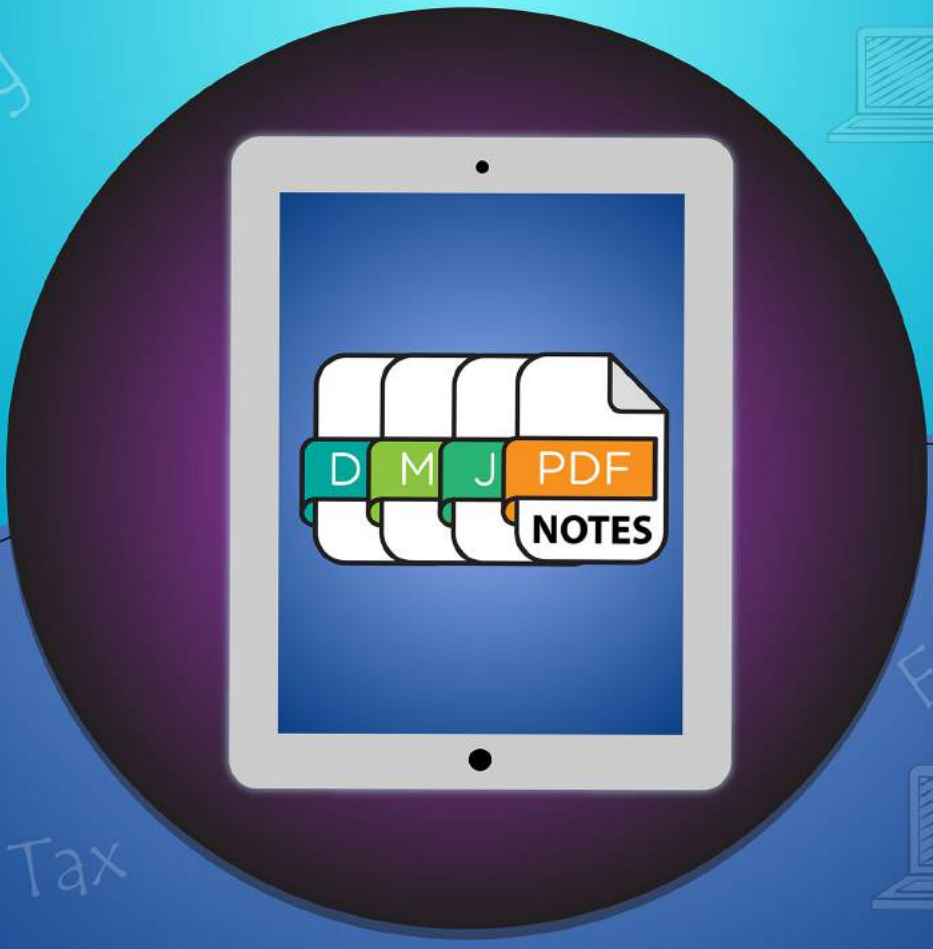
IndigoLearn

INDIGOLEARN.COM



Prepare for CA EXAMS LIKE NEVER BEFORE

1Fin by Indigolearn

#StudentFirst

Experience the world of e-learning

Online classes by faculties with AIRs

1FIN
BY INDIGOLEARN

Comprehensive coverage with cool visual effects

MCQ's with personalised analytics

Notes and flash cards at one click

Download our APP - 1FIN

IndigoLearn

CA Inter

Enterprise Information Systems

Paper-7A

Table of Contents

Ch:1 Automated Business Processes

1) What do you mean by Process?

Business Perspective

1. A Process is a co–ordinated and standardized flow of activities performed by people or machines, involving many functions or departments, to achieve a business objective.
2. A Process creates value for internal or external customers.
3. A Business is a collection of connected processes. These processes must be frequently re–aligned or re–connected in order to handle changing business environments and re–defined business objectives.

Systems Engineering Perspective

1. A Process is a sequence of events that uses inputs to produce outputs.
2. Sequences can involve many manual or machine activities, e.g. reading a file and transforming the file to a desired output format, or taking a customer order, filling that order, and issuing the Customer Invoice.

General Meaning

1. A Process comprises all the things done to provide the Stakeholders / Receivers, with what they expect to receive.
2. A Process is said to be complete when the Process delivers a clear product or service to an external stakeholder or another internal process.
3. The lifecycle of an end–to–end process is from the original trigger for the process, and runs upto the ultimate stakeholder satisfaction.

2) Differentiate between Functional Organisation and Process Organisation.

Functional Organisation vs Process Organisation

Aspect	Functional Organisation	Process Organisation
Viewpoint	Traditional View, considering an Entity as comprising of different departments / functions.	Comparatively refined view, considering an Entity as comprising of inter–linked processes.
Sub–Parts of Entity	Traditional Organizations are viewed as composed of Departments and Functional Stages.	This concept views Organizations as networks or systems of processes.
Work Unit	Department	Team
Key Figure	Functional Executive	Process Owner
Activity /work done	Every Department performs certain **specified functions**.	Every Process **creates value** for internal or external customers.
Benefits	(a) Focus on functional excellence and specialization. (b) Easier to implement work balancing because workers have similar skills.	(a) Responsive to market requirements. (b) Improved communication and collaboration between different functional tasks.

	(c) Clear management direction on how work should be performed. (d) Specialists / Experts can be employed for each function.	(c) Performance measurements can be aligned with process goals. (d) Creates better Team Spirit in Employees.
Weaknesses	(a)There may be barriers to communication between different functions. (b) Poor handover between functions, leading to deficient customer service. (c) Lack of end–to–end focus to optimize organizational performance.	(a) Duplication of functional expertise. (b) Inconsistency of functional performance between Processes. (c) Increased operational complexity. (d) Difficult to fix responsibility in certain situations.
Strategic Value	Supports **Cost Leadership** Strategy.	Supports **Differentiation** Strategy.

3) Write short notes on Process Management.

Process Management views an organisation as a system of inter–linked processes which involves concerted efforts to map, improve and adhere to Organisational processes.

Significance

1. Process Management is a functional group including (but not limited to) Operations Management, Supply Chain Management, Finance and Accounting, Marketing, and General Management.
2. Process Management should be implemented to ensure effective streamlining of processes.
3. Process Orientation is at the core of BPM. So, multi–functional Processes should be properly integrated.
4. Process Management provides a sequence of analytical tools that are essential to the modern Project Manager, Analyst, and Management Consultant.
5. A process–oriented corporate culture is useful to adapt to changes in management at the operational level, i.e. improvement and control of the processes essential to the Entity's goals.

4) What do you mean by Business Process?

(a) A Business Process is a prescribed sequence of work steps, performed in order to produce a desired result for the Entity.

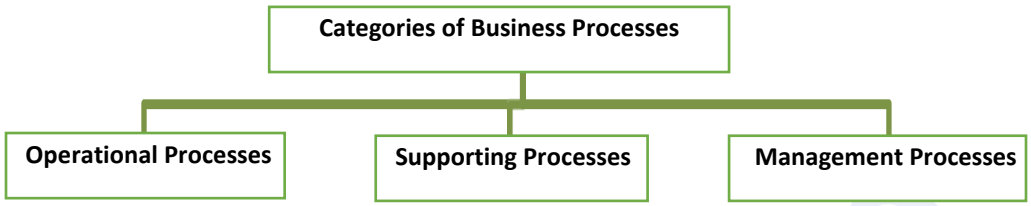
(b) A Business Process is initiated by a particular kind of event, has a well–defined beginning and end, and is usually completed in a relatively short period.

(c)The number and type of Business Processes and how the processes are performed vary across Entities, and is also influenced by the extent of automation.

(d) Business Process Management (BPM) is the achievement of an Entity's objectives through the improvement, management and control of essential business processes.

5) Explain the different ways in which Business Processes can be classified.

Depending on the organization, industry and nature of work; business processes are often broken up into different categories as shown in the Fig.



a) Operational Processes (or Primary Processes)

Operational or **Primary Processes** deal with the core business and value chain. These processes deliver value to the customer by helping to produce a product or service. Operational processes represent essential business activities that accomplish business objectives, e.g. generating revenue - Order to Cash cycle (O2C), Procurement – Purchase to Pay (P2P) cycle.

b) Supporting Processes (or Secondary Processes)

Supporting Processes back core processes and functions within an organization. Examples of supporting or management processes include Accounting, Human Resource (HR) Management and workplace safety. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. However, it should be noted that hiring the right people for the right job has a direct impact on the efficiency of the enterprise.

Example The main HR Process Areas are grouped into logical functional areas - Recruitment and Staffing; Goal Setting; Training and Development; Compensation and Benefits; Performance Management; Career Development and Leadership Development.

c) Management Processes

Management Processes measure, monitor and control activities related to business procedures and systems. Examples of management processes include internal communications, governance, strategic planning, budgeting, and infrastructure or capacity management. Like supporting processes, management processes do not provide value directly to the customers. However, it has a direct impact on the efficiency of the enterprise.

6) What is Enterprise Information System? Explain its advantages?

An **Enterprise Information System (EIS)** may be defined as any kind of information system which improves the functions of an enterprise business processes by integration.

- EIS provides a technology platform that enable Entities to integrate and coordinate their Business Processes.

- EIS collects data from all Business Processes– (a) Manufacturing & Production, (b) Sales & Marketing, (c) Finance and Accounting, and (d) Human Resources and Personnel, and stores the data in single Central Data Repository.
- By improving the performance, accuracy and efficiency of the key business processes, the Entity is made more efficient and responsive to Customer and Employee needs.

Advantages of using EIS includes –

a) high quality services and operational efficiency,
b) reduced Service Cycles, Product Development Cycles and Marketing Life Cycles,
c) increased business productivity and cost savings,
d) increased Customer Satisfaction,
e) smooth flow of information to proper Business Processes,
f) better coordination amongst various Business Processes,
g) dealing with large volumes of data,
h) usability at all levels of an Entity,
i) automation of Business Processes,
j) sharing of relevant information across all Functional Levels and Management Hierarchies, etc.

7) What do you mean by Business Process Automation (BPA)? What are its Objectives and Benefits?

Business Process Automation (BPA) refers to removing the human element from existing business processes by automating the repetitive or standardized process components. BPA is the automation of business processes. In BPA, Firms seek to identify any unnecessary amount of work (repetitive and tedious work), and eliminate inefficient labour. Business Process Automation (BPA) is a strategy to automate, optimize and streamline business processes, and benefit the enterprise in terms of cost, time and efforts.

- **Confidentiality:** To ensure that data is only available to persons who have right to see the same;
- **Integrity:** To ensure that no un-authorized amendments can be made in the data;
- **Availability:** To ensure that data is available when asked for; and
- **Timeliness:** To ensure that data is made available in at the right time.

Major benefits of automating Business Processes are as follows:

a. **Quality and Consistency:** Ensures that every action is performed identically - resulting in high quality, reliable results and stakeholders will consistently experience the same level of service.
b. **Time Saving:** Automation reduces the number of tasks employees would otherwise need to do manually. It frees up time to work on items that add genuine value to the business, allowing innovation and increasing employees' levels of motivation.
c. **Visibility:** Automated processes are controlled and consistently operate accurately within the defined timeline. It gives visibility of the process status to the organization.
d. **Improved Operational Efficiency:** Automation reduces the time it takes to

achieve a task, the effort required to undertake it and the cost of completing it successfully. Automation not only ensures systems run smoothly and efficiently, but that errors are eliminated and best practices are constantly leveraged.

8) Explain the steps in Business Process Automation.

The steps to go about implementing Business Process Automation are:

(a). Step 1: Define why we plan to implement a BPA?

A list of generic reasons for going for BPA may include any or combination of the following:

- Errors in manual processes leading to higher costs.
- Payment processes not streamlined, due to duplicate or late payments, missing early pay discounts, and losing revenue.
- Paying for goods and services not received.
- Poor debtor management leading to high invoice aging and poor cash flow.
- Not being able to find documents quickly during an audit or lawsuit or not being able to find all documents.
- Lengthy or incomplete new employee or new account on-boarding.
- Unable to recruit and train new employees, but where employees are urgently required.
- Lack of management understanding of business processes.
- Poor customer service.

(b). Step 2: Understand the rules / regulation under which enterprise needs to comply with?

One of the most important steps in automating any business process is to understand the rules of engagement, which include following the rules, adhering to regulations and following document retention requirements.

This governance is established by a combination of internal corporate policies, external industry regulations and local, state, and central laws**.**

It is important to understand that laws may require documents to be retained for specified number of years and in a specified format. Entity needs to ensure that any BPA adheres to the requirements of law.

Step 3: Document the process, we wish to automate

The following aspects need to be kept in mind while documenting the present process:

- What documents need to be captured?
- Where do they come from?
- What format are they in: Paper, FAX, email, PDF etc.?
- Who is involved in processing of the documents?

- What is the impact of regulations on processing of these documents?
- Can there be a better way to do the same job?
- How are exceptions in the process handled?

Step 4: Define the objectives/goals to be achieved by implementing BPA

- **Measurable:** Easily quantifiable in monetary terms,
- **Attainable:** Achievable through best efforts,
- **Relevant:** Entity must be in need of these, and
- **Timely**: Achieved within a given time frame.

Step 5: Engage the business process consultant

This is again a critical step to achieve BPA. To decide as to which company/ consultant to partner with, depends upon the following:

- Objectivity of consultant in understanding/evaluating entity situation.
- Does the consultant have experience with entity business process?
- Is the consultant experienced in resolving critical business issues?
- Whether the consultant can recommend and implementing a combination of hardware, software and services as appropriate to meeting enterprise BPA requirements?
- Does the consultant have the required expertise to clearly articulate the business value of every aspect of the proposed solution?

Step 6: Calculate the RoI for project

- Savings in Employee Salary by not having to replace those due to attrition.
- Cost of Space regained from paper, file cabinets, reduced.
- Eliminating Fines to be paid by Entity due to delays being avoided.
- Reducing the cost of audits and lawsuits.
- Lower Interest Cost and better Cash Flow management by availing early payment discounts, avoiding duplicate payments, collecting Accounts Receivable faster, etc.
- New Revenue Generation opportunities.
- Revenue by way of charging for instant access to records (e.g. Public Information, Student Transcripts, Medical Records, etc.)
- Building business by providing superior levels of customer service, higher goodwill, etc.

Step 7: Developing the BPA

Once the requirements have been document, ROI has been computed and top management approval to go ahead has been received, the consultant develops the requisite BPA. The developed BPA needs to meet the objectives for which the same is being developed.

Step 8: Testing the BPA

Once developed, it is important to test the new process to determine how well it works and identify where additional "exception processing" steps need to be included. The process of testing is an iterative process, the objective being to remove all problems during this phase.

Testing allows room for improvements prior to the official launch of the new process, increases user adoption and decreases resistance to change. Documenting the final version of the process will help to capture all of this hard work, thinking and experience which can be used to train new people.

9) Explain the various types of Flowcharts?

(a) System Outline Chart

System Outline Charts merely list the Inputs, Files processed and the Outputs without considering their sequence.

(b) System Flowchart

• A System Flowchart represents the overall view of the data flow and operations of a system, with a diagram drawn logically, and illustrates the correct flow of data or documents.

• It represents flow of documents, the operations or activities performed, the persons or workstations. It also reflects the relationship between Inputs, Processing and Outputs.

• In a Manual System, a System Flowchart may comprise several Flowcharts, prepared separately, such as Documents Flowchart, Activity Flowchart, etc.

• In a Computer System, the System Flowchart mainly consists of – (i) sources from which input data is prepared and the medium or devices used, (ii) the processing steps or sequence of operations involved, and (iii) the intermediary and final outputs prepared and the medium and devices used for their storage.

(c) Run Flowcharts

• Run Flowcharts are prepared from the Systems Flowchart and show the reference of computer operations to be performed.

• They expand the detail of each computer box on the System Flowchart showing Inputs, Files, and Outputs relevant to each run and the frequency of each run. (d)

(d) Program Flowchart

• Program Flowcharts are diagrammatic representation of the data processing steps to be performed within a computer program.

• They are used to translate the elementary steps of a procedure into a program of coded instructions for the Computer to operate effectively.

• They are used to depict the scientific, arithmetic and logical operations or steps which must be accomplished to solve the computer application problem.

(e) Cross Functional Flowcharts

• These are diagrams of Business Processes, and helps in identifying the role and responsibilities of each Department / Business Unit, for each part of the overall activity.
• The Flowchart is divided into different Units (called **Swimlanes**), each representing a particular Department / Business Unit.
• All activities and processes under the control of that Department / Business Unit, are depicted within that Swimlane. All such activities are inter–connected to form the overall Business Process Flowchart.

10) What are the benefits of Flowcharts?

Advantages of Flowcharts

(i) Quicker grasp of relationships - The relationship between various elements of the application program/business process must be identified. Flowchart can help depict a lengthy procedure more easily than by describing it by means of written notes.

(ii) Effective Analysis - The flowchart becomes a blue print of a system that can be broken down into detailed parts for study. Problems may be identified and new approaches may be suggested by flowcharts.

(iii) Communication - Flowcharts aid in communicating the facts of a business problem to those whose skills are needed for arriving at the solution.

(iv) Documentation - Flowcharts serve as a good documentation which aid greatly in future program conversions. In the event of staff changes, they serve as training function by helping new employees in understanding the existing programs.

(v) Efficient coding - Flowcharts act as a guide during the system analysis and program preparation phase. Instructions coded in a programming language may be checked against the flowchart to ensure that no steps are omitted.

(vi) Program Debugging - Flowcharts serve as an important tool during program debugging. They help in detecting, locating and removing mistakes.

(vii) Efficient program maintenance - The maintenance of operating programs is facilitated by flowcharts. The charts help the programmer to concentrate attention on that part of the information flow which is to be modified.

(viii) Identifying Responsibilities - Specific business processes can be clearly identified to functional departments thereby establishing responsibility of the process owner.

(ix) Establishing Controls - Business process conflicts and risks can be easily identified for recommending suitable controls.

11) What are the limitations of Flowcharts?

Limitations of Flowchart

(i) Complex logic – Flowchart becomes complex and clumsy where the problem logic is complex. The essentials of what is done can easily be lost in the technical details of how it is done.

(ii) Modification – If modifications to a flowchart are required, it may require complete re-drawing.

(iii) Reproduction – Reproduction of flowcharts is often a problem because the symbols used in flowcharts cannot be typed.

(iv) Link between conditions and actions – Sometimes it becomes difficult to

establish the linkage between various conditions and the actions to be taken there upon for a condition.

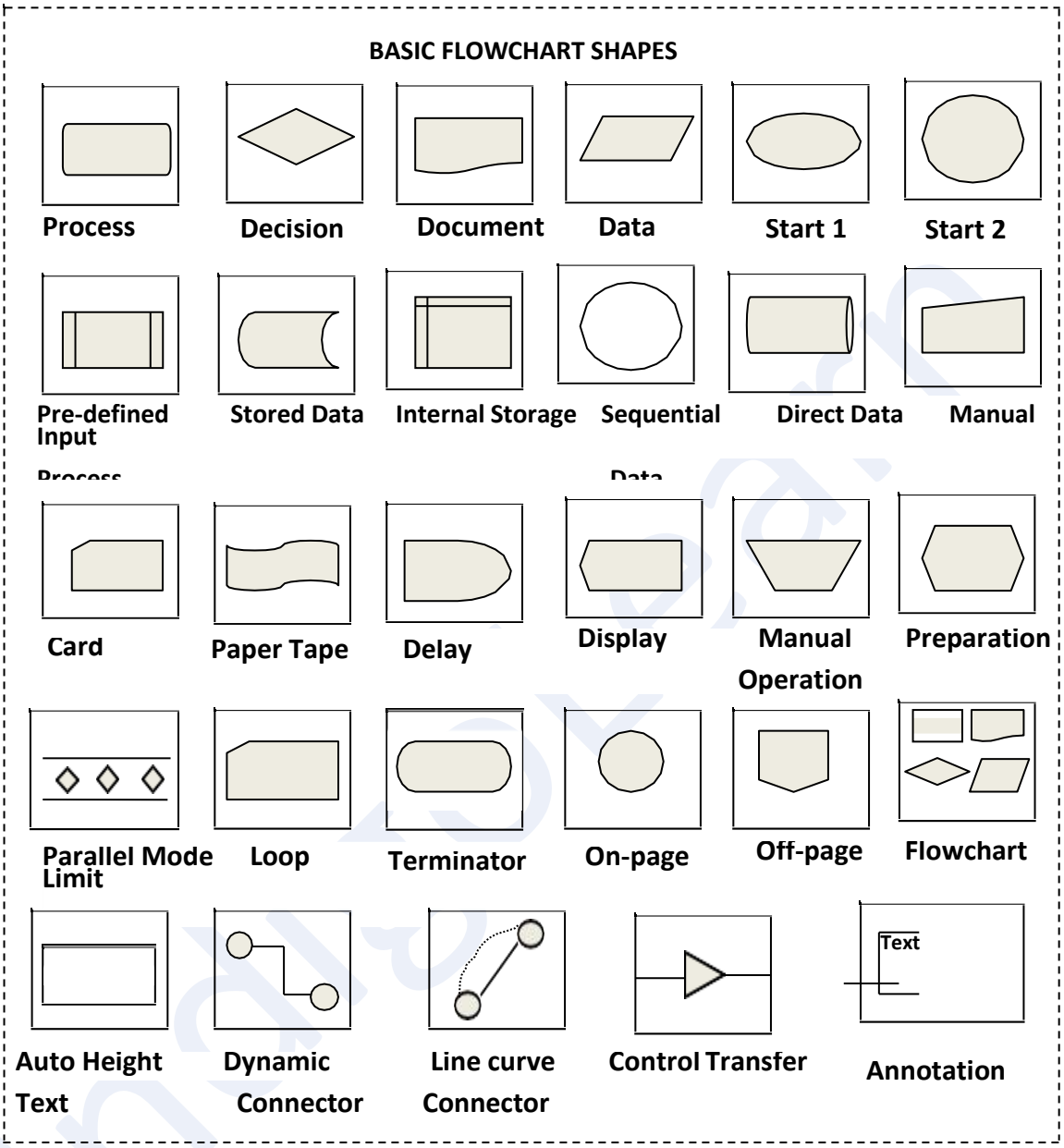
(v) **Standardization –** Program flowcharts, although easy to follow, are not such a natural way of expressing procedures as writing in English, nor are they easily translated into Programming language.

12) What are the commonly used Symbols in Flowcharts?

Symbols: On a System Flowchart, each component is represented by a **symbol** that visually suggests its function. A System Flowchart's symbols represent physical components, and the mere act of drawing one implies a physical decision.

Flow Lines: The Symbols are linked by **Flow Lines**. A given Flow Line might represent – (i) a Data Flow, (ii) a Control Flow, or (ii) a Hardware Interface.

Direction: By convention, the direction of flow is from the top left to the bottom right, and
Arrowheads must be compulsorily used when that convention is not followed. However, Arrowheads are recommended even when the convention is followed because they help to clarify the documentation.
Symbols used in System Flowcharts are given below –



13) Briefly explain the steps in Flowcharting a Business Process.

1. **Identify the Business Process** to be documented, and its significance and relevance in the context of the Entity's Business Objectives and Goals.
2. Obtain a **complete understanding** of the Process Flow, in terms of – (a) Business Units / Departments involved, (b)Process Owners / Data Owners, (c) Inputs used, (d) Authorizations required at various stages, etc.
3. Prepare a **Rough Diagram** of the Business Process from the above, and discuss the same with the Business Process Owner to confirm the understanding. [**Note:** The Business Process Owner is responsible for ensuring that adequate controls are implemented, to mitigate any perceived business process risks.]
4. Identify Control Weaknesses, Process Deficiencies, Duplication of Activities, Redundant Processes, etc. and the corrective measures required to handle them.

