing resources as a service through network, typically the Internet. With cloud computing users can access database resources via internet from anywhere, anytime and without worrying about the maintenance

[SM-SF]

Similarities (Cloud v/s Grid)		Differences (Cloud v/s Grid)	
Scalable	**Multi tasking**	**Storage**	**Focus**
Both are scalable, Scalability accomplished through **load balancing of application instances** (Resources). CPU and network bandwidth is **allocated and de-allocated on demand.**	Both computing types involve **multi-tenancy and multitasking**, meaning that many customers **can perform different tasks.** Sharing resources assists introducing infrastructure costs and peak load capacity.	**Cloud: Any size object stored** in cloud 1 byte to 5 gb / extra. **Grid:** Not economical for object less than 1 byte	**Cloud:** focuses on two instances **Standard and High CPU.** **Grid:** grid focuses on computationally intensive operations

- **Major Goals of Cloud Computing** (Write To in Start) [Memory - SCRAAP Enable]

S To **scale the IT ecosystem quickly, easily & cost-effectively** based on the evolving business needs;

C To **consolidate IT infrastructure** into a more integrated and manageable environment;

R To **reduce costs** related to **IT energy**/power consumption;

A To enable or **improve "Anywhere Access"** (AA) for ever increasing users;

A To **access services** and data from **anywhere at any time;**

P To create a highly efficient IT ecosystem, where **resources are pooled together** and costs are aligned with what resources are actually used;

Enable To enable rapidly provision resources as needed.

- **Cloud Computing Architecture**

Front End Architecture:	The front end of the cloud computing system **comprises of the client's devices & some applications needed for accessing the cloud computing system.** All the cloud computing sys do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer. Other types of systems have some unique applications which provide network access to its clients.
Back End Architecture:	Back end refers to some **service facilitating peripherals.** In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development & entertainment. Usually, every application would have its individual dedicated server for services.

• Characteristics of Cloud Computing [VPM HASHM]

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

• Advantages of Cloud Computing [AB Q CA]

Almost unlimited storage	Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no needs to worry about running out of storage space or increasing the current storage space availability.
Backup and recovery	Since all the data is stored in cloud, **backup and recovery is relatively much easier**. Cloud service providers are competent enough to handle recovery of information. Hence, this makes the entire process much simpler than other traditional methods of data storage.
Quick deployment	Cloud computing gives us the advantage of quick deployment. The **entire system can be fully functional in a matter of a few minutes.**
Cost efficiency	Cloud computing is probably the most **cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot, licensing fees very expensive.** The cloud is available at much cheaper rates and hence, can significantly **lower the company's IT expenses.**
Easy Access to information	One can access the information from anywhere, where there is an Internet connection. One move beyond time zone and geographic location issues.

• Security issues of Cloud Computing [M15] [CIPLAA GST]

Confidentiality	**Prevention of the unauthorized disclosure of the data** is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential.
Integrity	Integrity refers to the **prevention of unauthorized modification of data** & it ensures that data is of high quality, correct, consistent and accessible.
Privacy	Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design.
Legal Issues & Compliance	There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system.
Availability	Availability refers to the **prevention of unauthorised withholding of data** & it ensures the data backup through BCP & DRP. Availability also ensures that they meet the organization's continuity & contingency planning requirements.
Architecture	In the architecture of Cloud computing models, there should be a control over the security & privacy of the sys. The architecture of the Cloud is based on a specific service model.
Governance	There is a need of governance model, which controls the standards, procedures and policies of the organization.
Data Stealing	In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing.

Trust	Deployment model provided a trust to the Cloud environment. An org. has direct control as well as the federal agencies even have responsibility to protect the information system from the risk.

- **Implementation issues of Cloud Computing** [PHD-Inter] [RTP N19]

Threshold Policy	A threshold policy is of immense importance in a pilot study before moving the program to the production environment. This involves checking how policy detects sudden increases in the demand.
Hidden Cost	Cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges for storage terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software.
Software Development in Cloud	To develop software, use cloud server pools. This allows controlling costs for a project. The project managers can also assign individual hardware resources to different cloud types. To optimize assets, the managers can get cost-accounting data.
Interoperability	If a company outsources with one cloud computing vendor, the co. may find it difficult to change to another computing vendor that has Appln Programming Interfaces (APIs).