5. Establish the finalized list of **Activities** in each Process Step, and the **responsibility levels** for each activity.
6. Identify the **Starting Point** of the Process, i.e. trigger point or input that the Business seeks to convert into an output. Generally, Triggers / Starting Points may be –
(a) **External Events** – e.g. Sales Order by a Customer, Intimation of Due Date for filing Returns, etc.
(b) **Content Arrival** – i.e. arrival of a new document or similar content, e.g. preparation and posting of Purchase Requisition by Stores Department triggers action by the Purchase Department.
(c) **Human Intervention** – e.g. Rate Change request by a Supplier, Customer Complaints for Products, etc.
7. Identify the **sub–components** or Steps of the Process and the appropriate Symbols thereof – [This is called Business Processing Modelling Notation (**BPMN**)].

Ite	Description
(a) Events	Events require no action from the Business as such, e.g. Customer Order, Application for Credit Limit increase, etc.
(b) Activities	These are the Entity's Responses to the Events / Inputs, e.g. checking of credit limit, checking of stock availability at Warehouse, etc. A Processing Step or Activity is denoted by a Rectangular Box.
(c)Decision Gateways	These are Decision Steps that have two types of responses – "Yes" or "No", and the further path of the process is decided based on such response. These are denoted by Diamond Shapes.
(d) Arrows	The Events, Activities and Decision Gateways are linked and inter–connected by – (a) Solid Arrows (for Activity Flows), and (b) Dashed Arrows (for Message / Information Flows).

8. Identify the Business Unit /Department/Person, that is responsible for each Step, for creating various "**Swimlanes**".
9. Draw the Flowchart based on the above linkages and processes, and obtain **Final Approval** from the Entity.

14) Write short notes on Data Flow Diagrams?

Data Flow Diagrams Data Flow Diagrams (DFD) show the flow of data or information from one place to another. DFDs describe the processes showing how these processes link together through data stores and how the processes relate to the users and the outside world. It is used to – (i) document existing systems, and (ii) plan and design new systems. DFDs may be partitioned into levels that represent increasing information flow and functional detail. DFDs provide a mechanism for Functional Modelling as well as Information Flow Modelling.
DFD basically provides an overview of:

a. What data a system process;
b. What transformations are performed;
c. What data are stored;
d. What results are produced and where they flow.

It is mainly used by technical staff for graphically communicating between systems analysts and programmers

15) Outline the concept of Enterprise Risk Management (ERM)?

Following features in Enterprise Risk Management (ERM) provides enhanced capabilities to enable management to operate more effectively in environments filled with risks:

- **Align risk appetite and strategy:** Risk appetite is the degree of risk, on a broad- based level that an enterprise is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.
- **Link growth, risk and return:** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
- **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses - risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses:** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
- **Identify and manage cross-enterprise risks:** Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
- **Provide integrated responses to multiple risks:** Business processes carry many inherent risks and ERM enables integrated solutions for managing the risks.
- **Seize opportunities:** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- **Rationalize capital:** More robust information on an entity's total risk allows management to more effectively assess overall capital needs and improve capital allocation.

16) What are the benefits of ERM?

ERM provides enhanced capability to do the following:

- **Align risk appetite and strategy:** Risk appetite is the degree of risk, on a broad-based level that an enterprise (any type of entity) is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.
- **Link growth, risk and return:** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.

- **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses:** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
- **Identify and manage cross-enterprise risks:** Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
- **Provide integrated responses to multiple risks:** Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.
- **Seize opportunities:** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- **Rationalize capital:** More robust information on an entity's total risk allows management to more effectively assess overall capital needs and improve capital allocation.

17) What are the components of ERM?

ERM framework consists of eight interrelated components that are derived from the way management runs a business, and are integrated with the management process. These components are as follows:

(I) **Internal Environment:** The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. Management sets a philosophy regarding risk and establishes a risk appetite. The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

(II) **Objective Setting:** Objectives should be set before management can identify events potentially affecting their achievement. ERM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite.

(III) **Event Identification:** Potential events– internal and external – that might have an impact on the entity should be identified. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Opportunities are channeled back to management's strategy or objective-setting processes. Management identifies inter-relationships between potential events and may categorize events to create and reinforce a common risk language across the entity.

(IV) **Risk Assessment:** Identified risks are analyzed to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible

results may be associated with a potential event, and management needs to consider them together.

(V) **Risk Response:** Management selects an approach or set of actions to align assessed risks with the entity's risk tolerance and risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

(VI) **Control Activities:** Policies and procedures are established and executed to help ensure that the risk responses that management selected, are effectively carried out.

18) What are the various types of Risk Management Strategies that may be adopted by an Entity?

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained below:

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

19) What legal and regulatory compliances are called for in case of Business Process Automation?

Legal, Regulatory and Compliance Requirements in relation to BPA and Risk Management include the following –

- **Directors' Responsibility Statement** in relation to Maintenance of Accounting Records, Internal Financial Controls, [Sec.134 of Companies Act, 2013],
- **Reporting Requirements of Auditors** in relation to Maintenance of Accounting Records, Internal Financial Controls, [Sec.143 of Companies Act, 2013],
- **Corporate Governance** Requirements under Companies Act, 2013, Compliance with the requirements of the Information Technology Act, 2000.

20) What are the various types of Business Risks?

Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence.

Business Risks: Businesses face all kinds of risks related from serious loss of profits to even bankruptcy and are discussed below:

- **Strategic Risk**: These are the risks that would prevent an organization from accomplishing its objectives (meeting its goals). **Examples** include risks related to strategy, political, economic, regulatory, and global market conditions; also, could include reputation risk, leadership risk, brand risk, and changing customer needs
- **Financial Risk:** Risk that could result in a negative financial impact to the organization (waste or loss of assets). **Examples** include risks from volatility in foreign currencies, interest rates, and commodities; credit risk, liquidity risk, and market risk.
- **Regulatory (Compliance) Risk:** Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations. **Examples** include Violation of laws or regulations governing areas such as environmental, employee health & safety, local tax or statutory laws etc.
- **Operational Risk**: Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations. **Examples** include risks related to the organization's human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration.
- **Hazard Risk:** Risks that are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc.
- **Residual Risk:** Any risk remaining even after the counter measures are analyzed and implemented is called Residual Risk. An organization's management of risk should consider these two areas: Acceptance of residual risk and Selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. Residual risk must be kept at a minimal, acceptable level.

21) What are the types of Risks in BPA?

Risk Types in BPA: BPA–related Risks include the following –

(a) **Input:** Risk that all input transaction data may not be accurate, complete and authorized.

(b) **Transmission:** Risk that all the Files and Data transmitted may not be processed accurately and completely, due to Network error or system failure.

(c) **Processing:** Risk that valid input data may not be processed properly due to program errors or other reasons.

(d) **Output:** Risk that output is not complete and accurate, or risk that output is distributed to Unauthorized Personnel.

(e) **Access:** Risk that the Entity's Master Data and/or Transaction Data may be changed by Unauthorized Personnel due to weak access controls.

(f) **Backup:** Risk that all data & programs may be lost if there is no proper backup in the event of a disaster and the Entity's Operations could come to a standstill, due to lack of adequate infrastructure settings.

22) Controls in BPA may be manual, automated, or semi–automated. Explain with example?

Types of Control: Based on the mode of implementation, Internal Controls may be – (a) manual, (b) automated, or (c) semi–automated (partially manual and partially automated).

Area	Order to Cash (O2C)	Purchase to Pay (P2P)
Controls	Verification of – (a) Credit Limits of Customers, before Invoicing and Dispatch of Goods, (b) Availability of Warehouse Stock, to meet the Customer's Order Quantity requirements.	Verification of whether – (a) Supplier's Invoice shows Quantity and Price of Materials as per the Entity's Purchase Order, (b) Ordered Quantity of Goods has been actually received by the Entity.
Manual	Both (a) and (b) are done by manual processes.	Both (a) and (b) are done by manual processes.
Automated	Both (a) and (b) are done by System Verification.	Both (a) and (b) are done by System Verification.
Semi–Automated	(b) is done by System Verification, whereas (a) is done by Manual Processes, along with authorization of exceptions / deviations for special customers.	(b) is done by System Verification, whereas (a) is done by Manual Process, along with reconciliation of deviations/ variations, if any.

23) What are the purposes of Controls?

Control is defined as policies, procedures, practices and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

Purposes of Controls: An Internal Control System –

(a) ensures the orderly and efficient conduct of an Entity's business,

(b) promotes adherence to management policies,

(c) helps safeguarding the Entity's Assets,

(d) aids in the prevention and detection of fraud and error,

(e) helps in ensuring the accuracy and completeness of the accounting records,

(f) facilitates the effectiveness and efficiency of operations,

(g) assists compliance with applicable laws and regulations,

(h) helps the reliability of internal and external Financial Reporting on timely basis.

24) Checking of Controls is required at three levels, viz. Configuration, Masters and Transaction. Explain.

In computer systems, controls should be checked at three levels, namely **Configuration**, **Masters** and **Transaction** level.

Configuration

- Configuration refers to the way a software system is set up.
- Configuration is the methodical process of defining options that are provided.
- When any software is installed, values for various parameters should be set up (configured) as per policies and business process work flow and business process rules of the enterprise.
- The various modules of the enterprise such as Purchase, Sales, Inventory, Finance, User Access etc. must be configured.
- Configuration will define how software will function and what menu options are displayed.

Masters

- Masters refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory, and Finance etc.
- These drives how the software will process relevant transactions.
- The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed. Examples are Vendor Master, Customer Master, Material Master, Accounts Master, Employee Master etc.
- Any changes to these data have to be authorized by appropriate personnel and these are logged and captured in exception reports.

  example: The Customer Master will have the credit limit of the customer. When an invoice is raised, the system will check against the approved credit limit and if the amount invoiced is within the credit limit, the invoice will be created if not the invoice will be put on "credit hold" till proper approvals are obtained.

Transactions

- Transactions refer to the actual transactions entered through menus and functions in the application software, through which all transactions for specific modules are

initiated, authorized or approved.

example: Sales transactions, Purchase transactions, Stock transfer transactions, Journal entries and Payment transactions.

25) Write short notes on review of BPA from Risk and Control Perspectives?

Implementation or review of specific business process can be done from risk or control perspective

(a) Risk Perspective

1. Each key sub–process or activity performed in a Business Process should be examined, to look at existing and related control objectives and existing controls and the residual risks after application of controls.
2. The Residual Risk should be knowingly accepted by the Management

(b) Control Perspective

For each key sub–process or activity, the Entity should consider the following –

1. What is sought to be achieved by implementing controls,
2. Whether risks are mitigated by controls which are implemented at present,
3. What are the residual risks, and
4. Whether there is need to complement / add more controls.

26) Explain a few Risks and Control Objectives in O2C Process at Masters Level?

Risks and Controls related to the Order to Cash (O2C) business process are as follows:

Master Level

Risks	Controls
The customer master file is not maintained properly and the information is not accurate.	The customer master file is maintained properly and the information is accurate.
Invalid changes are made to the customer master file.	Only valid changes are made to the customer master file.
All valid changes to the customer master file are not input and processed.	All valid changes to the customer master file are input and processed.
Changes to the customer master file are not accurate.	Changes to the customer master file are accurate.
Changes to the customer master file are not processed in a timely manner.	Changes to the customer master file are processed in a timely manner.
Customer master file data is not up-to-date and relevant.	Customer master file data is up to date and relevant.

27) Explain a few Risks and Control Objectives in O2C Process at Transactions Level.

Risks and Controls related to the Order to Cash (O2C) business process are as follows:

Transaction Level

Risk	Control
Orders are processed exceeding customer credit limits without approvals.	Orders are processed only within approved customer credit limits.
Orders are not approved by management as to prices and terms of	Orders are approved by management as to prices and terms of sale.
Orders and cancellations of orders are not input accurately.	Orders and cancellations of orders are input accurately.
Order entry data are not transferred completely and accurately to the shipping and invoicing activities.	Order entry data are transferred completely and accurately to the shipping and invoicing activities.
All orders received from customers are not input and processed.	All orders received from customers are input and processed.
Invalid and unauthorized orders are input and processed.	Only valid and authorized orders are input and processed.

28) Explain a few Risks and Control Objectives in P2P Process at Masters Level?

Risks and Controls related to the Order to Cash (P2P) business process are as follows:

Master Level

Risk	Control
Unauthorized changes to supplier master file.	Only valid changes are made to the supplier master file.
All valid changes to the supplier master file are not input and processed.	All valid changes to the supplier master file are input and processed.
Changes to the supplier master file are not correct.	Changes to the supplier master file are accurate.
Changes to the supplier master file are delayed and not processed in a timely manner.	Changes to the supplier master file are processed in a timely manner.
Supplier master file data is not up to date.	Supplier master file data remain up to date.
System access to maintain vendor masters has not been restricted to the authorized users.	System access to maintain vendor masters has been restricted to the authorized users.

29) Explain a few Risks and Control Objectives in P2P Process at Transactions Level?

Risks and Controls related to the Order to Cash (P2P) business process are as follows:
Transaction Level

Risk	Control
Unauthorized purchase requisitions are ordered.	Purchase orders are placed only for approved requisitions.
Purchase orders are not entered correctly in the system.	Purchase orders are accurately entered.
Purchase orders issued are not input and processed.	All purchase orders issued are input and processed.
Amounts are posted in accounts payable for goods or services not received.	Amounts posted to accounts payable represent goods or services received.
Amounts posted to accounts payable are not properly calculated and recorded.	Accounts payable amounts are accurately calculated and recorded.
Amounts for goods or services received are not input and processed in accounts payable.	All amounts for goods or services received are input and processed to accounts payable.

30) Explain a few Risks and Control Objectives in Inventory Process at Masters Level?

Risks and Controls related to the Inventory process are as follows:
Master Level

Risk	Control
Invalid changes are made to the inventory management master file.	Only valid changes are made to the inventory management master file.
Invalid changes to the inventory management master file are input and processed.	All valid changes to the inventory management master file are input and processed.
Changes to the inventory management master file are not accurate.	Changes to the inventory management master file are accurate.
Changes to the inventory management master file are not promptly processed.	Changes to the inventory management master file are promptly processed.
Inventory management master file data is not up to date.	Inventory management master file data remain up to date.
System access to maintain inventory masters has not been restricted to the authorized users.	System access to maintain inventory masters has been restricted to the authorized users.

31) Explain a few Risks and Control Objectives in Inventory Process at Transactions Level?

Risks and Controls related to the Inventory process are as follows:

Transaction Level

Risk	Control
Adjustments to inventory prices or quantities are not recorded accurately.	Adjustments to inventory prices or quantities are recorded accurately.
Raw materials are received and accepted without valid purchase orders.	Raw materials are received and accepted only if they have valid purchase orders.
Raw materials received are not recorded accurately.	Raw materials received are recorded accurately.
Raw materials received are not recorded in system.	All raw materials received are recorded.
Receipts of raw materials are not recorded promptly and not in the appropriate period.	Receipts of raw materials are recorded promptly and in the appropriate period.
Defective raw materials are not returned promptly to suppliers.	Defective raw materials are returned promptly to suppliers.

32) What are the components of Human Resources Management Cycle?

The Human Resources (HR) Life Cycle refers to human resources management and covers all the stages of an employee's time within a specific enterprise and the role the human resources department plays at each stage. Typical stage of HR cycle includes the following:

(b) **Recruiting and On-boarding: Recruiting** is the process of hiring a new employee. The role of the human resources department in this stage is to assist in hiring. This might include placing the job ads, selecting candidates whose resumes look promising, conducting employment interviews and administering assessments such as personality profiles to choose the best applicant for the position. **On boarding is** the process of getting the successful applicant set up in the system as a new employee.

(c) **Orientation and Career Planning: Orientation** is the process by which the employee becomes a member of the company's work force through learning her new job duties, establishing relationships with co-workers and supervisors and developing a niche**. Career planning** is the stage at which the employee and her supervisors work out her long-term career goals with the company. The human resources department may make additional use of personality profile testing at this stage to help the employee determine her best career options with the company.

(d) **Career Development: Career development** opportunities are essential to keep an employee engaged with the company over time. After an employee, has established himself at the company and determined his long-term career objectives, the human resources department should try to help him meet his goals, if they're realistic. This can include professional growth and training to prepare the employee for more responsible positions with the company. The company also assesses the employee's work history and performance at this

stage to determine whether he has been a successful hire.

(e) **Termination or Transition:** Some employees will leave a company through retirement after a long and successful career. Others will choose to move on to other opportunities or be laid off. Whatever the reason, all employees will eventually leave the company. The role of HR in this process is to manage the transition by ensuring that all policies and procedures are followed, carrying out an exit interview.

33) Explain a few Risks and Control Objectives in HR Process at Configurations Level?

Risks and Control Objectives for Human Resource Process at Configuration Levels are as follows:

Risk	Control Objective
Employees who have left the company continue to have system access.	System access to be immediately removed when employees leave the company.
Employees have system access in excess of their job requirements.	Employees should be given system access based on a "need to know" basis and to perform their job function.

34) Explain a few Risks and Control Objectives in HR Process at Masters Level?

Risks and Control Objectives for Human Resource Process at Master Levels are as follows:

Risk	Control Objective
Additions to the payroll master files do not represent valid employees.	Additions to the payroll master files represent valid employees.
New employees are not added to the payroll master files.	All new employees are added to the payroll master files.
Terminated employees are not removed from the payroll master files.	Terminated employees are removed from the payroll master files.
Employees are terminated without following statutory requirements.	Employees are terminated only within statutory requirements.
Deletions from the payroll master files do not represent valid terminations.	Deletions from the payroll master files represent valid terminations.
Invalid changes are made to the payroll master files.	Only valid changes are made to the payroll master files.

35) What are the components of Fixed Assets Management Cycle?

Fixed Assets process ensures that all the fixed assets of the enterprise are tracked for the purposes of financial accounting, preventive maintenance, and theft deterrence. Fixed assets process ensures that all fixed assets are tracked and fixed asset record maintains details of location, quantity, condition, and maintenance and depreciation status.
Components of Fixed asset Management Cycle:

- **Procuring an asset:** An asset is most often entered into the accounting system; when the invoice for the asset is entered; into the accounts payable; or purchasing module of the system.
- **Registering or Adding an asset:** Most of the information needed to set up the asset for depreciation is available at the time the invoice is entered. Information entered at this stage could include; acquisition date, placed-in-service date, description, asset type, cost basis, depreciable basis etc.
- **Adjusting the Assets:** Adjustments to existing asset information is often needed to be made. Events may occur that can change the depreciable basis of an asset. Further, there may be improvements or repairs made to asset that either adds value to the asset or extend its economic life.
- **Transferring the Assets:** A fixed asset maybe sold or transferred to another subsidiary, reporting entity, or department within the company. These inter-company and intra-company transfers may result in changes that impact the asset's depreciable basis, depreciation, or other asset data. This needs to be reflected accurately in the fixed assets management system..
- **Depreciating the Assets:** The decline in an asset's economic and physical value is called depreciation. Depreciation is an expense which should be periodically accounted on a company's books, and allocated to the accounting periods, to match income and expenses. Sometimes, the revaluation of an asset, may also result in appreciation of its value
- **Disposing the Assets:** When a fixed asset is no longer in use, becomes obsolete, is beyond repair; the asset is typically disposed. When an asset is taken out of service, depreciation cannot be charged on it. There are multiple types of disposals, such as abandonments, sales, and trade-ins. Any difference between the book value, and realized value, is reported as a gain or loss

36) Explain a few Risks and Control Objectives in Fixed Assets Process at Masters Level?

Risks and Control Objectives for Fixed Asset Management Process at Master Levels are as follows:

Risk	Control Objective
Invalid changes are made to the fixed asset register and/or master file.	Only valid changes are made to the fixed asset register and/or master file.
Valid changes to the fixed asset register and/or master file are not input and processed.	All valid changes to the fixed asset register and/or master file are input and processed.
Changes to the fixed asset register and/or master file are not accurate.	Changes to the fixed asset register and/or master file are accurate.
Fixed asset register and/or master file data are not kept up to date.	Fixed asset register and/or master file data remain up to date.
System access to fixed asset master file / system configuration is not restricted to the authorized users.	System access to fixed asset master file / system configuration is restricted to the authorized users.

System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has not been correctly defined.	System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has been correctly defined.

37) Explain a few Risks and Control Objectives in Fixed Assets Process at Transactions Level?

Risks and Control Objectives for Fixed Asset Management Process at Transaction Levels are as follows:

Risk	Control Objective
Fixed asset acquisitions are not accurately recorded.	Fixed asset acquisitions are accurately recorded.
Fixed asset acquisitions are not recorded in the appropriate period.	Fixed asset acquisitions are recorded in the appropriate period.
Fixed asset acquisitions are not recorded.	All fixed asset acquisitions are recorded.
Depreciation charges are not accurately calculated and recorded.	Depreciation charges are accurately calculated and recorded.
Depreciation charges are not recorded in the appropriate period.	All depreciation charges are recorded in the appropriate period.
Fixed asset disposals/transfers are not recorded.	All fixed asset disposals/transfers are recorded.

38) What are the components of the General Ledger Cycle?

Components of General Ledger Cycle:

(a) General Ledger (GL) Process is the process of recording the transactions in the system to finally generating the reports from financial transactions entered in the System.

(b) Inputs to GL Process are the financial transactions. Outputs include various types of Financial Reports to Internal and External Users, viz. Financial Statements, Ratios, Funds Flow Statement, Common Size Statements, etc.

(c) GL Process Flow includes – (i) Data Input, (ii) Transaction Review, (iii) Transaction Approval, (iv) Transaction Posting, and (v) Report Generation.

39) Explain a few Risks and Control Objectives in General Ledger Process at Configuration Level?

Risks and Control Objectives for General Ledger at Configuration Levels are as follows:

Risk	Control Objective
Unauthorized general ledger entries could be passed.	Access to general ledger entries is appropriate and authorized.

System functionality does not exist to segregate the posting and approval functions.	System functionality exists to segregate the posting and approval functions.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliations to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliations to confirm accuracy of such accounts.
Systems do not generate reports of all	Systems generate reports of all recurring
recurring and non-recurring journal entries for review by management for accuracy.	and nonrecurring journal entries for review by management for accuracy.
Non-standard journal entries are not tracked and are inappropriate.	All non-standard journal entries are tracked and are appropriate.

40) Explain a few Risks and Control Objectives in General Ledger Process at Masters Level?

Risks and Control Objectives for General Ledger at Master Levels are as follows:

Risk	Control Objective
General ledger master file change reports are not generated by the system and are not reviewed as necessary by an individual who does not input the changes.	General ledger master file change reports are generated by the system and reviewed as necessary by an individual who does not input the changes.
A standard chart of accounts has not been approved by management and is not utilized within all entities of the corporation.	A standard chart of accounts has been approved by management and is not utilized within all entities of the corporation.

41) Explain a few Risks and Control Objectives in General Ledger Process at transactions Level?

Risks and Control Objectives for General Ledger at Transaction Levels are as follows:

Risk	Control Objective
General ledger balances are not reconciled to sub ledger balances and such reconciliation are not reviewed for accuracy and not approved by supervisory personnel.	General ledger balances reconcile to sub ledger balances and such reconciliation are reviewed for accuracy and approved by supervisory personnel.

Interrelated balance sheets and income statement accounts do not undergo automated reconciliation to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliation to confirm accuracy of such accounts.
Account codes and transaction amounts are not accurate and not complete, and exceptions are not reported.	Account codes and transaction amounts are accurate and complete, with exceptions reported.
A report of all journal entries completed as part of the closing process is not reviewed by management to confirm the completeness and appropriateness of all recorded entries.	A report of all journal entries completed as part of the closing process is reviewed by management to confirm the completeness and appropriateness of all recorded entries.
Entries booked in the close process are not complete and accurate.	Entries booked in the close process are complete and accurate.

42) What are the advantages of Cyber Laws?

Following are the few advantages of Cyber Laws:

1) The implications for the e-businesses would be that email would now be a valid and legal form of communication in India that can be duly produced and approved in a court of law.
2) Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
3) Digital signatures have been given legal validity and sanction in the Act.
4) The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
5) The Act now allows Government to issue notification on the web thus heralding e-governance.
6) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
7) The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
8) The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Ch:2 Finance and Accounting Systems

(1) Write short notes on "Finance and Accounting System"?

An Accounting Information System is a system of collecting, storing and processing financial and accounting data that are used by decision makers. An Accounting Information System is generally a computer–based method for tracking accounting activity in conjunction with information technology resources. Basic Objective& Process of an Accounting System is – (a) Record **Inputs** / Transactions, (b) **Process** Data, (c) Produce **Outputs / Reports** for Internal and External Users.

(2) How can Business Entities be classified for application of a Financial and Accounting System?

There are three different nature and types of businesses that are operated with the purpose of earning profit. Each type of business has distinctive features.

- **Trading Business –** Trading simply means buying and selling goods without any modifications, as it is. Hence inventory accounting is a major aspect in this case. Purchase and sales transactions cover major portion of accounting. This industry requires accounting as well as inventory modules.
- **Manufacturing Business –** This type of business includes all aspects of trading business plus additional aspect of manufacturing. Manufacturing is simply buying raw material, changing its form and selling it as a part of trading. Here also, inventory accounting plays a major role. This type of industry requires accounting and complete inventory along with manufacturing module.
- **Service Business –** This type of business does not have any inventory. It is selling of skills/knowledge/Efforts/time. Eg: Doctors, Architects, Chartered Accountants, are the professionals into service business. There may be other type of business into service, i.e. courier business, security service, etc. This industry does not require inventory module.

(3) What are the types of Accounting Vouchers? Explain from a Software Perspective?

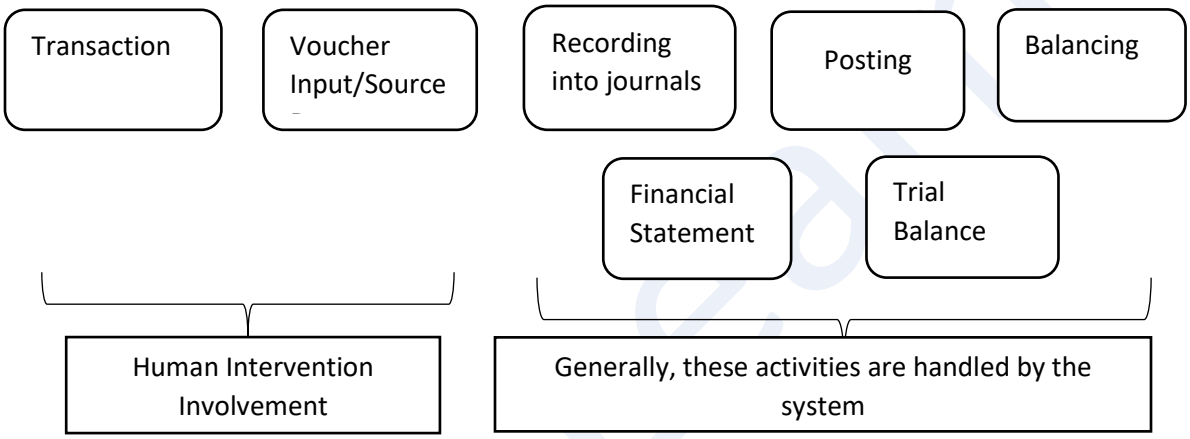
A **Voucher Number** or a **Document Number** is a unique identity of any voucher/document. A voucher may be identified or searched using its unique voucher number. Let us understand some peculiarities about voucher numbering.

- Voucher number must be unique.
- Every voucher type shall have a separate numbering series
- A voucher number may have prefix or suffix or both, e.g. ICPL/2034/17-18. In this case "ICPL" is the prefix, "17-18" is the suffix and "2034" is the actual number of the voucher.
- All vouchers must be numbered serially, i.e. 1,2,3,4,5,6 and so on.
- All vouchers are recorded in chronological order and hence voucher recorded earlier must have an earlier number, i.e. if voucher number for a payment voucher having date as 15thApril 2017 is 112, voucher number for all the vouchers recorded after this date shall be more than

112 only.

(4) Explain the "Accounting Process" Cycle from a Software Perspective?

Accounting or Book Keeping Cycle covers the business processes involved in recording and processing accounting events of an Entity. It begins when a Transaction or Financial Event occurs and ends with its inclusion in the Financial Statements. The flow of accounting from the angle of software, involves the following stages –

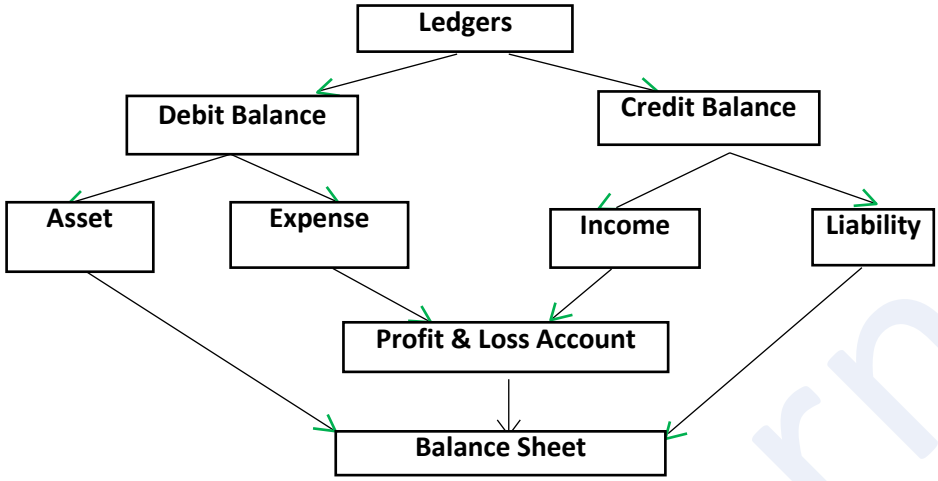


Note: Sometimes, certain transactions may be generated by the System itself, e.g. Depreciation, Interest, etc. In certain situations, there may be additional processes from Trial Balance to Financial Statements, viz.

- Trial Balance is first prepared **without** adjustments,
- **Adjustments** are made after due approval,
- **Adjusted Trial Balance** is prepared,
- **Closing Entries** are passed after finalization of Trial Balance. This is used for Financial Statements

(5) How are Accounting Ledgers from a Software Perspective?

In accounting, there are three types of ledger accounts, i.e. **Personal**, **Real** and **Nominal**. But as far as Financial and Accounting Systems are concerned, ledgers may be classified in two types only. Ledger having **Debit Balance** and ledger having **Credit Balance**.



(6) What are the types of Accounting Vouchers? Explain from a Software Perspective?

Voucher is a place where transactions are recorded. It is a data input form for inputting transaction data. In accounting, there may be different types of transactions; hence we use different voucher types for recording of different transactions. Generally following types of Accounting vouchers are used in accounting systems as shown

Module - Accounting		
Sl. No.	**Voucher Type**	**Use**
1	Contra	For recording of four types of transactions as under. a. Cash deposit in bank b. Cash withdrawal from bank c. Cash transfer from one location to another. d. Fund transfer from our one bank account to our own another bank account.
2	Payment	For recording of all types of payments. Whenever the money is going out of business by any mode (cash/bank).
3	Receipt	For recording of all types of receipts. Whenever money is being received into business from outside by any mode (cash/bank).
4	Journal	For recording of all non-cash/bank transactions. E.g. Depreciation, Provision, Write-off, Write-back, discount given/received, Purchase/Sale of fixed assets on credit, etc.
5	Sales	For recording all types of trading sales by any mode (cash/bank/credit).

6	Purchase	For recording all types of trading purchase by any mode (cash/bank/credit).
7	Credit Note	For making changes/corrections in already recorded sales/purchase transactions.
8	Debit Note	For making changes/corrections in already recorded sales/purchase transactions.
9	Memorandum	For recording of transaction which will be in the system but will not affect the trial balance.

(7) Differentiate between Master Data and Non–Master Data, in the context of Accounting System?

Point	**Master Data**	**Non–Master Data**
Meaning	It is relatively permanent **data**, which, once created, is not expected to change frequently.	It is **non–permanent** data, which is expected to change frequently. (also known as Transaction Data)
Types	Master Data may comprise – (a) Accounting Master, (b) Inventory Master, (c) Payroll Master, (d) Statutory Master, etc.	Details in each transaction, which differ from one another is called Transaction Data.
Significance	All Business Process Modules must use common Master Data.	Transaction Data, by its very nature, is not common, and is different for each transaction.
Data Input	Master Data is generally not typed by the User, it is selected from the available list of Masters (to ensure proper recording, and standardization).	Transaction Data is specifically keyed–in by the User in each transaction data entry. Sometimes, to permit standardization or to avoid wrong item selection, Transaction Data can also be selected from a list.
Changes to Data	Master Data Entry is done less frequently (e.g. annually, or when there is a need to update). Changes to Master Data should be properly authorised and	Transaction Data is entered by User. It is authorised/ approved by higher level Manager. Changes to data may be made by higher level

	checked by higher level Manager.	Manager, or by passing another rectification entry.

(8) What are the types of Master Data in the context of Accounting System?

Types of Master Data in the context of Accounting System

a. **Accounting Master Data –** This includes names of ledgers, groups, cost centers, accounting voucher types, etc.

E.g. Capital Ledger is created once and not expected to change frequently. Similarly, all other ledgers like, sales, purchase, expenses and income ledgers are created once and not expected to change again and again. Opening balance carried forward from previous year to next year is also a part of master data and not expected to change.

b. **Inventory Master Data –** This includes stock items, stock groups, godowns, inventory voucher types, etc. Stock item is something which bought and sold for business purpose, trading goods.

E.g. If a person is into the business of dealing in white goods, stock items shall be Television, Fridge, Air Conditioner, etc. For a person running a medicine shop, all types of medicines shall be stock items for him/her.

c. **Payroll Master Data –** Payroll is another area connecting with Accounting Systems. Payroll is a system for calculation of salary and recoding of transactions relating to employees. Master data in case of payroll can be names of employees, group of employees, salary structure, pay heads, etc. These data are not expected to change frequently.

E.g. Employee created in the system will remain as it is for a longer period of time, his/her salary structure may change but not frequently, pay heads associated with his/her salary structure will be relatively permanent.

d. **Statutory Master Data –** This is a master data relating to statute/law. It may be different for different type of taxes. We don't have any control on this data as statutory changes are made by Government and not by us. In case of change in tax rates, forms, categories, we need to update/change our master data.

E.g. Goods and Service Tax (GST), Nature of Payments for Tax Deducted at Source (TDS), etc. This data also shall be relatively permanent.

(9) Differentiate between Front–End and Back–End, in the context of Accounting System?

Differences between front and back end is as follows:

Point	Front End	Back End

Meaning	It is part of the overall Software which **actually interacts with the User** who is using the Software.	It is a part of the overall Software which does **not** directly interact with the User, but interacts with Front End only.
Purpose	It is meant for handling requests from Users.	It is meant for storing and handling the data.
Data	It handles processed data.	It handles Raw Data and processes it.
Language	Front–End speaks in the language understood by the User and also understands technical language.	Back–End speaks in technical language not directly understood by the User. Thus, it interacts only with
Presentation	It is meant for presenting information in proper format and structure, use of different colors, bold, italic letters, Tables, Charts etc.	It is meant for handling data, and not "presentation" of data to the User.
User Interface	Front–End Software guides a User to the desired report or feature. The User Interface of the Front–End is intuitive, i.e. minimum use of help should be sought by User.	Back–End Software is not intended to improve "User Experience". It is intended to handle the data processing requests effectively and communicate the same to the Front–End.

(10) Differentiate between Installed Applications and Web Applications, in the context of Accounting System?

Differences between Installed and web application is as follows

Particulars	Installed Applications	Web Applications
Meaning	These are Software Programs installed on the **Hard Disc of the User's Computer.**	These are installed on a **Web Server** and accessed using a **Browser** and **Internet Connection**.
Installation	This has to be installed on **every** Computer in an Entity. This may be a time–consuming exercise.	Software is not installed on every Computer, but in only one Computer, i.e. a Web Server. Installation on each User Computer is not required.
Maintenance	Maintenance and Updating of Software is required on each Computer, and takes time and efforts.	Maintenance and Updating of Software is only on the Web Browser, and is less time consuming.
Software Access	User can access the Software only from the Computer where it is	User can access the Software 24 x 7 without Hardware Restrictions, i.e.

	installed. It cannot be used from any Computer.	anywhere, anytime, using a Browser and Internet.
Data Storage	Data is physically stored in the Hard Disc of the User's Server Computer. So, User has full control over the data.	Data is stored on a Web Server, and not in the User's Server Computer. So, User will not have any control over the data.
Data Security	User can establish proper Physical Access Controls also, and ensure that only Authorised Users have access to the system and data.	Since Software and Data is maintained on a Web Server, there is a need for more Logical Access Controls to prevent unauthorized access.
Flexibility	Installed Applications have more flexibility and controls than Web Applications, as it is very easy to write Desktop Applications that take advantage of the User's Hardware.	Web Applications are generally applicable to all Users, and cannot have the flexibility of Desktop Applications.

(11) Write short notes on ERP. Explain?

An Enterprise Resource Planning (ERP) System is a **fully integrated business management system** covering functional areas of an Enterprise like Logistics, Production, Finance, Accounting and Human Resources. ERP organizes and **integrates operation processes and information flows** to make optimum use of resources such as men, material, money and machinery. ERP **aims at one database, one application and one user interface** for the entire Enterprise. It takes information from every function and that assists employees and Managers to plan, monitor and control the entire business. For a software system to be considered ERP, it must provide an organization with functionality for two or more systems. Some well–known ERPs today include SAP, Oracle, MFG Pro, MS Axapta, Baan, E–Applications, System 21, Prism, etc.

(12) Differentiate between Non–Integrated and Integrated System, in the context of Accounting System?

Point	Non–Integrated System	Integrated System (ERP System)
Meaning	A Non–Integrated System is a system of maintaining data in a	An Integrated System is a system of maintaining data in a Entity–wide centralized
Database	Each Department shall maintain its own data separately, and have a separate Database.	There is a Central Database, to which access is permitted appropriately to different departments.
Communi-cation	Each Department communicates relevant data generated by it to the other Departments, which have to process that data	Each Department / User is allowed access to the Central Database, based on pre–defined rights and privileges.
Tracking	There are multiple modes of communication like phone call, SMS, Email, WhatsApp or personal meeting, etc. There is no documentation	Every communication (any mode) between Departments is tracked and documented, leading to better control.
Advantages	• Reduced Risk of Data Loss, • Higher data security (on need to know basis)	• Single Point Data Entry & Capture, • Better Data Communication between
Disadvan-tages	• Communication Gaps, • Mismatch of Data across Departments, • Duplication of Processes on same data.	• Risk of Data Loss (being centralized), • Risk of Unauthorised Access to Data.

(13) List the features of ERP

An ERP System is an integration of various organization processes. Its features include –

- **Manufacturing:** Some of the functions include engineering, capacity, workflow management, quality control, bills of material, manufacturing process, etc.
- **Financials:** Accounts payable, accounts receivable, fixed assets, general ledger and cash management, etc.
- **Human Resources:** Benefits, training, payroll, time and attendance, etc.
- **Supply Chain Management:** Inventory, supply chain planning, supplier

scheduling, claim processing, order entry, purchasing, etc.

- **Projects:** Costing, billing, activity management, time and expense, etc.
- **Customer Relationship Management (CRM):** CRM is a term applied to processes implemented by a company to handle its contact with its customers. CRM software is used to support these processes, storing information on current and prospective customers. Information in the system can be accessed and entered by employees in different departments, such as sales, marketing, customer service, training, professional development, performance management, human resource development, and compensation.
- **Data Warehouse:** Usually this is a module that can be accessed by an organization's customers, suppliers and employees. Data warehouse is a repository of an organization's electronically stored data. Data warehouses are designed to facilitate reporting and analysis. An expanded definition for data warehousing includes business intelligence tools, tools to extract, transform, and load data into the repository, and tools to manage and retrieve metadata

(14) What are the advantages of ERP?

Benefits of an ERP System

- **Information integration:** The reason ERP systems are called integrated is because they possess the ability to automatically update data between related business functions and components.

  For example - one needs to only update the status of an order at one place in the order-processing system; and all the other components will automatically get updated.

- **Reduction of lead-time:** The elapsed time between placing an order and receiving it is known as the Lead-time. The ERP Systems by virtue of their integrated nature with many modules like Finance, Manufacturing, Material Management Module etc.; the use of the latest technologies like EFT (Electronic Fund Transfer), EDI (Electronic Data Interchange) reduce the lead times.
- **On-time Shipment:** Since the different functions involved in the timely delivery of the finished goods to the customers- purchasing, material management production, production planning, plant maintenance, sales and distribution – are integrated and the procedures automated; the chances of errors are minimal and the production efficiency is high. Thus, the ERP system ensures on-time delivery of goods to the customers.
- **Reduction in Cycle Time**: Cycle time is the time between placement of the order and delivery of the product. In an ERP System; all the data, updated to the minute, is available in the centralized database and all the procedures are automated, almost all these activities are done without human intervention. This efficiency of the ERP systems helps in reducing the cycle time
- **Increased Flexibility:** ERP Systems help the companies to remain flexible by making the company information available across the departmental barriers and automating most of the processes and procedures, thus enabling the company to react quickly to the changing market conditions.
- **Better Customer Satisfaction:** Customer satisfaction means meeting or

exceeding customers 'requirements for a product or service. With the help of web-enabled ERP systems, customers can place the order, track the status of the order and make the payment sitting at home. Since all the details of the product and the customer are available to the person at the technical support department also, the company will be able to better support the customer.

(15) ERP is not free from limitations?

Limitations of ERP

- An ERP System may provide current status only, and may not provide past data / trends, etc. Managers also require past data for effective decision–making.
- Methods used in ERP applications are not integrated with other organizational or divisional systems.
- ERP Systems may not include external intelligence, and may provide only internal operational data.
- ERP Systems may be too time–consuming and costly for certain organizations.

(16) What are the major Modules that are integrated in an ERP System?

Modules in an ERP

An ERP System maintains in a Single Database, the data needed for a variety of business functions (or Software Modules) such as Manufacturing, Supply Chain Management, Financials, Projects, Human Resources and Customer Relationship Management. So, the Software Modules in an ERP can include –

- Supply Chain Management (SCM) – Inventory, Supply Chain Planning, Supplier Scheduling, Claim Processing, Order
- Entry, Purchasing, etc.
- Manufacturing– Production Planning, Engineering, Capacity, Workflow Management, Quality Control, Bills of Material, Manufacturing Process, etc.
- Customer Relationship Management (CRM) – Enquiry Handling, Targeted Marketing, Quotation, Order
- Management, Delivery Management, Customer Service, Receivables Follow up, etc.
- Projects – Costing, Billing, Activity Management, Time and Expense, etc.
- Human Resources – Employee Benefits, Training, Payroll, Time and Attendance, etc.
- Financials – Accounts Payable, Accounts Receivable, Fixed Assets, General Ledger, Cash Management, etc.

(17) Write short notes on Risks and Controls in an ERP System?

Aspect	Risk	Control Required
Data Access	Data is stored centrally and all Departments access that Central Data. This creates a possibility of access to non–relevant data.	Access Rights should be defined very carefully. Access should be given on "**Need to know**" and "**Need to do**" basis only.

Data Safety	There is only one set of data. If this data is lost, the entire business may come to a standstill.	There should be strong physical control, along with effective Data Backup Arrangements.
Operation Speed	As the size of the Central Databases increases, it reduces the speed of operation.	Hardware should be upgraded regularly to increase speed. Redundant Data should be removed using techniques like Data Warehousing.
Change in Process	Since the overall system is integrated, a small change in process for one Department may require lot of time, efforts and cost.	All processes must be documented properly while designing the ERP, so as to avoid any changes that are costly to implement later.
Staff Turnover	In case of Staff Turnover, it is increasingly difficult to maintain the system, due to its complexity and integration.	There should be proper Staff Training System, Helpdesk / Operation Manuals, Backup Plans for Staff Turnover, etc.
System Failure	Due to Single Server and Central Database, in case of failure of system, the whole business may get affected badly.	There should be proper DRP and BCP Plans, including Secondary Server, Offsite Backup, alternate Hardware / Internet arrangements, etc.

(18) Write a short note on risk and corresponding control related to People issues.

Aspect	Risk associated	Control required
Change management	Change will occur in the employee's job profile in terms of some jobs becoming irrelevant and some new jobs created.	Proper training of the users with well documented manuals. Practical hands on training of the ERP System should be provided so that the transition from old system to ERP system is smooth and hassle free.
Training	Since the greater part of the raining takes place towards the end of the ERP implementation cycle, management may curtail the training due to increase in the overall cost budget.	Training is a project-managed activity and shall be imparted to the users in an organization by the skilled consultants and representatives of the

		hardware and package vendors
Staff turnover	As the overall system is integrated and connected with each other department, it becomes complicated and difficult to understand. Employee turnover – qualified and skilled personnel leaving the company - during the implementation and transition phases can affect the schedules and result in delayed implementation and cost overrun.	This can be controlled and minimized by allocation of employees to tasks matching their skill-set; fixing of compensation package and other benefits accordingly-thus keeping the employees happy and content and minimizing the staff turnover
Top management support	ERP implementation will fail if the top management does not provide the support and grant permission for the availability of the huge resources that are required during the transition	The ERP implementation shall be started only after the top management is fully convinced and assure of providing the full support.
Consultants	These are experts in the implementation of the ERP package and might not be familiar with the internal workings and organizational culture.	The consultants should be assigned a liaison officer - a senior manager – who can familiarize them with the company and its working.

(19) Write a short note on risk and corresponding control related to Process risk.

Aspect	Risk associated	Control required
Program Management	There could be a possibility of an information gap between day-to-day program management activities and ERP-enabled functions like materials and procurement planning, logistics and manufacturing.	This requires bridging the information gap between traditional ERP-based functions and high value operational management functions, such applications can provide reliable real-time information linkages to enable high-quality decision making.
Business Process Reengineering (BPR)	BPR means not just change – but dramatic change and dramatic improvements.	This requires overhauling of organizational structures, management systems, job descriptions, performance measurements, skill development., training and use of IT.

(20) Write a short note on risk and corresponding control related to Technology risk.

Aspect	Risk associated	Control required
Software Functionality	ERP systems offer a myriad of features and functions, however, not all organizations require those many features. Implementing all the functionality and features just for the sake of it can be disastrous for an organization.	Care should be taken to incorporate the features that are required by the organization and supporting additional features and functionality that might be required at a future date.
Technological Obsolescence	With the advent of more efficient technologies every day, the ERP system also becomes obsolete as time goes on.	This requires critical choice of technology, architecture of the product, ease of enhancements, ease of upgrading, quality of vendor support.
Enhancement and Upgrades	ERP Systems are not upgraded and kept up-to- date. Patches and upgrades are not installed and the tools are underutilized.	Care must be taken while selecting the vendor and upgrade/support contracts should be signed to minimize the risks.
Application Portfolio Management	These processes focus on the selection of new business applications and the projects required delivering them.	By bringing to the light the sheer number of applications in the current portfolio, IT organizations can begin to reduce duplication and complexity.