Cloud Environment

Type	Characteristics [CAS]	Advantages [PUS]	Disadvantages [BMW]
Private Cloud	1. Central control 2. Weak SLA 3. Secure	1. **Provide** High Level security and privacy to user 2. Improve org server **Utilisation**, allow to use low cost server and hardware. 3. **Small in size**, controlled & maintained by org	1. **Budget** is constraint. 2. IT team **may have to invest time** in buying, building & managing cloud. 3. **Weak loose SLA**.
Type	**Characteristics [SALSA]**	**Advantages [NISHA]**	**Disadvantages [SAP]**
Public Cloud	1. Highly Scalable 2. Highly Available 3. Less Secure 4. Stringent SLA 5. Affordable	1. No limit for no of user 2. No need to **est Infra** 3. **Strict SLA's** are followed 4. **Highly Scalable** 5. **Affordable cost** me availb.	1. Security assurance Less 2. Autonomy(Whole control) & Privacy of org not possible
Type	**Characteristics [SPAM]**	**Advantages [HB]**	**Disadvantages [SM]**
Hybrid Cloud (Pvt+Pub)	1. Scalable 2. Partially Secure 3. SLA stringent 4. Complex Cloud Mgmt.	1. Highly Scalable 2. Better Security-Pub se	1. Security not good as-pvt 2. Complex to manage
Type	**Characteristics [CPC]**	**Advantages [Low CSR]**	**Disadvantages [SAN]**
Community (Pvt+Pvt)	1. Collaborative n maint 2. Partially secure 3. Cost effectiveness	Estb Low cost pvt cloud Collaborative work on cloud Better security-Pub se Sharing responsibility	Security not good as-pvt. Autonomy of org lost. Not suited when no Collaboration

- **Private Cloud** Characteristic [CAS]

This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization’s benefits. These are also called Internal Clouds or Corporate Clouds.

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

- **Public Cloud** Characteristic [SALSA]

Public cloud is the cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis.

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

- **Hybrid Cloud** Characteristic [Pvt + Pub]

This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used.

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

- **Community Cloud** Characteristic [Pvt + Pub]

The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises.

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

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

	On-Premise Private Cloud	**Outsourced Private Cloud**
Management	Managed by the organization itself.	Managed by the third party.
SLA	SLAs are defined between the organization and its users.	These are usually followed strictly as it is a third party organization.
Network	Network management and network issue resolving are easier.	The cloud is fully deployed at the third party site & org's connect to the third party by means of either a dedicated connection or through Internet.
Security and Data Privacy	Comparatively, it is more resistant to attacks than any other cloud and the security attacks are possible from an internal user only.	Cloud is relatively less secure and the security threat is from the third party and the internal employee.
Location	The data is usually stored in the same geographical location where the cloud users are present.	Cloud is located off site & when there is a change of location the data need to be transmitted through long distances.

Cloud Computing Model

	Services [CSNL]	Characteristics [CM SE Web]	Instances
IaaS	**1. Compute:** It includes virtual CPUs & virtual main memory for the Virtual Machines (VMs) **2. Storage:** It provides back-end storage 4 the VM images. **3.Network:**It provides virtual networking components such as virtual router, switch, & bridge for the VMs. **4. Load Balancers:** Provide load balancing capability at the infrastructure layer.	**1. Centralized management:** The resources distributed are controlled from any mgmt console. **2. Metered Services:** allows users to rent the computing resources instead of buying it. Users will be charged based on the amount of usage. **3. Shared infrastructure:** allows multiple IT users to share the same physical infrastructure. **4. Elasticity & Dynamic Scaling:** where the usage of resources can be increased or decreased according to the requirements. **5. Web access to the resources:** enables the IT users to access infra. resources over Internet.	NaaS - Network Staas -Storage BaaS - Backend DBaaS - Database DTaaS - Desktop
	Services [LADO]	**Characteristics [TOBCO Web] [Nov 19]**	**Instances**
PaaS	**1. Programming Languages:** Provide variety of Programming languages like Java, PHP, Python etc. for developing applications. **2. Application Frameworks:** PaaS vendors provide application development framework like Joomla, Word Press, and Sinatra etc. for application development. **3. Database:** PaaS providers provide some of the popular databases like ClearDB, Cloudant, Redis etc. so that application can communicate with the databases. **4. Other Tools:** It providers provide all the tools that are required to develop, test, and deploy an application.	**1. Diverse Client Tools:** It offer variety of client tools like Web User Interface (UI), (API) etc. help developers to choose tool of their choice. **2. All in One:** It offer services like programming languages to develop test & deploy applications in same Integrated Development Environment (IDE). **3. Built-in Scalability:** Provide built-in scalability to an app^{n}. This ensures that the appl^{n}. is capable of handling varying loads efficiently. **4. Collaborative Platform:** To enable collaboration among developers, PaaS providers provide tools for project planning & comm^{n}. **5. Offline Access:** to enable offline development, some of the PaaS providers allows the developer to synchronize their local IDE with the PaaS services. **6. Web access to the development platform:** Provides web access to the development platform that helps the developers to create, modify, test, & deploy applications on the same platform.	
	Services [BDNaM]	**Characteristics [One BHASM Web]**	**Instances**
SaaS	**1. Business Services:** SaaS provide a variety of business services that include ERP, CRM, billing, sales etc. **2. Document Management:** provide services to create, manage, & track electronic documents. **3. Social Networks:** Since the number of users of social networking sites is increasing rapidly, cloud computing is perfect match for handling the variable load. **4. Mail Services:** To handle the unpredictable number of users and the load on e-mail services.	**1. One to Many:** Services are delivered as one-to-many models whereas single instance of the application can be shared by multiple customers. **2. Better Scalability:** ensure a better scalability than traditional software **3. High Availability:** SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented. **4. API Integration:** has the capability of integrating with other soft. through std. APIs. **5. Multi-device Support:** Services can be accessed from any end user devices such as desktops, laptops, tablets, smart phones etc. **6. Centralized Management:** Services are hosted & managed from the central location **7. Web Access:** allow end users to access the application from any location of the device is connected to the Internet.	Testing as a Service (TaaS): This provides users with software testing capabilities such as generation of test data. API as a Service (APIaaS): allows users to explore functionality of Web services such as Google Maps. Email as a Service (EaaS): It provides users with an integrated system of emailing, office automation and integration services