(21) Write a short note on risk and corresponding control related to Technology risk.

Aspect	Risk associated	Control required
Lengthy implementation time	ERP projects are lengthy that takes anywhere between 1 to 4 years depending upon the size of the organization. Due to technological developments happening every day, the business and technological environment during the start and completion of the project will never be the same. Employee turnover is another problem.	Care must be taken to keep the momentum high and enthusiasm live amongst the employees, so as to minimize the risk.

Insufficient Funding	The budget for ERP implementation is generally allocated without consulting experts and then implementation is stopped along the way, due to lack of funds.	It is necessary to allocate necessary funds for the ERP implementation project and then allocate some more for contingencies.
Data Safety	As there is only one set of data, if this data is lost, whole business may come to stand still.	Back up arrangement needs to be very strong. Also, strict physical control is needed for data.
Speed of Operation	As data is maintained centrally, gradually the data size becomes more and more and it may reduce the speed of operation.	This can be controlled by removing redundant data, using techniques like data warehousing and updating hardware on a continuous basis.
System Failure	As everybody is connected to a single system and central database, in case of failure of system, the whole business may come to stand still may get affected badly.	This can be controlled and minimized by having proper and updated back up of data as well as alternate hardware / internet arrangements. In case of failure of primary system, secondary system may be used.
Data Access	Data is stored centrally and all the departments access the central data. This creates a possibility of access to non-relevant data.	Access rights need to be defined very carefully and to be given on "Need to know" and Need to do" basis only.

(22) Outline the Audit Approach in relation to an ERP System?

Auditing aspects in case of any ERP system can be summarized as under:

(i) **Auditing of Data**

- **Physical Safety** – Ensuring physical control over data.
- **Access Control** – Ensuring access to the system is given on "need to know" (a junior accountant need not view Profit & Loss Account of the business) and "need to do basis" (HR executive need not record a Purchase Order).

(ii) **Auditing of Processes**

- **Functional Audit –** This includes testing of different functions / features in the system and testing of the overall process or part of process in the system and its comparison with actual process. It is quite possible that all the aspect present in the actual process may not be integrated in the ERP system. There may be some manual intervention.

- **Input Validations –** This stand for checking of rules for input of data into the system. E.g. a transaction of cash sales on sales counter must not be recorded in a date other than today (not a future date or a back date), amount field must not be zero, stock item field shall not be empty, etc. Input validations shall change according to each data input form.

(23) Write short notes on the Finance and Accounting (FA) Module of an ERP System?

Financial Accounting Module

This module is the most important module of the overall ERP System and it connects all the modules to each other. Every module is somehow connected with module. Following are the key features of this module:

- ♦ Tracking of flow of financial data across the organization in a controlled manner and integrating all the information for effective strategic decision making.
- ♦ Creation of Organizational Structure (Defining Company, Company Codes, business Areas, Functional Areas, Credit Control, Assignment of Company Codes to Credit Controls).
- ♦ Financial Accounting Global Settings (Maintenance of Fiscal Year, Posting Periods, defining Document types, posting keys, Number ranges for documents).
- ♦ General Ledger Accounting (Creation of Chart of Accounts, Account groups, defining data transfer rules, creation of General Ledger Account).
- ♦ Tax Configuration & Creation and Maintenance of House of Banks.
- ♦ Account Payables (Creation of Vendor Master data and vendor-related finance attributes like account groups and payment terms).
- ♦ Account Receivables (Creation of Customer Master data and customer- related finance attributes like account groups and payment terms.
- ♦ Asset Accounting.
- ♦ Integration with Sales and Distribution and Materials Management.

(24) **Write short notes on the Controlling (CO) Module of an ERP System?**

Controlling Module

This module helps in analysing the actual figures with the planned data and

in planning business strategies. Two kinds of elements are managed in Controlling Module –Cost Elements and Revenue Elements. These elements are stored in the Financial Accounting module.

Key features of this module are as under:

i. Cost Element Accounting: It provides overview of the costs and revenues that occur in an organization. They are the basis for cost accounting and enable the user the ability to display costs for each of the accounts that have been assigned to the cost element. Examples of accounts that can be assigned are Cost Centers, Internal Orders, WBS (work breakdown structures).

ii. Cost Centre Accounting: Cost Centers can be created for such functional areas as Marketing, Purchasing, Human Resources, Finance, Facilities, Information Systems, Administrative Support, Legal, Shipping/Receiving, or even Quality. Using Cost Centre Accounting are that the managers can set budget/cost Centre targets; Cost allocation methods; Assessments/Distribution of costs to other cost objects etc.

iii. Activity-Based-Accounting: This analysis cross-departmental business processes and allows for a process-oriented and cross- functional view of the cost centers.

iv. Internal Orders: Internal Orders provide a means of tracking costs of a specific job, service, or task. These are used as a method to collect those costs and business transactions related to the task. This level of monitoring can be very detailed but allows

(25) Write short notes on the Sales and Distribution (SD) Module of an ERP System?

Sales and Distribution Module: Sales and Distribution is used by organizations to support sales and distribution activities of products and services, starting from enquiry to order and then ending with delivery.

Key features of Sales and Distribution Module are discussed as under:

- **Setting up Organization Structure:** Creation of new company, company codes, sales organization, distribution channels, divisions, business area, plants, sales area, maintaining sales offices, storage location;
- **Assigning Organizational Units:** Assignment of individual components created in the above activities with each other per design like company code to company, sales organization to company code, distribution channel to sales organization, etc.;
- **Defining Pricing Components:** Defining condition tables, condition types, condition sequences;
- Setting up sales document types, billing types, and tax-related components; and
- Setting up Customer master data records and configuration.

(26) Write short notes on the Human Resources (HR) Module of an ERP System?

Human Resource Module

This module enhances the work process and data management within HR department of enterprises. Right from hiring a person to evaluating one's performance, managing promotions, compensations, handling payroll and other related activities of an HR is processed using this module.

- The module starts with the employee and workmen master.
- Employees being a part of a department so there will be provision of department and designation master. The job of this module is to **record the regular attendance** of every employee.
- Usage of **magnetic card or finger print recognition** devices will help to improve the attendance system and provide an overall security in terms of discarding proxy attendance.
- Moreover, if the attendance related information can be digitized then the major portion of **monthly salary can be automated**. But the authority should study the feasibility of this kind of system.
- This module will also deal with the financial entries like advance or loan to employees.
- From **Holiday master** provided with the module, the user could feed all possible holidays at the beginning of a year, so leave related information can be automated. This module will generate monthly wage sheet from which the salary payment can be made and respective accounts will be updated.
- All figures will be protected under password. Only authorized person will be eligible to **access information** from this module.

(27) Write short notes on the Production Planning (PP) Module of an ERP System.

Production Planning Module:

Process: Production Planning (PP) Module involves the following processes –

- Issue of Raw Material from Stores Department to Production Departments,
- Conversion of Raw Materials into WIP,
- Conversion of WIP into Finished Goods, (including handling out–sourced processes, components, etc.) Primary Packing of Finished Goods,
- Transfer of Packed Finished Goods into Warehouse.

Key Features: PP Module –

- includes software designed specifically for Production Planning and Management,
- consists of Master Data, System Configuration and Transactions, to accomplish Planned Procedure for Production,
- collaborates with other Business Processes like Sales and Operations Planning, Distribution Resource Planning,

- Material Requirements Planning, Product Cost Planning, etc.

(28) Write short notes on the Materials Management (MM) Module of an ERP System?

Material Management (MM) Module involves the following processes /activities –

- **Purchase Requisition:** Production Department (or Stores Department) sends a request to Purchase Department for purchase of the Raw Materials required for production.
- **Scrutiny:** Purchase Department evaluates the Requisition with current stock position and Purchase Order pending position, and decides about accepting or rejecting the requisition.
- **Quotation:** If the Requisition is accepted, Purchase Department seeks Quotations from prospective Vendors for supply of Raw Materials.
- **Analysis of Quotations:** Quotations received from Vendors are compared and evaluated, on various aspects.
- **Purchase Order:** Terms of Purchase are informed to the selected Vendors through the Purchase Order (PO), which provides details of –(i) Description of items to be purchased, (ii) Quantity, (iii) Price, (iv) Time of Delivery, (v) Place of Delivery, (vi) Payment Terms, (vii) Special Instructions, if any, etc.
- **Material Receipt:** Materials are received as per PO, after proper inspection thereof. A Material Receipt Note (MRN)or Goods Receipt Note (GRN) is prepared to increase the Stock Balance, after receipt of materials.
- **Issue of Materials:** Material received by Stores Department is issued to Production Departments as per requirement. A Bill of Materials (BOM) or Stores Requisition Note (SRN) is prepared for this purpose.
- **Purchase Invoice:** Invoice received from Vendor is recorded in the Books, resulting in a Liability (Payable) to the Vendor towards goods purchased.
- **Payment to Vendor:** Payment is made to Vendor based on Purchase Invoice, after verifying with GRN and PO.

(29) Write short notes on the Quality Management (QM) Module of an ERP System?

Quality Management Module

This module helps an organization to accelerate their business by adopting a structured and functional way of managing quality in different processes.

QM Process includes the following activities –

- Setting **Master Data and Standards** for quality management,
- Setting Quality **Targets**,
- Preparing a Quality Management **Plan**,
- Establishing **measurement norms** for Quality Targets,
- Creating a **Reporting System** for measuring actual quality achieved, compliance levels, etc.
- Identifying **Quality Issues** and improvements and changes to be made (including Training, Re–design, etc.),

- Initiating **Change Requests**, in case of any change is needed in the product / design / process, and
- Ensuring **ongoing compliance** with the overall level of quality achieved.

Key features of QM Module –

- helps to manage quality in production across processes in an Entity.
- seeks to adopt a structured and functional way of managing quality in different processes,
- collaborates in procurement and sales, production, planning, inspection, notification, control, audit, etc.

(30) Write short notes on the Plant Maintenance (PM) Module of an ERP System?

Plant Maintenance (PM) is a functional module which handles the maintaining of equipment and enables efficient planning of production and generation schedules.

Process: PM Process includes the following –

(a) Creating Masters in respect of –(i) Various items of Machinery and their Spare Parts, (ii) Maintenance Data, (iii) Schedule of Preventive Maintenance,

(b) Monitoring whether the Maintenance activities are actually performed as per Planned Schedules,

(c) Organizing Special / Break–down Maintenance to handle outages, etc.

Key Features: PM Module –

(a) handles the maintaining of equipment and enables efficient planning of production and generation schedules,

(b) ensures cost–efficient maintenance methods, viz. Risk–Based Maintenance or Preventive Maintenance,

(c) provides comprehensive Outage Planning, and powerful work order management,

(d) creates various Reports including – (i) PM Reminders, (ii) Monthly PMs, (iii) Maintenance Histories, (iv) PM Schedules, (v) Plant/ Equipment Masters, etc.

(31) Write short notes on the Project Systems (PS) Module of an ERP System?

PS Module is an Integrated Project Management Tool used for planning and managing projects. Project Management Tools include – (a)Cost and Planning Budget, (b) Project Scheduling, (c) Requisitioning of Materials and Services, etc. Project Systems Activities include – (a) Handling Project Requests, (b) Project Planning and Sanction, (c) Project. Budgeting, (d) Project Monitoring, (e) Project Implementation, and (f) Project Completion / Sign–off.

In Project System, each process has a defined set of tasks to be performed known as process flow in Project Lifecycle. When a project request is received, a project is created and it undergoes the following steps in project process flow/ lifecycle.

(32) Write short notes on Supply Chain Management (SCM) in relation to an ERP System?

A Supply Chain is a network of autonomous or semi-autonomous business entities collectively responsible for procurement, manufacturing, and distribution activities associated with one or more families of related products. In other words, a supply chain is a network of facilities that procure raw materials, transform them into intermediate goods and then finished products, and then finally deliver the products to customers through a distribution system or a chain. In Supply Chain Management System, any product which is manufactured in a company, first reaches directly from manufacturer to distributors where manufacturer sells the product to the distributor with some profit of margin. Distributors supply that product to retailer with his/her profit and then finally customers receive that product from retailer.

(33) Write short notes on Customer Relationship Management (CRM) in relation to an ERP System?

Customer Relationship Management (CRM): CRM is a system which aims at improving the relationship with existing customers, finding new prospective customers, and winning back former customers. This system can be brought into effect with software which helps in collecting, organizing, and managing the customer information. Key benefits of a CRM module are as under.

- **Improved customer relations:** One of the prime benefits of using a CRM is obtaining better customer satisfaction. Better services can be provided to customers through improved understanding of their issues and this in turn helps in increasing customer loyalty and decreasing customer agitation. In this way, continuous feedback from the customers regarding the products and services can be received.
- **Increase customer revenues:** By using a CRM strategy for any business, the revenue of the company can be increased. Using the data collected, marketing campaigns can be popularized in a more effective way. With the help of CRM software, it can be ensured that the product promotions reach a different and brand-new set of customers, and not the ones who had already purchased the product, and thus effectively increase the customer revenue.
- **Maximize up-selling and cross-selling:** A CRM system allows up-selling which is the practice of giving customers premium products that fall in the same category of their purchase. The strategy also facilitates cross selling which is the practice of offering complementary products to customers. This is done by interacting with the customers and getting an idea about their wants, needs, and patterns of purchase. The details thus obtained will be stored in a central database, which is accessible to all company executives.
- **Better internal communication:** Following a CRM strategy helps in building up better communication within the company. The sharing of customer data between different departments will enable them to work as a team. This is better than functioning as an isolated entity, as it will help in increasing the

company's profitability and enabling better service to customers.

- **Optimize marketing:** CRM enables to understand the customer needs and behavior in a better way, thereby allowing any enterprise to identify the correct time to market its product to the customers. CRM will also give an idea about the most profitable customer groups, and by using this information, similar prospective groups, at the right time will be targeted

(34) Explain the concept of "Integration" amongst various Modules in an ERP System?

Module	Description
Finance & A/cg (FA) And Controlling (CO)	➢ Integration takes place in areas like Material Valuation, Vendor Payments, Material Costing, etc. ➢ If any Inventory Posting is done, GL Accounts (Suppliers) are updated online by the System. ➢ Transport (Logistics) Invoice Verification will create Vendor Liability in Vendor A/c immediately on posting the document.
Production Planning (PP)	➢ Integration takes place in areas like Material Requirement Planning, Receipts/Issues against Production Orders, Availability Check for Stocks, etc. ➢ Material Requirement Planning isgenerates planned Orders or Purchase Requisitions which can be converted to Purchase Orders/Contracts, based on Stocks, expected Receipts, expected Issues.
Sales &Distribution (SD)	➢ Integration takes place in areas like Delivery, Availability Check, Stock Transfer Requirements, etc. ➢ When a Sales Order is created, it can initiate a dynamic Availability Check of Stocks on hand.
Quality Management (QM)	➢ Integration with QM takes place for Quality Inspection at Goods Receipt, WIP Inspection, etc. ➢ In the case of a goods movement, the system determines whether the material is subject to an Inspection Operation. If so, a corresponding activity is initiated for the movement in the Quality Management System.
Plant Maintenance (PM)	➢ Material/Service Requirement as mentioned in the Maintenance Order, leads to generation of Purchase Requisition (PR) for Maintenance. ➢ This PR will be converted to Purchase Order (PO) by MM Module.

(35) Write short notes on "Reports" in the context of Finance and Accounting Systems?

Reports: A Report is a presentation of information in proper and meaningful way. So, Reporting System is a system of regular reporting on the pre–decided aspects.

Examples of Reports in Finance and Accounting Systems:

(a) **Financial Statements**, i.e. Balance Sheet, Profit and Loss Statement and Cash Flow Statement,

(b) Information in respect of Management **Discussion & Analysis (**MD&A) section the Annual Report, which discusses how Management have prepared the financial statement, their interpretation of the Company's performance, the industry in which they operate, to provide critical guidance on where the Company is heading.

(c) Information in respect of **Corporate Social Responsibility Report**, where applicable,

(d) Periodic **Internal Management Reports** – (i) Variance Reports, (ii) Budget vs Actual, (iii) Year to Date reports, etc. used for internal evaluation and control function.

(36) What are the features of MIS Reports? How should information be presented in MIS Reports?

Meaning: A MIS Report is a tool that Managers use to evaluate Business Processes and Operations. MIS Reports generated by the Entity's IT Systems, are used by Business Managers at all levels of an Entity, to help them evaluate their business' daily activities or problems that arise, make decisions, and track progress

Features of MIS Reports: MIS Reports can be –

- auto–generated by the IT System on periodic basis (e.g. Daily Stock Report), or generated on–demand basis,
- generated by the specific Manager at his end, or can be generated by a specialized MIS Department, if any,
- customized to provide relevant information in user–friendly fashion, including Spreadsheets, etc.
- made specific to each Functional Unit / Division, e.g. Production, Despatch, Sales, Accounts, HR, etc.

Information in MIS Reports: To be useful, Information in a MIS Report should have the following features –

- **Timeliness:** The information should be available at the right time for the Decision Maker / Manager,
- **Adequacy:** The information should be adequate to meet the requirements of the Decision Maker / Manager,
- **Purposive:** The basic purpose of a MIS Report is to inform, evaluate, persuade and organize. MIS Information must be purposeful, when it is given to a Manager in the Entity.
- **Frequency:** The frequency with which the MIS Report is transmitted or received affects its value. Frequency is related to both the – (a) level of management, and (b) operational need.
- **Relevant:** MIS Reports need to be specific to the business area they address. A Report that includes unnecessary information might be ignored.
- **Structured:** Information in an MIS Report should be understandable to the Manager using it.

- **Accurate:** MIS Reports should be correct and accurate, to the extent required for supporting effective decisions.

(37) Explain the concept of Data Analytics, and the steps involved therein?

Data Analytics: It is the process of examining data sets to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software. Data Analytics predominantly refers to an assortment of applications, from basic Business Intelligence (BI), Reporting and Online Analytical Processing (OLAP) to various forms of advanced analytics.

Steps in Data Analytics:

(a) Data Collection

Identification of the information required for an analytics application. **Assembling** the required information. **Combining** the data using Data Integration Routines, and transforming into a common format. **Loading** the Data into an Analytics System.

(b) Data Organizing

Finding and **fixing data quality problems.** Running **Data Profiling** and **Data Cleansing** jobs to ensure consistency of information. **Manipulating and organizing** the data for the planned analytics use. Applying **Data Governance Policies** to ensure that the data is being used properly.

(c) Modelling and Training

Building of an analytical model, by a Data Scientist, using predictive modeling tools or other analytics software and programming languages (e.g. Python, Scala, R and SQL). Running the model against a partial data set to test its accuracy. Revising and running the model again and again, until it functions as intended.

(d) Data Analytics

The Model is run in Production Mode against the full data set, to address a specific information need or on an ongoing basis as the data is updated.

(e) Reporting

Communicating the results generated by Analytical Models to Executives and End–Users to aid in their decision–making it can be made easier to understand and quick to grasp by creating Charts and Infographics using Data Visualization Techniques.

(38) What do you understand by Business Intelligence? Explain its features?

Business Intelligence (BI) is a technology-driven process for analyzing data and presenting actionable information to help corporate executives, business managers and other end users make more informed business decisions.

BI encompasses a wide variety of tools, applications and methodologies that enable organizations to collect data from internal systems and external sources, prepare it for analysis, develop and run queries against the data, and create reports, dashboards and data visualizations to make the analytical results available to corporate decision makers as well as operational workers.

Features of business intelligence are:

- BI uses both historical information as well as new data from various source systems.
- BI can support both strategic and tactical decision–making processes.

- BI can be used by Data Analysts and similar IT Professionals, as also by Executives and Workers, who can run BI using self–service BI and data discovery tools.
- Separate BI Applications can be bought from different Vendors, or a unified BI Platform from one Vendor.
- BI Programs can incorporate advanced analytics tools, like Data Mining, Predictive Analytics, Text Mining, Statistical Analysis and Big Data Analytics.

(39) Write short notes on Business Reporting?

Business Reporting or **Enterprise Reporting** is the public reporting of operating and financial data by a business enterprise or the regular provision of information to decision-makers within an organization to support them in their work.

Organizations conduct a wide range of reporting, including financial and regulatory reporting; Environmental, Social, and Governance (ESG) reporting (or sustainability reporting); and, increasingly, integrated reporting.

Organizations communicate with their stakeholders about:

- ♦ mission, vision, objectives, and strategy;
- ♦ governance arrangements and risk management;
- ♦ trade-offs between the shorter- and longer-term strategies; and
- ♦ financial, social, and environmental performance (how they have fared against their objectives in practice).

Significance of Business Reporting:
Effective and transparent Business Reporting –

- allows Entities to present a cohesive explanation of their business,
- helps Entities communicate with internal and external Stakeholders, including Customers, Employees, Shareholders, Creditors, and Regulators,
- provides the backbone of strong and sustainable Entities, Financial Markets, and Economies,
- provides data for Stakeholders to assess an Entity's performance and make informed decisions of the Entity's
- capacity to create and preserve value (**Note:** Value = Monetary, Social, Environmental and Economic Value),
- reduces the risk for lenders and may lower the cost of capital,
- promotes better internal decision–making.

(40) Explain the concept of XBRL Reporting?

eXtensible Business Reporting Language (XBRL) is an open international standard for digital business reporting that provides a language in which reporting terms can be authoritatively defined. XBRL lets reporting information move between organizations rapidly, accurately and digitally. XBRL is a standard-based

way to communicate and exchange business information between business systems. Important features of XBRL are as follows:

a. **Clear Definitions:** XBRL allows the creation of reusable, authoritative definitions, called taxonomies, that capture the meaning contained in all the reporting terms used in a business report, as well as the relationships between all the terms.

b. **Testable Business Rules:** XBRL allows the creation of business rules that constrain what can be reported. **for example**, these business rules can be used to stop poor quality information being sent to a regulator or third party, by being run by the preparer while the report is in draft; stop poor quality information being accepted by a regulator or third party, by being run at the point that the information is being received.

c. **Multi-lingual Support:** XBRL allows concept definitions to be prepared in as many languages as necessary. This means that it's possible to display a range of reports in a different language to the one that they were prepared in, without any additional work.

d. **Strong Software Support:** XBRL is supported by a very wide range of software from vendors large and small, allowing a very wide range of stakeholders to work with the standard.

(41) Can the same software be used for Accounting and Tax Compliance also? Explain?

Regulatory compliance and accounting systems are closely connected with each other. Most of the regulatory compliance requires accounting data and accounting data comes from accounting systems. E.g. Income tax returns are prepared based on accounting data only. There may be two approaches for making compliances requiring accounting data.

a. Using same software for accounting and tax compliance; and

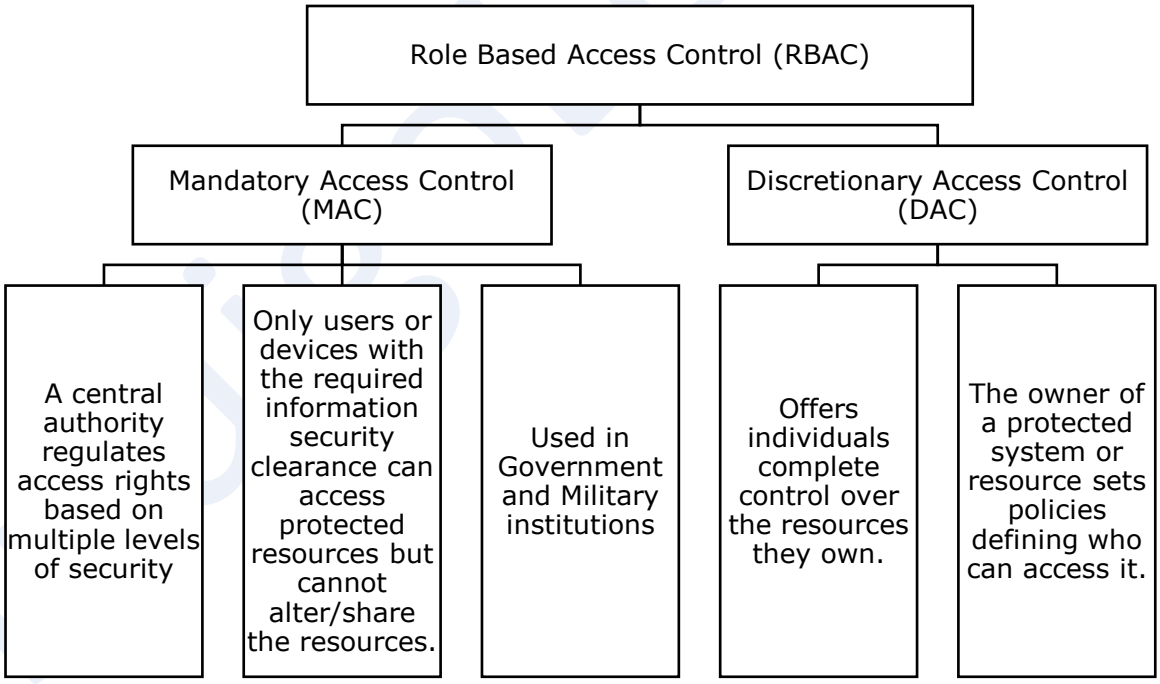
b. Using different software for accounting and tax compliance.

Software is needed for tax compliances as almost all the tax compliance today is through electronic mode only. If separate software is used for accounting and tax compliance, we need to put data in tax compliance software either manually or electronically.

Sl. No	Particulars	Accounting & Tax Compliance Software	Only Tax Compliance Software
1	Ease of software operation	Less – as this is integrated system of accounting and tax compliance, everything connected with other and making changes at one place may affect other aspects also.	More – as this is used only for one single purpose, i.e. tax compliance, it is less complicated and bound to be easy.

2	Features and facilities	Less – as this system is not an exclusive system for tax compliance, it may have limited features for tax compliance.	More – as this is an exclusive and specifically designed system for tax compliance, naturally more features and facilities shall exist in this system.
3	Time and efforts required	Less – as this is an integrated system, time required to transfer data to compliance software is zero.	More – as this is a separate software, data from accounting software need to put in this for preparation of returns. This may take extra time and efforts.
4	Accuracy	More – As this is an integrated system and hence accounting data and tax compliance data shall always be same. No need to transfer data to compliance software and reconcile the data.	Less – as there are two separate systems, reconciliation with accounting data is needed, and possibility of mismatch of data is always there.

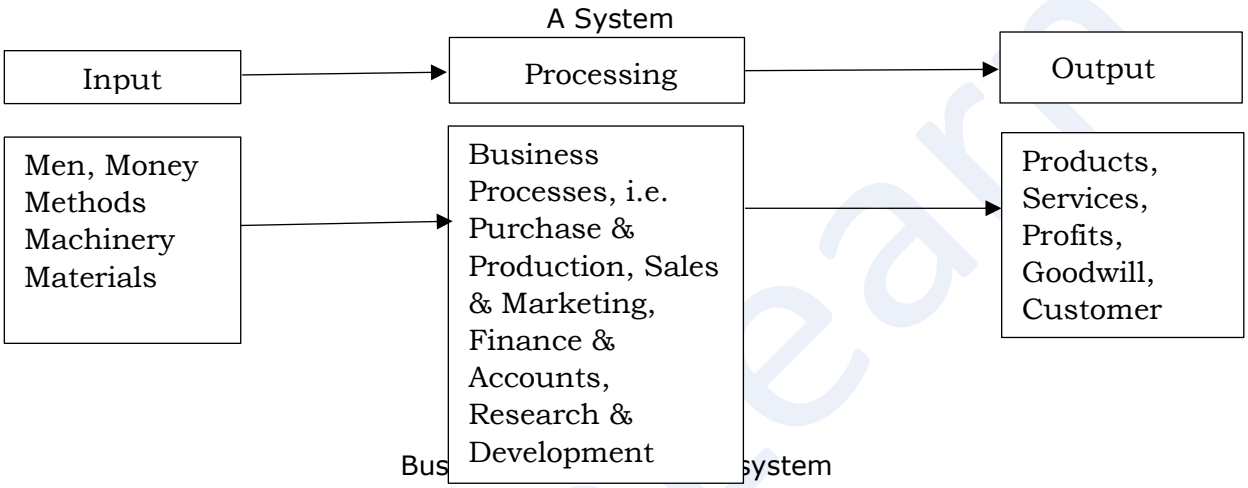
(42) Explain MAC and DAC in RBAC



Ch:3(a) Information Systems

(1)Define a System and give examples. Explain Business Enterprise as a System.

System is a set of inter–related and interacting elements that operate collectively to accomplish some common purpose or goal, accepting Inputs and producing outputs in an ordered transformation process. A System is described by specifying – (a) its parts, (b) the way in which they are related, and (c) the goals which they are expected to achieve. Examples: Human Body, Business Enterprise, Computer System, etc.



(2)Enumerate the characteristics of a Computer Based Information System

CBIS is a combination of People, IT and Business Processes that helps management in taking important decisions to carry out the business successfully.

CBIS consist of the following elements / components -

Item	Description
1. People	The end–objective of the CBIS is to be useful to people. People cover all type of persons, within and outside the Entity.
2. Hardware	(a) Hardware consists of Physical Components including Computer System, i.e. CPU, and all of its support equipment, i.e. peripherals e.g. Input Devices, Storage Devices, and Communications Devices. It includes Server or Smart Terminals with different configurations and Processors, etc. (b) Hardware Resources refer to – (i) Machines – Computers, Video Monitors, Magnetic Disk Drives, Printers, Optical Scanners, and (ii) Media – Floppy Disks, Magnetic tape, Optical Disks, Plastic Cards, Paper Forms, etc.
3. Software	(a) Software consists of Computer Programs and their User Documentation or Manuals. (b) Programs are machine–readable instructions that direct the CBIS Hardware to produce useful information from data. (c) Software includes – (i) different types of Operating Systems like UNIX, LINUX, WINDOWS, etc. (ii)Application Software

	(computer programs designed to perform specific tasks), and (iii) Utility Software (e.g. Tools). (d) Software Resources refer to – (i) Programs – Operating System Programs, Spreadsheet Programs, Word Processing Programs, Payroll Programs, and (ii) Procedures – Data Entry Procedures, Error Correction Procedures, Pay check Distribution Procedures, etc.
4. Data	(a)Data are facts that are used by programs to produce useful information. Like Programs, Data are generally stored in machine–readable form on disk or tape until the Computer needs them. (b)Data may be alphanumeric, text, image, video, audio and other forms. (c)In a CBIS, Data is organized in terms of a Database Management System (DBMS).
5. Network	Network means the Communication Media – Internet, Intranet, Extranet, etc.

(3)Write short notes on "Information System".

Information System (IS) is a combination of people, hardware, software, communication devices, network and data resources that processes data and information for a specific purpose.

- The system needs inputs from user which will then be processed using technology devices such as computers, and produce output that will be sent to another user or other system via a network and a feedback method that controls the operation.
- The main aim and purpose of each Information System is to convert the data into information which is useful and meaningful.
- An Information System is an arrangement of a number of elements that provides effective information for-
  - Decision Making, and /or
  - Control of some operations of an organization.
- Components: An Information System comprises of People, Hardware, Software, Data and Network for communication support.
- An Information System model comprises of following steps:
  - Input: Data is collected from an organization or from external environments and converted into suitable format required for processing.
  - Process: A process is a series of steps undertaken to achieve desired outcome or goal. Information Systems are becoming more and more integrated with organizational processes, bringing more productivity and better control to those processes.
  - Output: Then information is stored for future use or communicated to user after application of respective procedure on it.

(4)What are the basic activities of an "Information System Model"?

An Information System Model involves the following steps. These basic activities of an Information System help Entities in making decisions, control operations, analyse problems and create new products or services

1. Input: Data is collected from internal and external environments of an Entity, and converted into a suitable format required for processing,
2. Processing: Data is converted into information (i.e. more meaningful form) obtained after manipulation of these collected data.
3. Storage and Output: Information is stored for future use or communicated to User after application of specified procedures thereon.
4. Feedback: Feedback represents output that is returned to appropriate members of the Enterprise, to help them to evaluate at the input stage.

(5)Write short notes on Information Processing Cycle.

Information Management: To manage information effectively, every Enterprise has to –

1. Identify its information needs,
2. Acquire / Obtain that information from various sources,
3. Organize that information in a meaningful way,
4. Ensure information quality, and
5. Provide Software Tools for Users to access the required information.

The above activities may be referred to as the Information Processing Cycle.

(6)Differentiate between a Manual Information Processing and Computer–Based Information Processing.

Differences between a Manual Information Processing and Computer Based Information Processing

Point	Manual Information Processing	Computer–Based Information Processing (CBIS)
Concept	These are the systems where the level of manual intervention is very high, with little or no room for Computer Processing.	These are systems where Computers are used at every stage of transaction processing. Human intervention is very limited, or sometimes even Nil.
Input	Recording details in various Register maintained in paper form.	Entering data into computer, sometimes online real time basis.
Process	Summarize the Information using various arithmetic/logical processes.	Performing various arithmetic / logical operations on the data.
Output	Presentation of information to Users and Management in the form of Statements and Reports.	Presentation of information to Users and Management using various tools, like pictures, graphs, reports, etc.

Storage	Records stored in paper form, occupying huge space, and sometimes retained for a certain period only.	Records are stored in digital form, occupy less space, and can be stored for any time period in some cases.
Examples	Teaching, Valuation of Exam Papers, Medical Treatment like Surgery, etc.	Valuation of Exam in Multiple Choice Questions through Character Recognition, Filing of Income Tax Returns in e–form, etc.
Merits	Scope for handling exceptions, suitable for small volume of data, etc.	Huge abilities for processing data, storage, immediate feedback, timely, accurate, fast and reliable info, etc.

(7) What are the components of a Computer–Based Information System? Explain briefly.

CBIS is a combination of People, IT and Business Processes that helps management in taking important decisions to carry out the business successfully. CBIS consists of the following elements / components -

Item	Description
People	The end–objective of the CBIS is to be useful to people. People cover all type of persons, within and outside the Entity.
Hardware	(a) Hardware consists of Physical Components including Computer System, i.e. CPU, and all of its support equipment, i.e. peripherals e.g. Input Devices, Storage Devices, and Communications Devices. It includes Server or Smart Terminals with different configurations and Processors, etc. (b) Hardware Resources refer to – (i) Machines – Computers, Video Monitors, Magnetic Disk Drives, Printers, Optical Scanners, and (ii) Media – Floppy Disks, Magnetic tape, Optical Disks, Plastic Cards, Paper Forms, etc.
Software	(a) Software consists of Computer Programs and their User Documentation or Manuals. (b) Programs are machine–readable instructions that direct the CBIS Hardware to produce useful information from data. (c) Software includes – (i) different types of Operating Systems like UNIX, LINUX, WINDOWS, etc. (ii)Application Software (computer programs designed to perform specific tasks), and (iii) Utility Software (e.g. Tools). (d) Software Resources refer to – (i) Programs – Operating System Programs, Spreadsheet Programs, Word Processing

	Programs, Payroll Programs, and (ii) Procedures – Data Entry Procedures, Error Correction Procedures, Pay check Distribution Procedures, etc.
Data	Data are facts that are used by programs to produce useful information. Like Programs, Data are generally stored in machine–readable form on disk or tape until the Computer needs them. Data may be alphanumeric, text, image, video, audio and other forms. In a CBIS, Data is organized in terms of a Database Management System (DBMS).
Network	Network means the Communication Media – Internet, Intranet, Extranet, etc.

(8) Write short notes on "People" as a component of a Computer–Based Information System.

"People" as a component of a Computer–Based Information System:

- People constitute the most important elements in almost all Computer–Based Information Systems (CBIS).
- Both Internal Users (Management, Staff, System Users) and External Users (Government, Vendors, Customers, etc.) may require information provided by the CBIS, and constitute the "People" Component of the CBIS.
- Within the Entity, People include System Users and Information System Personnel, i.e. all the people who manage, run, program and maintain the system.
- Internal Users may be at all levels of the Entity's hierarchy, – (a) End Users – the persons who can use Hardware and Software for retrieving the desired information, (b) Programmers, (c) System Analysts, & (d) Database Administrators.
- All persons, from the Helpdesk to the System Programmers and up to the Chief Information Officer (CIO), all persons are an integral part of the CBIS.
- Role of People is significant in terms of "Innovation", i.e. using Technology productively to increase efficiency and improve an Entity's competitive advantage.

(9) Explain the following terms in the context of "Hardware" in a CBIS – (a) Input Devices, (b) Processing Devices, (c) Storage Devices, (d) Output Devices

Hardware is the tangible portion of our computer systems; something we can touch and see. It basically consists of devices that perform the functions of input, processing, data storage and output activities of the computer.

(a) **Input devices:** There are devices through which the user interact with the systems. Input devices include -

Device	**Type of Input**
Keyboards	Text–based input
Mouse and other Pointing Devices	Position–based input
Scanners & Bar Code / MICR Readers, Webcams	Image–based input
Microphone	Voice–based input

Stylus/ Touch Screen	Screen Touch input

(b) **Processing Devices:** Processing Devices refer to computer chips that contain the Central Processing Unit (CPU or Microprocessor) and Main Memory.

- CPU is the actual hardware that interprets and executes the program (software) instructions and coordinates how all the other hardware devices work together.
- CPU is built on a small flake of silicon and can contain the equivalent of several million transistors. Transistors can be viewed as switches which could be" on" or "off", i.e. taking a value of 1 or 0 respectively.
- CPU is the brain of the computer, and its main function is to execute programs stored in memory.
- CPU consists of three functional units –

I. **Control Unit (CU):** CU controls the flow of data and instruction to and from memory, interprets the instruction and controls which tasks to execute and when.

II. **Arithmetic and Logical Unit (ALU):** ALU performs various arithmetic operations (e.g. addition, subtraction, multiplication, division, etc.), and logical operations (e.g. comparison of numbers: Equal to, Greater than, Less than, etc.)

III. **Registers:** These are high speed memory units within CPU for storing small amount of data (mostly 32 or 64 bits).

Registers could be –

- **Accumulators**: They can keep running totals of arithmetic values.
- **Address Registers**: They can store memory addresses which tell the CPU as to where in the memory an instruction is located.
- **Storage Registers:** They temporarily store data that is being sent to or coming from the system memory.
- **Miscellaneous:** These are used for several functions for general purpose.

(c) **Data Storage Devices:** These refer to the memory where data and programs are stored. Some of the types of memory techniques / devices are –

Type	Description
Internal Memory	Registers are internal memory within CPU, which are very fast, but very small.
Primary Memory	a) Primary Memory (Main Memory) is used by CPU for execution of programs b) In Main Memory, any location can be accessed in any order (in contrast with sequential order). c) Main Memory is not used for storing data, and is generally small in terms of storage capacity. d) Main Memory is primarily of two types – RAM and ROM
Cache Memory	a) Cache is a smaller, faster memory, which stores copies of the data from the most frequently used Main Memory locations, so that Processor/Registers can access it more rapidly than Main Memory.

	b) Cache is the property of locality of reference, which allows improving substantially the effective memory access time in a computer system. c) Cache Memory is used to bridge the huge speed difference between Registers and Primary Memory
Virtual Memory	a) Virtual Memory is an allocation of hard disk space to help RAM. b) It is not a separate device as such, but an imaginary memory area supported by some Operating Systems (e.g. Windows) in conjunction with the hardware. c) If a Computer lacks the RAM needed to run a program or operation, Windows OS moves data from RAM to a space (in the Hard Disk) called a Paging File. d) Moving data to and from the Paging File frees up RAM, and the Program / Operation can now be completed by combining the Computer's RAM with temporary space on the Hard Disk
Secondary Memory	a) Secondary Memory is available in bigger sizes to store programs and data. b) Secondary Storage is accessible by the CPU, only through Input / Output Channels. The CPU then transfers the desired data using intermediate area in Primary Storage. c) Some commonly used Secondary Storage are: USB Pen Drives, Floppy Drive, Hard Drive, CD, DVD, Blue Ray Disks and Smart Cards. d) Features of Secondary Memory devices are – • non–volatility (contents are permanent in nature, and not lost if switched off), • greater capacity (available in larger size), • greater economy (low cost when compared to Registers and RAMs), • slow speed (slower when compared to Registers or Primary Storage), and • portability (can be used across various devices / computers).

(d) **Output Devices:** These are devices through which the Computer provides output / information to the User / Decision–maker. Output may be classified into the following types –

- Textual Output –characters that are used to create words, sentences, and paragraphs.
- Graphical Outputs – drawings, charts, photographs, and animation, which provide digital representations of non–text information.
- Tactile Output – e.g. Raised Line Drawings which may be useful for visually challenged persons.
- Audio Output – music, speech, or any other sound.
- Video Output – Images played back at speeds to provide the appearance of full motion.

(10) Differentiate between RAM and ROM

Differences between RAM and ROM

Random Access Memory (RAM)	Read Only Memory (ROM)
Volatile in nature means Information is lost as soon as power is turned off.	Non-volatile in nature (contents remain intact even in absence of power).
Purpose is to hold program and data while they are in use.	Used to store small amount of information for quick reference by CPU.
Information can be read as well as modified.	Information can be read not modified.
Responsible for storing the instructions and data that the computer is using at that present moment.	Generally used by manufacturers to store data and programs like translators that is used repeatedly.

(11) What are the activities and functions of System Software and Operating Systems? System Software is the Computer Software that is designed to operate the computer hardware, and to give and maintain a platform for running Application Software. Computer Operating Systems is one of the widely used System Software.

Meaning of Operating Systems (OS):

a) OS is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs.
b) Application Programs require an Operating System to function, which provides a convenient environment to Users for executing their programs.
c) Windows, Linux, UNIX, etc. are some widely used Operating Systems.

Functions / Activities:

- **Hardware Functions:** OS acts as an Intermediary between the Application Program and the Hardware. Application Programs obtain input from Keyboards, retrieve data from Disks & display output on Monitors, using the OS.
- **User Interfaces' provides User Interface –** (a) Command Based User Interface, i.e. text commands in DOS Systems, and (b) Graphic User Interface (GUI) using icons & menus.
- **Hardware Independence**: OS provides Application Program Interfaces (API), which can be used by Application Developers to create application software for all types of Hardware. Thus, OS gives us Hardware independence.
- **Memory Management:** OS manage as to how memory is accessed and maximize available memory & storage. OS also provides Virtual Memory (Virtual RAM) by carving an area of hard disk to supplement the functional memory capacity of RAM.
- **Task Management:** Task Management feature of Operating system helps in allocating resources to make optimum utilization of resources. This facilitates – (a) one User working on various applications (i.e. multi–tasking), and also (b) multiple User to use the system (i.e. timesharing)
- **Networking Capability:** OS provides systems with features & capabilities to help connect Computer Networks, both Intranet and Internet.

- **Logical Access Security:** OS provide logical security by establishing a procedure for identification & authentication using a User ID and Password. It also creates logs on User Access.
- **File Management:** OS keeps a track of where each file is stored and who can access it, based on which it provides the file retrieval.

(12) What is a DBMS? Explain its significance.

DBMS may be defined as a software that aid in organizing, controlling and using the data needed by the application programme. They provide the facility to create and maintain a well-organized database.

Significance:

a) DBMS is a tool to integrate the information flow within an Entity.
b) DBMS highlights the importance of data as a resource in the Entity, and as something that has to be carefully managed.
c) DBMS provide the facility to create and maintain a well–organized database.
d) DBMS is the Software that aid in organizing, controlling and using the data needed by the Application Programme, Applications access the DBMS, which then accesses the data.

(13) What are the various activities performed using DBMS?

Data Base Management System (DBMS) is a computer program which organizes data in a database, providing information storage, organisation, and retrieval capacities, including simultaneous access to multiple databases through a shared field.

DBMS helps us do various operations on the files, viz. –

a. Adding new files to Database,
b. Deleting existing files from Database,
c. Inserting data in existing files,
d. Modifying data in existing files,
e. Deleting data in existing files, and
f. Retrieving or querying data from existing files.

(14) Explain the concept of "Hierarchy of Database".

Database is a collection of facts (data) in files, and is similar to an electronic filing cabinet, i.e. a collection of computerized data files. A Database Model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated.

Hierarchy of database is as under:

Hierarchy	Description	Example
Database	This is a collection of Files	History of Income Tax Return details of Assesses
File	This is a collection of Records	Income Details of one Financial Years of an Assessee
Record	This is a collection of Fields	Name, Residential Status, Income Tax PAN of Assessee

Field	This is a collection of Characters	10–Digit Income Tax Permanent Account Number (PAN)
Characters	These are a collection of Bits	Each Digit / Alphabet in Income Tax PAN

(15) Explain the various types of "Record Relationships" in a Database.

When designing the Database to make it easy for the end user to use the database for different purposes, the following relationships are to be considered –

Relationship	Example
One : One	In a Multi–Speciality Hospital, the Doctor sees a patient and writes a prescription for that patient.
One : Many	A Doctor sees many patients and writes prescriptions for each person separately
Many : One	Many Specialist Doctors see a single patient.
Many : Many	The Billing Section of the Hospital processes the bills of different patients from different doctors.

(16) List a few merits and demerits of DBMS.

Merits of DBMS: -

- **Permitting Data Sharing:** One of the principle advantages of a DBMS is that the same information can be made available to different users.
- **Minimizing Data Redundancy:** In a DBMS, duplication of information or redundancy is, if not eliminated, carefully controlled or reduced i.e. there is no need to repeat the same data repeatedly. Minimizing redundancy reduces significantly the cost of storing information on storage devices.
- **Integrity can be maintained:** Data integrity is maintained by having accurate, consistent, and up-to-date data. Updates and changes to the data only must be made in one place in DBMS ensuring Integrity.
- **Program and File consistency:** Using a DBMS, file formats and programs are standardized. The level of consistency across files and programs makes it easier to manage data when multiple programmers are involved as the same rules and guidelines apply across all types of data.
- **User-friendly:** DBMS makes the data access and manipulation easier for the user. DBMS also reduces the reliance of users on computer experts to meet their data needs.
- **Improved security:** DBMS allows multiple users to access the same data resources in a controlled manner by defining the security constraints. Some sources of information should be protected or secured and only viewed by select individuals. Using passwords, DBMS can be used to restrict data access to only those who should see it.
- **Achieving program/data independence:** In a DBMS, data does not reside in applications but data bases program & data are independent of each other.
- **Faster Application Development:** In the case of deployment of DBMS, application development becomes fast. The data is already therein databases,

application developer has to think of only the logic required to retrieve the data in the way a user need.

Demerits of a DBMS: -

- **Cost:** Implementing a DBMS system in terms of both system and user-training can be expensive and time-consuming, especially in large enterprises. Training requirements alone can be quite costly.
- **Security:** Even with safeguards in place, it may be possible for some unauthorized users to access the database. If one gets access to database, then it could be an all or nothing proposition.