IaaS	IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand. This allows users to maximize the utilization of computing capacities.
PaaS	PaaS provides the users ability to develop & deploy an application on the development platform provided by the service provider. In traditional application development, application will be developed locally & will be hosted in the central location. In stand-alone application development, the application will be developed by traditional development platforms. PaaS changes the application development from local machine to online. For eg- Google App Engine, Windows Azure Compute etc.
SaaS	SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider. Thus, the end users are exempted from managing or controlling an application the development platform. SaaS changes the way the software is delivered to the customers.

- **Other**

Communication as a Service (CaaS)	CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates the large capital investments. Examples are: Voice over IP (VolP), Instant Messaging (IM), and Collaboration and Videoconferencing application using fixed and mobile devices.
Data as a Service (DaaS)	DaaS provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. DaaS users have access to high-quality data in a centralized place and pay by volume or data type, as needed. However, as the data is owned by the providers, users can only perform read operations on the data. DaaS is highly used in geography data services and financial data services.
Security as a Service (SECaaS)	It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. Four mechanisms of Cloud security that are currently provided are Email filtering, Web content filtering, Vulnerability management and Identity management.
Identity as a Service (IDaaS)	It is an ability given to the end users; typically an enterprise; to access the authentication infrastructure that is built, hosted, managed & provided by the third party service provider. Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

Mobile Computing

Mobile Computing refers to the technology that allows transmission of data via a computer without having to be connected to fixed physical link. Mobile voice communication is widely established throughout the world & has a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send & receive data across cellular networks.

Components [M18, Nov 19]

Mobile Communication:	This refers to the infrastructure put in place to ensure that seamless & reliable communication goes on. This would include communication properties & concrete technologies.
Mobile Hardware:	This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA). At the back end, there are various servers like Application Servers, Database Servers, MCSS (Mobile Communications Server Switch) or a wireless gateway. The characteristics of mobile computing hardware are defined by the size, weight, primary storage, secondary storage, and means of input, means of output, battery life, expandability and durability of the device.

Mobile Software:	Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks of malware and access to personal information of mobile owner.

• Mobile Computing - Tangible Benefits [Memory - MUJRA]

M It enable to **Improve mgmt effectiveness** by enhancing information quality, information flow.

U It enables mobile **sale personnel to Update work order status** in real time, facilitating excellent communication.

J It provide **remote access** to **corporate knowledge base** at the **job location.**

R It provide mobile workforce with **remote access to w/ order detail** like, w/order location, contact info.

A It **facilitate access** to corporate services and information **at any time from anywhere.**

• Limitation [SHaPITH]

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

• Issues in Mobile Computing

Security Issues	Confidentiality	Preventing unauthorized users from gaining access to critical information of any particular user.
	Integrity	Ensures unauthorized modification, destruction or creation of information cannot take place.
	Availability	Ensuring authorized users getting the access they require.
	Legitimate	Ensuring that only authorized users have access to services.
	Accountability	Ensuring that the users are held responsible for their security related activities by arranging the user and activities are linked if and when necessary.
Bandwidth:	Bandwidth utilization can be improved by logging and compression. Technique of caching plays an important role. Cached data can improve query response time. Cached data can support disconnected operations.	
Power Consumption:	Mobile Computers will rely on their batteries as the primary power source. Power consumption should be minimized to increase battery life.	
Reliability, coverage, cap., & cost:	Wireless network is less reliable, have less geographic coverage and reduced bandwidth, are slower, and cost more than the wired-line network.	
End-to-end design & performance:	Since mobile computing involves multiple networks and multiple server platforms; end-to-end design and network response time estimates are difficult to achieve. "	

Business challenges:	Mobile computing also faces business challenges. This is due to the lack of trained professionals.