(17) Differentiate between Hierarchical and Network Database Models.

Differentiation between Hierarchical and Network Database Models as follows:

Hierarchical database Model:

a) Here, the records are logically organized into a hierarchy of relationships and involve an inverted tree structure.
b) The Tree is composed of a hierarchy of Nodes, the uppermost node is called the Root (Top Parent Record).
c) A Node which has other dependent nodes is called Parent while the dependent nodes are called as Children.
d) With the exception of the Root, every Node is related to a Node at a higher level called its Parent.
e) No Child Record can have more than one Parent Record. However, each Parent Record can have multiple lower level (Child) records.

Network Database Model:

a) Network Model is a modification of the Hierarchical Model, and permits multiple–branches from one or more Nodes.
b) The Child–Parent relationship of the Hierarchical Model is replaced by Owner–Member Relationship under the Network Model.
c) The Records are viewed in Sets. Each Set has an Owner Record and one or more Member Records.
d) Each Record can be a Member of one or more Parent Set at the same time. This means that each Node (Child or Member Record) may have several Parents (or Owner Records).
e) Network Model is useful for all relationship types – one–to–one, one–to–many, many–to–one and many–to–many.
f) Network Databases implement the set relationships users Pointers that directly address the location of a record on disk. This gives excellent retrieval performance, at the expense of operations such as database loading and reorganization.
g) Network Model is able to represent redundancy in data more efficiently than in the Hierarchical Model.

(18) Explain the following concepts in the context of Database – (a) Big Data, (b) Data Warehouse, (c) Data Mining.

(a) Big data: Big Data refers to massive and huge data sets, that traditional Database–Management tools do not have the processing power to analyse them. Storing, analysing, processing and interpreting such data requires the best tools and techniques based on advanced technology. Examples: Details of Cash Deposits and Withdrawals in the Banking System during a period, Item– wise Details of Sweets sold by an Entity during a festival season, etc.

(b) Data warehouse: Data from an Entity's Database(s) that support its day–to–day operations are extracted periodically and sent to a Data Warehouse [i.e. a "Master Database"] for storage and analysis. A Data Warehouse should be designed so that it meets the following criteria –

(i) It uses Non–Operational data, i.e. data which is not required for day–to–day operations.
(ii) It is updated on scheduled basis, i.e. current data from an Entity's Active / Operational Databases are pulled into the Data Warehouse on a regular, scheduled basis.
(iii) It contains time–variant data, i.e. whenever data is loaded into the Data Warehouse, it receives a time stamp, which allows for comparisons between different time periods.
(iv) It uses standardised data, drawn from multiple Database(s) in the Entity. If the data format is not the same amongst these Databases, it is first converted into a standard format using Extraction–Transformation–Load (ETL) Process.

A Data Warehouse may be designed using two approaches –

(i) **Bottom–Up Approach** builds small Data Warehouses, called Data Marts, to solve specific business problems initially. All these Data Marts are then integrated into a larger Data Warehouse.
(ii) **Top–Down Approach** leads to the creation of an Entity–wide Data Warehouse and subsequent creation of smaller Data Marts from the bigger Warehouses, to address specific business needs.

(c) Data mining: Data Mining is the process of analysing data to find previously unknown trends, patterns, and associations to make decisions. Data Mining is achieved through automated means, in extremely voluminous and large data sets, such as a Data Warehouse. Data Mining may be approached from two angles –

(i) Analysing data without any such previous assumption / pre–supposition.
(ii) Analysing data to understand whether a particular hypothetical assumption about people behaviour / data is correct,

Examples: Income Tax Department mines data of higher amounts of Cash Deposits / Withdrawals in the Banking System, to identify potential taxpayers.

Data Mining involves –

(i) Selecting Relevant / Target Data from Databases,

(ii) Integrating all the Target Data into a Data Warehouse,
(iii) Using Mining Tools and Techniques to identify Data Patterns,
(iv) Evaluating and interpreting the data patterns, to support Business Knowledge and Strategies.

(19) What is a Computer Network? What are its conceptual types?

Computer Network is a collection of computers and other hardware, inter–connected by communication channels that allow sharing of resources and information. Computer Networks can be conceptualized into two types –

(i) **Connection oriented networks:** Here, a connection is first established and then data exchanged. This is similar to operation of telephone networks.
(ii) **Connectionless networks:** Here, there is no prior connection made before data exchanges. Data being exchanged has a complete contact information of Recipient, and at each intermediate destination, it is decided how to proceed further, similar to Postal Networks.

(20) Explain the benefits of Computer Networks.

The following are the important benefits of a computer network:

(i) **Distributed nature of information**: There would be many situations where information must be distributed geographically. E.g. in the case of Banking Company, accounting information of various customers could be distributed across various branches but to make Consolidated Balance Sheet at the year-end, it would need networking to access information from all its branches.
(ii) **Resource Sharing:** Data could be stored at a central location and can be shared across different systems. Even resource sharing could be in terms of sharing peripherals like printers, which are normally shared by many systems. E.g. In the case of a CBS, Bank data is stored at a Central Data Centre and could be accessed by all branches as well as ATMs.
(iii) **Computational Power:** The computational power of most of the applications would increase drastically if the processing is distributed amongst computer systems. For example: processing in an ATM machine in a bank is distributed between ATM machine and the central Computer System in a Bank, thus reducing load on both.
(iv) **Reliability:** Many critical applications should be available 24x7, if such applications are run across different systems which are distributed across network then the reliability of the application would be high. E.g. In a city, there could be multiple ATM machines so that if one ATM fails, one could withdraw money from another ATM.
(v) **User communication:** Networks allow users to communicate using e-mail, newsgroups, video conferencing, etc.

(21) Outline the significance of Telecommunications in Computer Networks. Significance of Telecommunications in Computer Networks:

(i) **Time compression:** Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.

(ii) **Overcoming geographical dispersion:** Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit. The firm can then reap benefits of scale and scope which would otherwise be unobtainable.

(iii) **Restructuring business relationships:** Telecommunications make it possible to create systems which restructure the interactions of people within a firm as well as a firm's relationships with its customers. Operational efficiency may be raised by eliminating intermediaries from various business processes.

(22) Write short notes on Segregation of Duties (SoD) in the context of IT.

SoD Concept seeks to ensure that a single individual does not possess excess privileges, that could result in unauthorized/harmful activities like fraud or the manipulation or exposure of sensitive data.

Example: In the area of Payment Processing, the activities of – (i) Creation of Vendor Code, (ii)Authorisation of Vendor's Bills, and (iii) Printing of Cheques are handled by separate individuals.

SoD Controls –

- are in the nature of Preventive and Detective Controls place to manage segregation of duties matters.
- can be manual or even automated, depending on the nature of transaction, situation, and sometimes require manual intervention in an automated control.

(23) Write short notes on Roles and Responsibilities in the context of IT.

Several roles and responsibilities fall upon all individuals throughout the organization.

a) Executive management: The most senior managers and executives in an organization are responsible for developing the organization's mission, objectives, and goals, as well as policy. Executives are responsible for enacting security policy, which defines (among other things) the protection of assets.

b) Owner: An owner is an individual (usually but not necessarily a manager) who is the designated owner-steward of an asset. Depending upon the organization's security policy, an owner may be responsible for the maintenance and integrity of the asset, as well as for deciding who is permitted to access the asset. If the asset is information, the owner may be responsible for determining who may access and make changes to the information.

c) Manager: A manager is, in the general sense, responsible for obtaining policies and procedures and making them available to their staff members. They should also, to some extent, be responsible for their staff members' behaviour.

d) User: Users are individuals (at any level of the organization) who use assets in the performance of their job duties. Each user is responsible for how he or she uses the asset, and does not permit others to access the asset in his or her name. Users are responsible for performing their duties lawfully and for conforming to organization policies.

These generic roles and responsibilities should apply across the organization chart to include every person in the organization.

(24) What is a Job Title? What is its significance?

Job Title is a label that is assigned to a job description. It denotes a position in the organization that has a given set of responsibilities, and which requires a certain level and focus of education and prior experience.

Significance of job titles:

(i) **Recruiting:** When the organization needs to find someone to fill an open position, the use of standard job titles will help prospective candidates more easily find positions that match their criteria.

(ii) **Compensation base lining**: Because of the chronic shortage of talented IT workers, organizations are forced to be more competitive when trying to attract new workers. To remain competitive, many organizations periodically undertake a regional compensation analysis to better understand the levels of compensation paid to IT workers in other organizations. The use of standard job titles makes the task of comparing compensation far easier.

(iii) **Career advancement:** When an organization uses job titles that are consistent in the industry, IT workers have a better understanding of the functions of positions within their own organizations and can more easily plan how they can advance. The remainder of this section includes many IT job titles with a short description (not a full job description by any measure) of the function of that position.

(25) Give a few examples of Job Titles and Job Descriptions in IT in the following areas (a) Executive Management, (b) Systems Management, (c) Software Management, (d)Data Management, (e) Network Management, (f) Security Management, (g) Operations Management, (h) Service Desk.

a) **Executive Management:** Executive managers are the chief leaders and policymakers in an organization. They set objectives and work directly with the organization's most senior management to help make decisions affecting the future strategy of the organization.

(i) **CIO (Chief Information Officer):** This is the title of the top most leaders in a larger IT organization.

(ii) **CTO (Chief Technical Officer):** This position is usually responsible for an organization's overall technology strategy. Depending upon the purpose of the organization, this position may be separate from IT.

(iii) **CSO (Chief Security Officer):** This position is responsible for all aspects of security, including information security, physical security, and possibly executive protection (protecting the safety of senior executives).

(iv) **CISO (Chief Information Security Officer):** This position is responsible for all aspects of data-related security. This usually includes incident management, disaster recovery, vulnerability management, and compliance.

(v) **CPO (Chief Privacy Officer):** This position is responsible for the protection and use of personal information. This position is found in organizations that collect and store sensitive information for large numbers of persons.

b) Systems Management: Positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems. This may include desktop operating systems as well.

(i) **Systems Architect:** This position is responsible for the overall architecture of systems (usually servers), both in terms of the internal architecture of a system, as well as the relationship between systems. This position is usually also responsible for the design of services such as authentication, e-mail, and time synchronization.

(ii) **Systems Engineer:** This position is responsible for designing, building, and maintaining servers and server operating systems.

(iii) **Storage Engineer:** This position is responsible for designing, building, and maintaining storage subsystems.

(iv) **Systems Administrator:** This position is responsible for performing maintenance and configuration operations on systems.

c) Software Development: Positions in software development are involved in the design, development, and testing of software applications.

(i) **Systems Architect:** This position is usually responsible for the overall information systems architecture in the organization. This may or may not include overall data architecture as well as interfaces to external organizations.

(ii) **Systems Analyst:** A systems analyst is involved with the design of applications, including changes in an application's original design. This position may develop technical requirements, program design, and software test plans. In cases where organizations license applications developed by other companies, systems analysts design interfaces to other applications.

(iii) **Software Developer and Programmer:** This position develops application software. Depending upon the level of experience, persons in this position may also design programs or applications. In organizations that utilize purchased application software, developers often create custom interfaces, application customizations, and custom reports.

(iv) **Software Tester:** This position tests changes in programs made by software developers.

d) Data Management: Positions in data management are responsible for developing and implementing database designs and for maintaining databases.

(i) **Database Architect:** This position develops logical and physical designs of data models for applications. With sufficient experience, this person may also design an organization's overall data architecture.

(ii) **Database Administrator (DBA):** This position builds and maintains databases designed by the database architect and those databases that are included as a part of purchased applications. The DBA monitors databases, tunes them for performance and efficiency, and troubleshoots problems.

(iii) **Database Analyst:** This position performs tasks that are junior to the database administrator, carrying out routine data maintenance and monitoring tasks.

e) **Network Management:** Positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks, including connections to outside business partners and the Internet.
   (i) **Network Architect:** This position designs data and (increasingly) voice networks and designs changes and upgrades to the network as needed to meet new organization objectives.
   (ii) **Network Engineer:** This position builds and maintains network devices such as routers, switches, firewalls, and gateways.
   (iii) **Network Administrator:** This position performs routine tasks in the network such as making minor configuration changes and monitoring event logs.
   (iv) **Telecom Engineer:** Positions in this role work with telecommunications technologies such as data circuits, phone systems, and voice email systems.

f) **Security Operations:** Positions in security operations are responsible for designing, building, and monitoring security systems and security controls, to ensure the confidentiality, integrity, and availability of information systems.
   (i) **Security Architect:** This position is responsible for the design of security controls and systems such as authentication, audit logging, intrusion detection systems, intrusion prevention systems, and firewalls.
   (ii) **Security Engineer:** This position is responsible for designing, building, and maintaining security services and systems that are designed by the security architect.
   (iii) **Security Analyst:** This position is responsible for examining logs from firewalls, intrusion detection systems, and audit logs from systems and applications. This position may also be responsible for issuing security advisories to others in IT.
   (iv) **User Account Management:** This position is responsible for accepting approved requests for user access management changes and performing the necessary changes at the network, system, database, or application level. Often this position is carried out by personnel in network and systems management functions; only in larger organizations is user account management performed in security or even in a separate user access department.
   (v) **Security Auditor:** This position is responsible for performing internal audits of IT controls to ensure that they are being operated properly.

g) **General Operations:** Positions in operations are responsible for day-to-day operational tasks that may include networks, servers, databases, and applications.
   (i) **Operations Manager:** This position is responsible for overall operations that are carried out by others. Responsibilities will include establishing operations shift schedules.
   (ii) **Operations Analyst:** This position may be responsible for the development of operational procedures; examining the health of networks, systems, and databases; setting and monitoring the operations schedule; and maintaining operations records.
   (iii) **Controls Analyst:** This position is responsible for monitoring batch jobs, data entry work, and other tasks to make sure that they are operating correctly.

(iv) **Systems Operator:** This position is responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.

(v) **Data Entry:** This position is responsible for keying batches of data from hard copy sources.

(vi) **Media Librarian:** This position is responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

h) Service Desk: Positions at the service desk are responsible for providing front line support services to IT and IT's customers.

(i) **Help desk Analyst:** This position is responsible for providing front line user support services to personnel in the organization.

(ii) **Technical Support Analyst:** This position is responsible for providing technical support services to other IT personnel, and perhaps also to IT customers.

Ch:3(b) Information Systems' Controls

(1) Outline the need for IS Controls and IS Audit.

The need for control and audit of computer–based information systems are brought out as under –

(i) **Information = Asset:** Information is an enterprise's most valuable asset. So, its protection from unauthorized use, from both within and outside the entity, is an IT priority.

(ii) **Incorrect Decision Making:** Management and Operational Controls by Managers involve detection, investigations and correction of out–of–control processes. These decisions require accurate data to make quality decision rules.

(iii) **Value of IT Resources:** IT Resources, viz. Hardware, Software and Personnel, are critical resources of an organization, which has a credible impact on its infrastructure and business competitiveness.

(iv) **Costs of Data Loss:** Loss of Data is a critical matter, and affects the organisation's ability to adapt and survive in a changing environment.

(v) **Cost of Computer Abuse:** Unauthorised access to computer systems, computer viruses, unauthorized physical access to computer facilities and unauthorized copies of sensitive data, can lead to destruction of IT Assets.

(vi) **Costs of Computer Error:** In a CIS Environment where many critical processes are performed through computers, data error during entry or process would cause a substantial damage.

(vii) **Maintenance of Privacy:** Data collected in a business process contains details about an individual on medical, educational, employment, residential and other details. There is a risk of loss of privacy of such personal information.

(viii) **Controlled evolution of Computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

(2) List some critical control aspects, which are lacking in a computerized environment

Some of the critical control lacking in a computerized environment are as follows:

(i) Lack of management understanding of IS risks and related controls;

(ii) Absence or inadequate IS control framework;

(iii) Absence of weak general controls and IS controls;

(iv) Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;

(v) Complexity of implementation of controls in distributed computing environments and extended enterprises;

(vi) Lack of control features or their implementation in highly technology driven environments; and

(vii) Inappropriate technology implementations or inadequate security functionality in technologies implemented.

(3) Explain the meaning of the terms – (a) Control, (b) Control Objectives, in the context of IT.

Control is defined as the policies, procedures and practices of enterprise structure, that are designed to provide reasonable assurance that –

(a) business objectives will be achieved, and

(b) undesirable events are prevented or detected and corrected.

The major Control Objectives are –

(i) **Authorization:** All transactions are approved by responsible personnel in accordance with their specific or general authority before the transaction is recorded.

(ii) **Completeness:** No valid transactions should be omitted from the accounting records.

(iii) **Accuracy:** All valid transactions are accurate, consistent with the originating transaction data, and information is recorded in a timely manner.

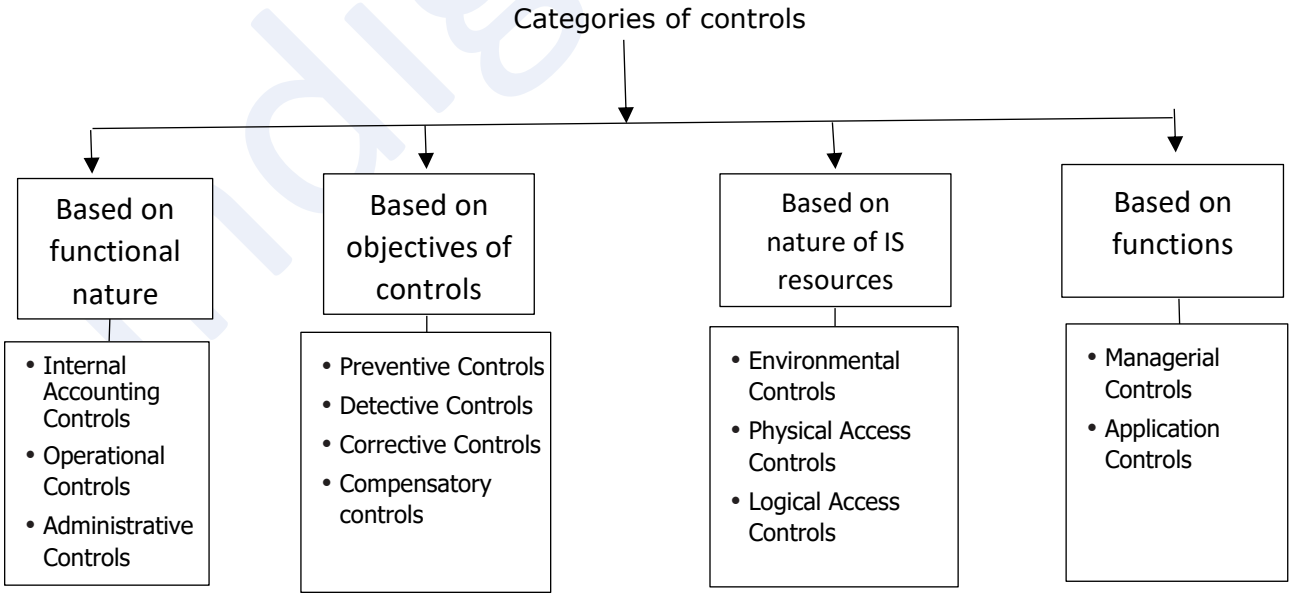
(iv) **Validity:** All recorded transactions fairly represent the economic events that actually occurred, are lawful in nature, and have been executed in accordance with Management's general authorization

(v) **Physical Safeguards and Security:** Access to physical assets and information systems are controlled and properly restricted to authorized personnel.

(vi) **Error Handling:** Errors detected at any stage of processing receive prompts corrective action and are reported to the appropriate level of Management.

(vii) **Segregation of Duties:** Duties are assigned to individuals such that no one individual can control both the recording function and the procedures relative to processing a transaction.

(4) What are the different ways in which IT Controls can be classified?



(5) Briefly explain the classification of IT Controls based on Objectives Controls based on objectives.

1) **Preventive controls:** Preventive controls prevent errors, omissions or security incidents from occurring. In other words, Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Some of the examples of Preventive Controls are as follows:
   a) Employing qualified personnel for certain jobs.
   b) Training and re–training of staff.
   c) Segregation of duties and authorization of transactions.
   d) Access Control, e.g. use of Passwords
   e) Documentation.
   f) Validation and Edit Checks in the application.
   g) Firewalls.
   h) Anti–Virus Software
2) **Detective controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. In other words, Detective Controls detect errors or incidents that elude preventive controls. Detective controls can also include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. The main characteristics of such controls are given as follows:
   a) Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
   b) An established mechanism to refer the reported unlawful activities to the appropriate person or group;
   c) Interaction with the preventive control to prevent such acts from occurring
   d) Surprise checks by supervisor.
3) **Corrective controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. It is desirable to correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data-entry errors, to identifying and removing unauthorized users or software from systems or networks, to recovery from incidents, disruptions, or disasters. The main characteristics of the corrective controls are as follows:
   a) Minimizing the impact of the threat;
   b) Identifying the cause of the problem;
   c) Providing Remedy to the problems discovered by detective controls;
   d) Getting feedback from preventive and detective controls;
   e) Correcting error arising from a problem; and
   f) Modifying the processing systems to minimize future occurrences of the incidents.

(6) Briefly explain the classification of IT Controls based on Nature of IS Resources.

Based on the nature of IS Resources to which they are applied, Controls are classified as under –

1) **Environmental Controls:** Controls relating to housing IT Resources, e.g. Power, Air–Conditioning, UPS, Smoke Detectors, Fire–Extinguishers, Dehumidifiers, etc.
2) **Physical Access Controls:** Controls relating to physical security of the tangible IS Resources and intangible resources stored on tangible media, etc. Such controls include Access Control Doors, Security Guards, Door Alarms, restricted entry to secure areas, visitor logged access, video monitoring, etc.

3) **Logical Access Controls:** Controls relating to logical access to information resources, e.g. Operating Systems Controls, Application Software Boundary Controls, Networking Controls, Access to Database Objects, Encryption Controls, etc.

(7) Write short notes on the General Considerations in Protection from Environmental Exposures / Risks.

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

Fire: It is a major threat to the physical security of a computer installation. Some of the controls are as follows:

- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
- Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water-based systems, halon etc., depending upon the situation may be used.
- Manual fire extinguishers can be placed at strategic locations.
- Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire-Resistant Office Materials such as waste-baskets, curtains, desks, and cabinets should be used.

Electrical Exposures: These include risk of damages that may be caused due electrical faults. These include non-availability of electricity, spikes (temporary very high voltages), fluctuations of voltage and other such risk.

- The risk of damage due to power spikes can be reduced using Electrical Surge Protectors that are typically built into the Un-interruptible Power System (UPS).
- Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power.
- Emergency Power-Off Switch: When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

Water Damage: Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc.

- Wherever possible have waterproof ceilings, walls and floors;
- Ensure an adequate positive drainage system exists;
- Install alarms at strategic points within the installation;
- Water proofing; and
- Water leakage Alarms.

Pollution Damage and others: The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors.

Some of the controls are as follows:

- Power Leads from Two Substations: Electrical power lines that are exposed to many environmental dangers such as water, fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply.
- Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility: These activities should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

(8) What are the special precautions to be taken for Protection of IT Systems from Fire?

Following are the special precautions to be taken for Protection of IT Systems from Fire: -

- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
- Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation may be used.
- Manual fire extinguishers can be placed at strategic locations.
- Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as waste-baskets, curtains, desks, and cabinets should be used.
- Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
- All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
- Less Wood and plastic should be in computer rooms.
- Use a gas based fire suppression system

(9) What are the special precautions to be taken for Protection of IT Systems from Electric Shock / Spike, etc?