Bring Your Own Devices - BYOD

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

Advantages [N18, Nov 19] [Memory - HIIL Tech]

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

Risk [Memory NADI] [N18,Nov 19]

Network Risk	It is exemplified in **'Lack of Device Visibility'.** When company-owned devices are used by all employees, the org.'s IT practice has **complete visibility of devices connected to the network.** This helps to analyze traffic & data exchanged over the Internet.
Application Risk	It is normally exemplified and hidden in **'Application Viruses and Malware'.** Majority of employees' phones and smart devices that were connected to the corporate network weren't **protected by security software. (Quick heal)**
Device Risks	It is normally exemplified and hidden in **'Loss of Devices'.** A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the **device may hold sensitive corporate information.**
Implementation Risk	It is normally exemplified and hidden in **'Weak BYOD Policy'.** The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy.

Web 2.0

Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online.The **two major contributors of Web 2.0 are the technological advances enabled by Ajax (Asynchronous JavaScript and XML) & other applications such as RSS (Really Simple Syndication).** This refers to the **transition from static HTML Web pages to a more dynamic Web** that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication & more open sharing of information. Thus it can be said that the **migration is from the "read-only web" to "read-write web".**

• **Major Component** [Community Folk ka Blog File Share and Mash up kiya]

Communities	These are an online space formed by a **group of individuals** to **share their thoughts, ideas** & have variety of tools to promote Social Networking. There various tools available online to create communities, which are very cost efficient as well as easy to use.
Folksonomy	This allows the free classification of information available on the web, which helps the users to classify and find information, **using approaches such as tagging**.
Blogging	A blog is a journal, diary, or a personal website that is maintained on the internet, and it is updated frequently by the user. Blogging allows a user to make a post to web log / blog.
File Sharing	This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.
Wikis	A Wiki is a set of co-related pages on a particular sub. & allow users to share content. Wikis replace d complex document mgmt systems & are very easy to create & maintain.
Mash up	This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service.

Applications:

Social Media: Social Media/Social Network is an important application of web 2.0 as it provides a fundamental shift in the way people communicate and share information.

Marketing: Web 2.0 offers excellent opportunities for marketing by engaging customers in various stages of the product dev. cycle. It allows the marketers to collaborate with consumers on various aspects.

Education: Web 2.0 technologies can help the education scenario by providing students and faculty with more opportunities to interact and collaborate with their peers.

Web 3.0

Web 3.0 **also known as the Semantic Web**, describes sites wherein the computers will be **generated raw data on their own without direct user interaction.** Web 3.0 are considered as the **next logical step** in the evolution of the Internet & Web technologies.

Web 2.0 technologies allows the **use of read/write web**, blogs, interactive web applications, rich media, tagging/ folksonomy while sharing content, and also social networking sites focusing on communities. At the same time, Web 3.0 standard uses semantic web technology, drag & drop mash-ups, widgets, user behaviour, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users.

Web 3.0 technology **uses the "Data Web" Technology**, which features the data records that are publishable & reusable on the web through query- able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

• **Component:**

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

Green IT Practices

- Reduce Paper consumption [PRESS]

Reduce paper consumption by **use of email**

While printing paper, Use both side paper, use

Use **online marketing** rather than paper based.

- Recycle

a **Dispose e-waste** according to central, state and local regulations

b Discard used / unwanted electronic equipment in a environmentally responsible manner

c Manufacture must **offer recycling option** when product becomes unusable

d Recycle computers through manufactures recycling services

- Conserve Energy

a **Usd LCD** (Liq Crystal Display) instead of CRT (Cathode Ray Tube)

b **Power down** CPU during **inactive periods**

c Use notebook computer rather than desktop computers

d Use power management features to turnoff hard drives & display after several minutes of inactivity

e Employ alternative energy sources for computing workstations, servers, networks & data centre's

- Make env sound purchase Decision

Purchase of desktop computer, notebooks based on environmental attributes

Provide clear consistent set of performance criteria for the design of product

Use server storage virtualisation

- Develop a sustainable green computing plan

a Involve stakeholders to includes checklist, recycling policies and recommendation for purchasing green comp. equip.

b On-going communication about the campus commitment to green IT best practices to produce notable results

c **Use cloud computing** so resources of multiple org will be shared

d Encourage IT community to consider green computing practices and guidelines