Following are the special precautions to be taken for Protection of IT Systems from Electric Shock / Spike: -

- The risk of damage due to power spikes can be reduced using Electrical Surge Protectors that are typically built into the Un-interruptible Power System (UPS).
- Un-interruptible Power System (UPS)/Generator: In case of a power failure, the UPS provides the back up by providing electrical power from the battery to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to

permit an orderly computer shutdown.

- Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power.
- Emergency Power-Off Switch: When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

(10) Outline the various categories of Physical Access Control Techniques?

Controlling Physical Access

1) **Perimeter Fencing:** Fencing at the boundary of the facility will enhance the security mechanism.
2) **Video Cameras:**
   a. Cameras should be placed at specific locations and monitored by security guards.
   b. Refined video cameras can be activated by motion.
   c. Video supervision recording must be retained for possible future playback / evidence purposes.
3) **Controlled Visitor Access:**
   a. Visitors may be Friends, Maintenance Personnel, Computer Vendors, Consultants & External Auditors.
   b. A responsible employee should escort all visitors to the employee whom the Visitor intends to meet.
4) **Controlled Single Entry Point:** All incoming personnel should use controlled only a Single-Entry Point. This controlled entry point should be monitored by a Receptionist and Security Guards. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or dead–locked.
5) **Security Guards:**
   a. Extra security can be provided by appointing guards aided with video cameras and locked doors.
   b. Guards supplied by an external agency should be made to sign a bond, in order to protect the organisation from loss.
6) **Dead Man Doors:**
   a. These consist a pair of doors, that are generally found in entries to facilities like computer rooms and document stations.
   b. The first entry door must close and lock, for the second door to operate, and only one person will be permitted in the holding area.
   c. Only a single person is permitted to enter at a given point of time. This will reduce the risk of piggybacking, i.e. when an unauthorized person follows an authorized person through a secured entry.
7) **Alarm System:**
   a. Illegal entry can be avoided by linking an alarm system at places like –
      i. inactive entry point motion detectors, and
      ii. reverse flows of enter only or exit only doors, so as to avoid illegal entry / exit.

b. Security personnel should be able to hear the alarm when activated.

8) **Non–exposure of Sensitive Facilities:**
   a. There should be no explicit indication (e.g. presence of windows or directional signs), hinting the presence of facilities like computer rooms.
   b. Only the general location of the Information Processing Facility (IPF) should be identifiable.
9) **Computer Terminal Locks:** These locks ensure that a node / device / terminal is not turned on or used by unauthorized persons.
10) **Indemnity Bonds:**
   a. All service contract personnel, (e.g. cleaning / maintenance staff, off–site storage service staff, etc.) should be asked to sign a bond, i.e. Bonded Personnel.
   b. This may not be a measure to improve physical security as such, but this can limit the financial exposure of the organisation, to a certain extent.
11) **Out of hours of Employees:**
   a. Employees who are out of office for a longer duration, during the office hours, should be monitored carefully.
   b. Their movements must be noted and reported to the concerned officials frequently.
12) **Secured Report/Document Distribution Cart:** Secured Carts / Trays, such as Mail Carts / Trays, must be covered and locked and should always be attended.

(11) What are the various kinds of Locks on Doors, in the context of Physical Access Control?

Kinds of Locks on Doors

(i) **Cipher locks (Combination Door Locks) -** Cipher locks are used in low security situations or when many entrances and exits must be usable all the time. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period, usually ten to thirty seconds.

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

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

(12) Write short notes on "Physical Identification Media", in the context of Physical Access Control.

Physical Identification Medium: These are discussed below: -

(i) **Personal Identification Numbers (PIN):** A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His/her entry will be matched with the PIN number available in the security database.

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

(iii) **Identification Badges:** Special identification badges can be issued to personnel as well as visitors. For easy identification purposes, their colour of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys.

(13) Write short notes on "Logging on Utilities", in the context of Physical Access Control.

Logging on Facilities: These are given as under: -

(i) **Manual Logging**: All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both fronts - reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

(ii) **Electronic Logging:** This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted.

(14) What are the various means of "Controlling Physical Access", in the context of Physical Access Control?

Other means of Controlling Physical Access: Other important means of controlling physical access are given as follows:

(i) **Video Cameras:** Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.

(ii) **Security Guards:** Extra security can be provided by appointing guards aided with CCTV feeds. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.

(iii) **Controlled Visitor Access:** A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

(iv) **Bonded Personnel:** All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organization.

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

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

(vii) **Computer Terminal Locks:** These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.

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

(ix) **Alarm System:** Illegal entry can be avoided by linking alarm system to inactive entry point and the reverse flows of enter or exit only doors, to avoid illegal entry. Security personnel should be able to hear the alarm when activated.

(x) **Perimeter Fencing:** Fencing at boundary of the facility may also enhance the security mechanism.

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

(xii) **Secured Report/Document Distribution Cart:** Secured carts, such as mail carts, must be covered and locked and should always be attended.

(15) Outline the various categories of issues arising in relation to Logical Access Control. The issues that may arise in relation to Logical Access Systems/ Controls are –

Technical Exposures	**Asynchronous Attacks**	**Computer Crime Exposures**
a) Data Diddling	a) Data Leakage	a) Financial Loss
b) Bombs	b) Wire–tapping	b) Legal battles
c) Trojan Horse	c) Piggybacking	c) Loss of credibility and competitive edge
d) Worms	d) Shutdown of Computer/ Denial of Service attack	d) Blackmail/ Industrial Espionage
e) Rounding down		e) Disclosure of confidential, sensitive or
f) Salami Techniques		f) embarrassing information
g) Trap Doors		g) Sabotage
h) Spoofing		

(16) Explain the various kinds of "Technical Exposures/Threats", in the context of Logical Access Control.

Technical Exposures include unauthorized implementation or modification of data and software. The following are the major technical exposures –

1. **Data Diddling:**
   a. Meaning: Data Diddling involves the change of data before, during or after it is entered into the system in order to delete, alter or add key system data.
   b. Risk: Data Diddling is of high risk, since it occurs before computer security can protect data.
   c. Low Expertise: Only a limited technical knowledge is required for data diddling.

2. **Bombs:**
   a. Meaning: Bomb is a piece of bad code in a program, deliberately planted by an insider or supplier of a program. Bombs cause a destructive process, e.g. disruption of computer system, modification of data, destruction of stored data, etc.
   b. Risk: The Bombs explode when the conditions of explosion get fulfilled, causing the damage immediately.

c. No infection: Generally, Bombs cannot infect other programs. Since Bombs do not circulate by infecting other programs, chances of a widespread epidemic are comparatively less.

3. **Trojan Horse:**
   a. Meaning: Trojan Horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. So, these are malicious unauthorised instructions / programs that are hidden under any authorized and properly functioning program. Trojan Horse is similar to Bombs, but a computer clock / particular circumstances do not necessarily activate it.
   b. Risk: A Trojan Horse may –
      - Change or steal the password, or
      - May modify records in protected files, or
      - May allow illicit users to use the systems.
4. **Worms:**
   a. Meaning: Worms are standalone programs, but hidden in a host program. They can be detected easily in comparison to Trojans and Computer Viruses.
   b. Risks:
      - Worms can help to sabotage systems.
      - A Worm actively transmits / copies itself directly to other systems on the network.
      - Worms do not usually live long, but they are destructive when they are alive.
5. **Rounding Down or Rounding off:**
   a. In this case, the computer rounds down all interest (or similar) calculations to small fractions of a denomination, and transfers all these small fractions in an account controlled by the perpetrator.
   b. It is difficult to detect because the rounding off is only a small fraction in each transaction.
6. **Salami Techniques:**
   a. This involves slicing of small amounts of money from a computerized transaction or account.
   b. Salami Technique is slightly different from a rounding technique in the sense only last few digits are rounded off here.
7. **Trap Doors:**
   a. Here, the perpetrator enters the system through a back door that bypasses normal system controls, and perpetrates a fraud.
   b. They exist out of an authorized program and allow insertion of specific logic, (e.g. program interrupts) that permit a review of data. They also permit insertion of unauthorized logic.
8. **Spoofing:**
   a. A Spoofing Attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique.
   b. A perpetrator duplicates the logon procedure, captures the user's password, attempts for a system crash and makes the user login again. The perpetrator makes the User think that he is interacting with the operating system. But it is only the second time the User actually logs into the system.
   c. Spoofing occurs only after a particular machine has been identified as vulnerable.

(17) Explain the various kinds of "Asynchronous Attacks", in the context of Logical Access Control.

Asynchronous Attack occur in many environments where data can be moved synchronously across telecommunication lines. 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 and are of following types:

(i) **Data Leakage:** This involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

(ii) **Subversive Attacks**: These can provide intruders with important information about messages being transmitted and the intruder may attempt to violate the integrity of some components in the sub-system.

(iii) **Wire- Tapping**: This involves spying on information being transmitted over communication network.

(iv) **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 the user and modifying them or substituting new messages.

(18) Logical Access violation can be done by many persons. Explain.

Logical Access Violators are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. They are mainly as follows:

(i) Hackers: Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally;

(ii) Employees (authorized or unauthorized);

(iii) IS Personnel: They have easiest to access to computerized information since they come across to information during discharging their duties. Segregation of duties and supervision help to reduce the logical access violations;

(iv) Former Employees: should be cautious of former employees who have left the organization on unfavourable terms;

(v) End Users; Interested or Educated Outsiders; Competitors; Foreigners; Organized Criminals; Crackers; Part-time and Temporary Personnel; Vendors and consultants; and Accidental Ignorant – Violation done unknowingly.

(19) Explain the Logical Access Control Measures under "User Access Management".

User Access Management: This is an important factor that involves following:

(i) **User Registration:** Information about every user is documented. Some questions like why and who is the user granted the access; has the data owner approved the access, and has the user accepted the responsibility? etc. are answered. The de-registration process is also equally important.

(ii) **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities and are to be minimal w.r.t their job functions. For example, an operator at the order counter shall have direct access to order processing activity of the application system.

(iii) **User password management:** Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password.

(iv) **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.

(20) Explain the Logical Access Control Measures under "User Responsibilities".

User Responsibilities: User awareness and responsibility are also important factors and are as follows:

(i) **Password use:** Mandatory use of strong passwords to maintain confidentiality.

(ii) **Unattended user equipment:** 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.

(21) Explain the Logical Access Control Measures under "Network Access".

Network Access Control: An Internet connection exposes an organization to the harmful elements of the outside world. The protection can be achieved through the following means:

(i) **Policy on use of network services:** 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.

(ii) **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.

(iii) **Segregation of networks:** 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

(iv) **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.

(v) **Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.

(vi) **Firewall:** A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall that will allow only authorized traffic between the organization and the outside to pass through it. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.

(vii) **Encryption:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm with a key to convert the original message called the Clear text into

Cipher text. This is decrypted at the receiving end. Two general approaches are used for encryption viz. private key and public key encryption.

(viii) **Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.

(22) Explain the Logical Access Control Measures under "Operating System Access".

Operating System Access Control: Operating System(O/S) is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Hence, protecting operating system access is extremely crucial and can be achieved using following steps:

(i) **Automated terminal identification:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.

(ii) **Terminal log-in procedures:** A log-in procedure is the first line of defense against unauthorized access as it does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users and accordingly authorizes the log-in.

(iii) **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.

(iv) **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or 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.

(v) **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.

(vi) **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

(vii) **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.

(viii) **Use of system utilities**: System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.

(ix) **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.

(x) **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.

(xi) **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time. For example, no computer access after 8.00 p.m. and before 8.00 a.m. or on a Saturday or Sunday.

(23) Explain the Logical Access Control Measures under "Application and Monitoring System Access".

Application and Monitoring System Access Control: Some steps are as follows:

(i) **Information Access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user can 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, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.

(ii) **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. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

(iii) **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

(iv) **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 extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.

(v) **Clock Synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

(24) What are the sub–systems under Management Controls?

Management Controls are adopted by the Management of an Enterprise are to ensure that the information systems function correctly and that they meet the strategic business objectives. Management Controls may be further analysed into the following sub–systems: -

Controls	**Scope: Controls in this area cover –**
(a) Top Management and Information Systems Management Controls	Top Management's role in planning. organizing. leading and controlling the IS Function. Role of Top Management in long–run policy decision–making and in translating long–run policies into short–run goals and objectives.
(b) System Development Management Controls	Contingency Perspective on models of the IS Development Process that Auditors can use as a basis for evidence collection and evaluation
(c) Programming Management Controls	Major Phases in the Program Development Life Cycle and the important controls that should be exercised in each phase.
(d) Data Administration / Resource Management Controls	Role of Database Administrator and the controls to be exercised in each phase.
(e) Quality Assurance Management Controls	Major functions that QA Management should perform to ensure that the development. implementation. operation. and maintenance of IS, conform to Quality Standards.
(f) Security Administration / Management Controls	Major Functions performed by Security Administrators to identify major threats to the IS functions, and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.
(g) Operations Management Controls	Major Functions performed by Operations Management to ensure the day–to–day operations of the IS function are well controlled.

(25) Explain the functions of Top Management and IS Management in the context of IS Controls.

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives. The scope of control here includes framing high-level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization. The major functions that a senior manager must perform are Planning, Organizing, Leading and Controlling.

(i) **Planning –** This includes determining the goals of the information systems function and the means of achieving these goals. The steering committee shall comprise of representatives from all areas of the business, and IT personnel that would be responsible for the overall direction of IT. The steering committee should assume overall responsibility for the activities of the information systems function.

(ii) **Organizing –** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.

(iii) **Leading –** This includes motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives; i.e. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.

(iv) **Controlling –** This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. This involves determining when the actual activities of the information system's functions deviate from the planned activities.

(26) What are the various activities performed under Systems Development Management Controls?

It includes controls at controlling new system development activities. The activities discussed below deal with system development controls in IT setup.

- Problem definition and Feasibility assessment:

  The feasibility assessment is done to obtain a commitment to change and to evaluate whether cost-effective solutions are available to address the problem or opportunity that has been identified.

  All the stakeholders must reach to agreement on the problem and should understand the possible threats associated with possible solutions/systems related to asset safeguarding, data integrity, system effectiveness, and system efficiency. All solutions must be properly and formally authorized to ensure their economic justification and feasibility.

- Analysis of existing system:

  Designers need to analyze the existing system that involves two major tasks:

  Studying the existing organizational history, structure, and culture to gain an understanding of the social and task systems in place, the ways these systems are coupled, and the willingness if stakeholders to change.

  Studying the existing product and information flows as the proposed system will be based primarily on current product and information flows. The designers need to understand the strengths and weaknesses of existing product to determine the new system requirements and the extent of change required.

- Information Processing System design:

  This phase involves following activities
  - Elicitation of detailed requirements: Either ask the stakeholders for their requirement in case they are aware about it or discover the requirement through analysis and experimentation in case stakeholders are uncertain about their need.
  - Design of data/information flow: The designers shall determine the flow of data/information and transformation points, the frequency and timing of the data and information flows and the extent to which data and information flows will be formalized. Tools such as DFD can be used for this purpose.
  - Design of Database and user interface: Design of database involves determining its scope and structure, whereas the design of user interface determines the ways in which users interact with a system.
  - Physical design: This involves breaking up the logical design into units which in turn can be decomposed further into implementation units such as programs and modules.
  - Design of the hardware/software platform: In case the hardware and software platforms are not available in the organization, the new platforms are required to be designed to support the proposed system.
- Hardware/Software acquisition and procedures development:

  To purchase the new application system or hardware, a request for a proposal must be prepared, vendor proposals are sought, and final decisions is made based on evaluation. During procedures development, designers specify the activities that users must undertake to support the ongoing operation of the system and to obtain useful output.
- Acceptance Testing and Conversion:

  Acceptance Testing is carried out to identify errors or deficiencies in the system prior to its final release into production use. The conversion phase comprises the activities undertaken to place the new system in operation.
- Operation and Maintenance:

  In this phase, the new system is run as a production system and periodically modified to better meet its objectives. A formal process is required to identify and record the need for changes to a system and to authorize and control the implementation of needed changes. The maintenance activities associated with these systems need to be approved and monitored carefully

(27) Proper IS Controls can be exercised during every stage of SDLC Process. Explain.

Program Development and Implementation Phase of SDLC aims to produce or acquire and to implement high–quality programs. The Program Development Life Cycle (PDLC) has six major phases with the following control aspects –

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

(28) Outline the scope and significance of Quality Assurance (QA) Management Controls.

Scope and significance of Quality Assurance (QA) Management Controls: -

(i) **Scope:** Quality Assurance Management is concerned with ensuring that the –

a. Information Systems produced by the IS Function achieve certain Quality Goals, and
b. Development, implementation, operation and maintenance of IS, comply with a set of Quality Standards.

(ii) **Importance:** The reasons for the emergence of QA in many organizations are as follows –

a. Organizations are producing many safety–critical systems, where quality is a important evaluation criteria.
b. Organizations are undertaking more ambitious projects when they build software.
c. Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work,
d. Organizations are becoming more concerned about their liabilities if they produce and sell defective software
e. Poor Quality Control over the production, implementation, operation, and maintenance of software can lead to problems of – missed deadlines, dissatisfied Users, lower morale among IS Staff, higher maintenance, and abandonment of many strategic projects.
f. Improving the quality of IS is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.

(29) Explain the functions performed under Operations Management Controls.

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as below:

(i) **Computer Operations:** The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available.

(ii) **Network Operations:** This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files. Data may be lost or corrupted through component failure.

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

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

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

(vi) **Documentation and Program Library:** This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to- date and that adequate backup exists for documentation. The documentation may include reporting of responsibility and authority of each function; Definition of responsibilities and objectives of each functions; Reporting responsibility and authority of each function; Policies and procedures; Job descriptions and Segregation of Duties.

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

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

(ix) **Management of Outsourced Operations:** This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

(30) What are the types of Application Controls? Briefly explain their Accounting and Operations Audit Trail?

Application Controls can be classified into the following categories-

Boundary Controls	**Input Controls**	**Communication Controls**	**Process Controls**	**Database Controls**	**Output Controls**
1. Cryptography 2. Passwords 3. PIN 4.Identification Cards 5.Biometric Devices	1. Source Document 2. Data Coding 3. Batch 4. Validation 5.Existence /Recovery	1.Physical Component Controls 2.Line Error Controls 3.Flow Controls 4.Link Controls 5.Topological Controls 6.Channel Access Controls 7. Controls over subversive threats 8.Internetworking Controls	1.Run–to–Run Totals 2.Reasonableness Verification 3.Edit Checks 4.Field Initialization 5.Exception Reports 6.Existence/ Recovery Controls	1.Update Controls 2.Report Controls	1.Storage & Logging of sensitive, critical forms 2. Logging of Output Program Executions 3.Spooling / Queueing Controls 4. Controls over Printing 5. Report Distribution and Collection Controls 6. Retention Controls 7. Existence / Recovery Controls

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill

statutory requirements, detect the consequences of error and allow system monitoring and tuning.

- 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.

(31) Explain the various Boundary Control Techniques.

Major Boundary Control are as follows:

- **Cryptography**
  - It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file.
  - A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst.
  - Three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).
- **Access Controls**

  These controls restrict the use of computer system resources to authorized users, limit the actions authorized users can take with these resources and ensure that users obtain only authentic computer system resources

  The access control mechanism involves three steps: Identification, Authentication and Authorization.

  - User's identification is done by user itself by providing his/her unique user id allotted to him/her or account number.
  - Authentication mechanism is used for proving the identity with the help of a password which may involve personal characteristics like name, birth date, employee code, designation or a combination of two or more of these. Biometric identification including thumb or finger impression, eye retina etc. and information stored in identification cards can also be used in an authentication process.
  - Authorization refers to the set of actions allowed to a user once authentication is done successfully. For example – Read, Write, Print, etc. permissions allowed to an individual user.
- **Personal Identification Numbers**

  PIN is like a password assigned to a user by an institution, a random number stored in its database independent to a user identification details.

A PIN may be exposed to vulnerabilities at any stage of the life cycle of PIN and therefore, controls need to be put in place and working to reduce exposures to an acceptable level.

Several phases of the life cycle of PINs include the steps that are

- Generation of the PIN
- Issuance and delivery of PIN to users
- Validation of the PIN upon entry at the terminal device
- Transmission of the PIN across communication lines
- Processing of the PIN
- Storage of the PIN
- Change of PIN
- Replacement of PIN
- Termination of PIN

- **Digital Signature**

  Establishing the authenticity of persons and preventing the denial of message or contracts are critical requirements when data is exchanged in electronic form. A counterpart known as Digital Signature (a string of 0's and 1's) is used as an analog signature for such e-documents. Digital Signatures are not constant like analog signatures – they vary across messages and cannot be forged.

- **Plastic Cards**

  Plastic cards are used primarily for identification purpose. This includes the phases namely - application for a card, preparation of the card, issue of the card, use of the card and card return or card termination.

(32) Write short notes on Input Controls

Input control:

- Input Controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system, sometimes using data codes.
- Input Controls are important since substantial time is spent on input of data, involve human intervention and are therefore prone to error and fraud.
- Input Controls include Existence/Recovery Controls, since it might be necessary to re–process input data in case the Master Files are lost, corrupted, or destroyed.
- Source Documents or Transaction Listings are generally stored securely for longer periods for reasons like statutory requirements, change verification, audit trail, etc.
- Input Controls are further classified into – (a) Source Document Control, (b) Data Coding Controls, (c) Batch Controls, and (d) Validation Controls.

(33) Explain the concept of Source Document Controls, in the context of Input Controls.

Source Document Controls: Frauds with respect to Source Documents include data entry of fictitious transactions, as well as non–recording of certain transactions. Some Controls with respect to Source Documents are –

- **Pre–Numbered Documents:** Source Documents should be pre–numbered from the printer with a unique sequential number on each document. This enables accurate accounting of document usage and provides an audit trail for tracing transactions through accounting records.
- **Sequential Use of Documents:** Source Documents should be distributed to the Users and used in sequence. There should be adequate physical security / restricted access over the source document inventory at the User site.
- **Periodical Audit:** Missing source documents should be identified by reconciling document sequence numbers, i.e. Printed less Cancelled less Used = Inventory of Documents. Documents not accounted for, cancelled but not available for audit, etc. should be reported to Management.

(34) Explain the concept of Data Coding Controls, in the context of Input Controls.

Data Coding Controls: Two types of errors - Transcription and Transposition errors can corrupt a data code and cause processing errors. Any of these errors can cause serious problems in data processing if they go undetected. These simple errors can severely disrupt operations.

- **Transcription Errors:** It is a special type of data entry error that is commonly made by human operators or by Optical Character Recognition (OCR) programs. Like Addition errors (when an extra digit is added to the code); Truncation Errors (when a digit is removed from the code) and Substitution Errors (replacement of on digit in a code with another).
- **Transposition Errors:** It is a simple error of data entry that occur when two digits that are either individual or part of larger sequence of numbers are reversed (Transpose) when posting a transaction. For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed.

(35) Explain the concept of Batch Controls, in the context of Input Controls.

Batch Controls: Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercises over the batch to prevent or detect errors or irregularities. To identify errors or irregularities in either a physical or logical batch, three types of control totals are as follows:

- **Financial totals:** Grand totals calculated for each field containing money amounts.
- **Hash totals:** Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totalled.
- **Document/Record Counts:** Grand totals for number of documents in record in batch.

(36) Explain the concept of Validation Controls, in the context of Input Controls.

Validation Controls: Input validation controls are intended to detect errors in the transaction data before the data are processed. Some of these controls include the following:

- Field interrogation: It involves programmed procedures that examine the characters of the data in the field. This includes the checks like Limit Check (against predefined

limits), Picture Checks (against entry into processing of incorrect/invalid characters), valid check codes (against predetermined transactions codes, tables) etc.

- Record interrogation: This includes the reasonableness check (Whether the value specified in a field is reasonable for that particular field?); Valid Sign (to determine which sign is valid for a numeric field) and Sequence Check (to follow a required order matching with logical records.)
- File Interrogation: This includes version usage; internal and external labelling; data file security; file updating and maintenance authorization etc.

(37) Explain the controls to mitigate the exposure in the Communication sub–system.

Some communication controls are as follows:

- Physical Component Controls

The physical components shall have characteristics that make them reliable and incorporate features and controls that mitigate the possible effects of exposures. Major physical components that affect the reliability of communication subsystem are Transmission media, Communication lines, Modem, Port protection devices, Multiplexers, and Concentrators etc.

- Line Error Control

Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

- *Flow Controls*

Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data. For example, a main frame can transmit data to a microcomputer terminal.

- *Topological Controls*

Communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes. The network must be available for use at any one time by a given number of users that may require alternative hardware, software, or routing of messages.

- *Link Controls*

In Wide Area Network (WAN), line error control and flow control are important functions in the component that manages the link between two nodes in a network.

- *Channel Access Controls:*

Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used.

Therefore, some type of channel access control techniques like polling method (defining an order in which a node can gain access to a channel capacity) or

contention method (nodes in network must compete with each other to gain access to a channel) must be used.

- *Controls over Subversive threats:*

  Firstly, the physical barriers are needed to be established to the data traversing into the subsystem. Secondly, in case the intruder has somehow gained access to the data, the data needs to be rendered useless when access occurs.

- *Internetworking Controls:*

  Different internetworking devices like bridge, router, gateways are used to establish connectivity between homogeneous or heterogeneous networks. Therefore, several control functions in terms of access control mechanisms, security and reliability of the networks are required to be established.

(38) Write short notes on Processing Controls.

Processing Controls: The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are the Central Processor in which programs are executed, the real or virtual memory in which program instructions and data are stored, the operating system that manages system resources, and the application programs that execute instructions to achieve specific user requirements. Some of these controls are as follows:

(i) **Central Processor Controls:** Some Controls to reduce expected losses from errors and irregularities associated with Central Processors are –

Control	Explanation
Error Detection and Correction	(a) Processors may malfunction due to design errors, manufacturing defects, damage, electromagnetic interference, and ionizing radiation. (b) Various types of Error Detection and Correction Strategies must be used.
Multiple Execution States	(a) Determination of number and nature of the execution states enforced by the Processor is very critical for the auditors. (b) They help to determine unauthorized activities, such as gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes, etc.
Timing Controls	An Operating System might get stuck in an infinite loop. In the absence of any control, the program will not allow the Processor to function and prevent other programs from performing.
Component Replication	Failure of Processor can result in significant losses. Redundant Processors allow errors to be detected and corrected. If Processor Failure is permanent in multicomputer or multiprocessor architectures, the system might re–configure itself to isolate the failed processor.

(ii) **Real Memory Controls:**

a. It comprises of fixed amount of primary storage in which programs or data must reside to carry out the Instructions from the Central Processor.
b. It also tries to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

(iii) **Virtual Memory Controls:**

a. Virtual Memory exists when the addressable storage space is larger than that of the available Real Memory Space.
b. To achieve this outcome, a Control Mechanism is used to map Virtual Memory Addresses into Real Memory Addresses

(iv) **Data Processing Controls:**

a. These perform validation checks to identify errors during processing of data.
b. They are required to ensure both the completeness and the accuracy of data being processed.
c. Normally, the processing controls are enforced through database management system that stores the data.

(39) Explain the concept of Update Controls and report controls, in the context of Database Controls.

Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called Update Controls and Report Controls

Control	Explanation
(a) Access Controls	These controls in database subsystem seek to prevent unauthorized access to and use of the data.
(b) Integrity Controls	These are required to ensure that the accuracy, completeness, and uniqueness of instances used within the data or conceptual modeling are maintained.
(c) Application Software Controls	DBMS depends on application software to pass across a correct sequence of commands and update parameters so that appropriate actions can be taken when certain types of exception condition arise. This is achieved through Update Controls that ensure that changes to the database reflect changes to the real-world entities and associations between entities that data in the database is supposed to represent and Report Controls that identify errors or irregularities that may have occurred when the database has been updated.

(d) Concurrency Control	These are required to address the situation that arises either due to simultaneous access to the same database or due to deadlock.
(e) Cryptographic Control	These controls can be well used for protecting the integrity of data stored in the database using block encryption.
(f) File Handling Control	Used to prevent accidental destruction of data contained on a storage medium. These are exercised by hardware, software, and the operators or users who load/unload storage media.

(40) What are the different types of Output Control Techniques?

Output can be in any form, it can either be a printed data report or a database file in a removable media.

Control	Explanation
(a) Inference Controls	These are used to prevent compromise of statistical databases from which users can obtain only aggregate statistics rather than the values of individual data items
(b) Batch Output Production and Distribution Controls	It includes several controls like • Report program execution Controls to ensure that only authorized users are permitted to execute batch report programs and these events are logged and monitored • Spooling file Controls so that the user(s) can continue working while a queue of documents waiting to be printed on a particular printer to ensure that the waiting files to get printed shall not be subject to unauthorized modifications • Printing Controls to ensure that output is made on the correct printer, and unauthorized disclosure of printed information does not take place • Report collection Controls to ensure that report is collected immediately and secured to avoid unauthorized disclosure and data leakage

	• User/Client service Review Controls to ensure user should obtain higher quality output and detection of errors or irregularities in output • Report distribution Controls ensuring that the time gap between generation and distribution of reports is reduced, and a log is maintained for reports that were generated and to whom these were distributed • User output Controls to be in place to ensure that users review output on a timely basis • Storage Controls to ensure proper perseverance of output in an ideal environment, secured storage of output and appropriate inventory controls over the stored output • Retention and Destruction Controls in terms of deciding the time duration for which the output shall be retained and then destroyed when not required.
(c) Batch Report Design Controls:	Batch report design features should comply with the control procedures laid down for them during the output process. The information incorporated in a well-designed batch report shall facilitate its flow though the output process and execution of controls.
(d) Online output production and Distribution Controls	It deals with the controls to be considered at various phases as follows • Source controls ensure that output which can be generated or accessed online is authorized, complete and timely • Distribution Controls to prevent unauthorized copying of online output when it was distributed to a terminal • Communication Controls to reduce exposures from attacks during transmission • Receipt Controls to evaluate whether the output should be accepted or rejected • Review Controls to ensure timely action of intended recipients on the output • Disposition Controls to educate employees the actions that can be taken on the online output they receive • Retention Controls to evaluate for how long the output is to be retained and Deletion Controls to delete the output once expired.

Ch:3(c) Information Systems – Audit

(1) What are the objectives of IS Audit?

IS Auditing is defined as the process of attesting objectives that focus on asset safeguarding, data integrity and management objectives that include effectiveness and efficiency both. This enables organizations to better achieve four major objectives that are as follows:

(i) **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.

(ii) **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organization requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.

(iii) **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.

(iv) **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

(2) Write short notes on Audit Trails.

Audit trails: Audit Trails refers to the Logs that are designed to record activities at the System, Application and User levels. When properly implemented, Audit Trails provide an important detective control to help in accomplishing security policy objectives. Audit Trails serves 3 main purposes–

a. to detect unauthorized access to the system,
b. to facilitate the reconstruction of events, and
c. promote personal accountability.

Contents of Log: The Audit Trail / Log should contain –

a. specific events,
b. important activities, and
c. other relevant and important information perceived by the management for effective control.

Types: Audit Trail may be of two types –

a. Accounting Audit Trail – to show the source and nature of data and processes that update the database.
b. Operations Audit Trail – to maintain a record of attempted or actual resource consumption within a system.

(3) What are the Security Objectives of Audit Trails?

Audit Trails serve as a control tool and helps to achieve security policy objectives in the following ways –

1. Detecting Unauthorised Access:

a) Unauthorized Access can be detected on–line or after such access has been made.

b) On–line detection protects the system from outsiders trying to break system controls. A Real–time audit trail reports changes in system performance caused by infection of a Virus or Worm. But, such real–time detection involves a significant amount of cost, and can also reduce operational performance and speed.
c) After–the–fact detection logs are stored electronically and reviewed periodically. They are used to determine whether the unauthorised access was successful, or was only a failed attempt.

2. Reconstructing Events:

a) Audit Trail helps to reconstruct events that led to system failures, security violations or application processing errors, by means of an Audit Analysis.
b) Audit Analysis identifies and analyses the conditions that caused system failure. For example, by maintaining a record of all the changes to account balances, the Audit Trail can be used to reconstruct accounting data files that were corrupted by system failure. The knowledge of such conditions helps to assign responsibility and avoid future recurrence.

3. Personal Accountability:

a) Audit Trails monitor user activity even at the lowest level. This serves as a preventive control.
b) Individuals are afraid of social stigma and hence hesitate to violate security policy if they know that their actions are recorded in an audit log. This minimizes security violations.

(4) Write short notes on Integrated Test Facility (ITF) Technique.

The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.

- A small set of fictitious records is placed in the master files. The records may be a fictitious division, department or branch office or a customer or a supplier.
- Processing test transactions to update these dummy records will not affect the actual records.
- As fictitious & actual records are processed together, the Company employees are unaware of this testing.
- The system application must distinguish ITF records from actual records, collect information on the effects of the test transactions, and report the results.
- The IS Auditor compares the processing and expected results to verify the correctness of systems operations.
- In a Batch Processing System, this technique eliminates the need to reverse test transactions. It is also easily concealed from employees operating with the system.

(5) Write short notes on Snapshot Technique.

Tracing a transaction in a computerized system can be performed, with the help of Snapshots or extended records. The Snapshot Software is built into the system at those points where material processing occurs, which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to be considered while using snapshots are –

(a) to locate the snapshot points based on materiality of transactions,

(b) to determine when the snapshot will be captured, and
(c) to ensure that the reporting system design and implementation leads to presentation of data in a meaningful way.

(6) Write short notes on System Control Audit Review File (SCARF) Technique?

System Control Audit Review File (SCARF) Technique:

- SCARF uses embedded audit modules within the host application system to monitor transaction activity continuously and collect data on transactions of special audit significance.
- The data collected is recorded in a SCARF Master File or Audit Log.
- SCARF File records transactions like the following – transactions exceeding a specified rupee limit, involving inactive accounts, deviating from Company policy, or containing write–downs of asset values.
- The Auditor receives a periodic printout of the SCARF File, examines the information to identify questionable transactions, and performs necessary follow–up investigation.

(7) Write short notes on Continuous and Intermittent Simulation (CIS) Technique.

Continuous and Intermittent Simulation (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:

- The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- CIS replicates or simulates the application system processing.
- Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written to an exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

(8) Write short notes on Audit Hooks Technique.

Audit Hooks: Audit Hooks are audit routines that flag or mark suspicious transactions.

- When audit hooks are employed, the Auditors are informed of questionable transactions immediately on their occurrence by displaying a message on the Auditor's terminal. This immediate notification is called real–time notification.
- Example: The Internal Auditor of a Bank, envisaged that Pensioners' Accounts, where the pension is directly credited to the pensioner's account, is vulnerable to fraud, unless a Life Certificate is obtained each year from the individual concerned. They devised a system of Audit Hooks to tag records where Life Certificate was not obtained. The Internal Audit Department will be notified / informed when a transaction takes place in a tagged record. The Audit Department can take steps to investigate fraud, if any.

(9) Explain the Role and Duties of the IS Auditor in the Audit of Managerial Controls.

Role and Duties of the IS Auditor in the Audit of Managerial Controls:

1) Top Management and Info. Systems Management Controls: The role of Auditor at each activity is as under –

Activity	Role of auditors
(a) Planning	• To evaluate whether or not Top Management has formulated a high–quality Information Systems plan that is appropriate to the needs of an organization. • To see whether strategic and operational plans are linked properly, plans are reviewed, etc.
(b) Organizing	• To examine the effectiveness of the IS function based on the quality of IS Staff, i.e. whether they are up to date and motivated in their jobs. • To see how efficiently the Entity has handled the complex activity of acquiring and retaining good IS Staff, in an environment of intense competition and high turnover. • To see whether Employees of the Entity, are likely persons to perpetrate irregularities.
(c) Leading	• To find variables that indicate when motivation problems exist or suggest poor leadership, e.g. Staff Turnover, frequent failure of projects to meet their budget and absenteeism levels. • To evaluate how well Top Managers' communicate with their Staff, using both formal and informal sources of evidence. • To assess both the short–run and long–run consequences of poor communications within the IS Function and to assess the implications for asset safeguarding, data integrity, system effectiveness, and system efficiency.
(d) Controlling	• To evaluate whether Top Management's choice to the means of control over the Users of IS Services is likely to be effective or not. • To evaluate controls in ensuring that the IS Function meets its objectives at a global level

2) Systems Development Management Controls: Three different types of audits may be conducted during System Development Process as under –

Type	Role of Auditors
(a) Concurrent Audit	• As Members of the System Development Team, Auditors assist the Team in improving the quality of Systems Development for the specific system they are building and implementing.
(b) Post – Implementation Audit	• Auditors help an Entity learn from its experiences in the development of a specific application system. Auditors also help in evaluating whether the system needs to be

	scrapped, continued, or modified in some manner.
(c) General Audit	• Auditors evaluate Systems Development Controls overall, to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about Management's Assertions relating to the Financial Statements for systems effectiveness and efficiency.

3) Programming Management Controls: In Programming Management Controls, the role of Auditors is as under –

Phase	**Audit Trails / Role of Auditors**
(a) Planning	• To evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. • To examine and evaluate how well the planning work is being undertaken.
(b) Design	• To find out whether Programmers use some type of systematic approach to design. • To obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
(c) Control	• To evaluate whether the nature of and extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. • To obtain evidence on whether the control procedures are operating reliably, e.g. by choosing a sample of past and current software development and acquisition projects carried out at different locations in the Entity.
(d) Coding	• To evaluate the level of care exercised by Programming Management in choosing a Module Implementation and Integration Strategy. • To determine whether Programming Management ensures that Programmers follow structured programming conventions. • To check whether Programmers use automated facilities to assist them in their coding work.
(e) Testing	• To evaluate how well Unit Testing is conducted, by using Interviews, Observations, and examination of documentation. • To evaluate the quality of Integration Testing work carried out by IS Professionals.

	• To see that Whole–of–Program Tests have been undertaken for all material programs and that these tests have been well–designed and executed.
(f) Operation and Maintenance	• To ensure timely reporting of maintenance needs occurs and maintenance is carried out in a well–controlled manner. • To see if Management has implemented a review system and assigned responsibility for monitoring the status of Operational Programs.

4) Data Resource Management Controls: The Auditors' Role include the following –

(a) To determine what controls are exercised to maintain data integrity.
(b) To interview Database Users to determine their level of awareness of these controls.
(c) To employ test data to evaluate whether Access Controls and Update Controls are working.

5) Quality Assurance Management Controls: Using Interviews, Observations, and Reviews of Documentation, IS Auditors can evaluate the following –

(a) To evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
(b) To evaluate how well QA Personnel, make recommendations for improved standards or processes.
(c) To evaluate how well QA Personnel, undertake the reporting function and training.

6) Security Management Controls: The Auditors' Role include the following –

(a) To evaluate whether or not Security Administrators are conducting ongoing, high–quality security reviews,
(b) To check whether or not the Entity has an appropriate, high–quality Disaster Recovery Plan in place, and
(c) To check whether or not the Entity have opted for an appropriate Insurance Plan.

7) Operations Management Controls: Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to Authorized Personnel. Auditors can use interviews, observations, and review of documentation to evaluate –

(a) the activities of Documentation Librarians,
(b) how well Operations Management undertakes the Capacity Planning and Performance Monitoring function,
(c) the reliability of Outsourcing Vendor Controls,
(d) whether Operations Management is monitoring compliance with the outsourcing contract, and
(e) whether Operations Management regularly assesses the financial viability of any Outsourcing Vendors

(10) Explain the Role and Duties of the IS Auditor in the Audit of Application Controls.

Role and Duties of the IS Auditor in the Audit of Application Controls: -

Audit Trail Controls: Two types of audit trails that should exist in each subsystem are as follows:

- An Accounting Audit Trail to maintain a record of events within the subsystem; and
- An Operations Audit Trail to maintain a record of the resource consumption associated with each event in the subsystem.

1) Boundary Controls: This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. This includes the following:

- Identity of the would-be user of the system;
- Authentication information supplied;
- Resources requested;
- Action privileges requested;
- Terminal Identifier;

1. Accounting Audit Trail

☐ Action privileges allowed/denied.

2. Operations Audit Trail

☐ Resource usage from log-on to log-out time.

☐ Log of Resource consumption.

2) Input Controls: This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.

1. Accounting Audit Trail

- The identity of the person(organization) who was the source of the data;
- The identity of the person(organization) who entered the data into the system;
- The time and date when the data was captured;
- The identifier of the physical device used to enter the data into the system;

2. Operations Audit Trail

- Time to key in a source document or an instrument at a terminal;
- Number of read errors made by an optical scanning device;
- Number of keying errors identified during verification;
- Frequency with which an instruction in a command language is used;

3) **Communication Controls:** This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

1. **Accounting Audit Trail**
   - Unique identifier of the source/sink node;
   - Unique identifier of each node in the network that traverses the message; Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched;
   - Time and date at which the message was received by the sink node;
   - Time and date at which node in the network was traversed by the message.
2. **Operations Audit Trail**
   - Number of messages that have traversed each link and each node;
   - Queue lengths at each node; Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors;
   - Log of system restarts; and
   - Message transit times between nodes and at nodes.

4) **Processing Controls:** The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

1. **Accounting Audit Trail**
   - To trace and replicate the processing performed on a data item.
   - To follow triggered transactions from end to end by monitoring input data entry, intermediate results and output data values.
   - To check for existence of any data flow diagrams or flowcharts that describe data flow in the transaction, and whether such diagrams or flowcharts correctly identify the flow of data.
   - To check whether audit log entries recorded the changes made in the data items at any time including who made them.
2. **Operations Audit Trail**
   - A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.
   - A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

5) **Database Controls:** The audit trail maintains the chronology of events that occur either to the database definition or the database itself.

1. **Accounting Audit Trail**
   - To confirm whether an application properly accepts, processes, and stores information.

- To attach a unique time stamp to all transactions.
- To attach before-images and after-images of the data item on which a transaction is applied to the audit trail.
- Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.
- To not only test the stated input, calculation, and output rules for data integrity, but also should assess the efficacy of the rules themselves.

2. Operations Audit Trail

- To maintain a chronology of resource consumption events that affects the database definition or the database.

6) Output Controls: The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.

1. Accounting Audit Trail

- What output was presented to users;
- Who received the output;
- When the output was received; and
- What actions were taken with the output?

2. Operations Audit Trail

- To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

(11) Explain the Role and Duties of the IS Auditor in the Audit of Environmental Controls.

Auditing environmental controls requires attention to these and other factors and activities, including:

(i) **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, line conditioners, surge protectors, or motor generators, are used, inspected and maintained and if this is performed by qualified personnel.

(ii) **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. S/he should examine maintenance records to see how frequently these components are maintained and if this is done by qualified personnel.

(iii) **Heating, Ventilation, and Air Conditioning (HVAC):** The IS auditor should determine if HVAC systems are providing adequate temperature and humidity levels, and if they are monitored. Also, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.

(iv) **Water detection:** The IS auditor should determine if any water detectors are used in rooms where computers are used. He or she should determine how frequently these are tested and if they are monitored.

(v) **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if they are tested. He or she should determine how frequently fire suppression systems are inspected and tested, and if the organization has emergency evacuation plans and conducts fire drills.

(vi) **Cleanliness:** The IS auditor should examine data centres to see how clean they are. IT equipment air filters and the inside of some IT components should be examined to see if there is an accumulation of dust and dirt.

(12) Explain the Role and Duties of the IS Auditor in the Audit of Physical Access Controls.

Role of IS Auditor in Auditing Physical Access Controls: Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

(13) Explain the Role and Duties of the IS Auditor in the Audit of Logical Access Controls.

Auditing Logical Access Controls requires attention to several key areas that include the following:

- **Network Access Paths:** The IS auditor should conduct an independent review of the IT infrastructure to map out the organization's logical access paths. This will require considerable effort and may require the use of investigative and technical tools, as well as specialized experts on IT network architecture.
- **Documentation:** The IS auditor should request network architecture and access documentation to compare what was discovered independently against existing documentation. Similar investigations should take place for each application to determine all of the documented and undocumented access paths to functions and data.

(14) What are the benefits of big data process?

Benefits of Big Data Processing are as follows:

- **Ability to process Big Data brings in multiple benefits, such as-**
  - Businesses can utilize outside intelligence while taking decisions.
  - Access to social data from search engines and sites like Facebook, Twitter are enabling organizations to fine tune their business strategies.
  - Early identification of risk to the product/services, if any

- **Improved customer service**
  - Traditional customer feedback systems are getting replaced by new systems designed with Big Data technologies. In these new systems, Big Data and natural language processing technologies are being used to read and evaluate consumer responses.
- **Better operational efficiency**
  - Integration of Big Data technologies and data warehouse helps an organization to offload infrequently accessed data, this leading to better operational efficiency.

Ch 4(a) E–Commerce and M–Commerce

1. **Write short notes on the concept of E–Commerce.**
   E-Commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of Business-To-Business (B2B) and Business-To-Consumer (B2C) transactions through reliable and secure connections. E–Commerce is a sophisticated combination of technologies and consumer–based services integrated to form a new paradigm in business transaction processing. . Transaction Flow in E–Commerce: (a) Order, (b) Authorisation Request, (c) Authorisation Response, (d) Product Dispatch, (e) Settlement Request, and (f) Settlement Deposit. [**Note:** Sometimes, payment is made before dispatch.]

2. ***What are the benefits of E–Commerce?***

Benefits of E-Business

E-business benefits individuals, businesses, government and society at large. The major benefits from e-business are as follows:

Benefits to Customer / Individual / User

- **Convenience:** Every product at the tip of individual's fingertips on internet.
- **Time saving:** No. of operations that can be performed both by potential buyers and sellers increase.
- **Various Options:** There are several options available for customers which are not only being easy to compare but are provided by different players in the market.
- **Easy to find reviews:** There are often reviews about a particular site or product from the previous customers which provides valuable feedback

Benefits to Business / Sellers

- **Increased Customer Base:** Since the number of people getting online is increasing, which are creating not only new customers but also retaining the old ones.
- **Instant Transaction:** The transactions of e commerce are based on real time processes. This has made possible to crack number of deals.
- **Easier entry into new markets:** This is especially into geographically remote markets, for enterprises regardless of size and location.
- **Better quality of goods:** As standardized specifications and competition have increased and improved variety of goods through expanded markets and the ability to produce customized goods.

Benefits to Government

- Instrument to fight corruption: -In line with Government's vision, e commerce provides a pivotal hand to fight corruption.
- Reduction in use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects).

3. Differentiate between Traditional Commerce and E–Commerce.

Difference between Traditional Commerce and E-Commerce are as follows: -

BASE FOR COMPARISON	TRADITIONAL COMMERCE	E-COMMERCE
Definition	Traditional commerce includes all those activities which encourage exchange, in some way or the other of goods / services which are manual and non-electronic.	E-Commerce means carrying out commercial transactions or exchange of information, electronically on the internet.
Transaction Processing	Manual	Electronically
Availability for commercial transactions	For limited time. This time may be defined by law. Like special stores which may run 24 hours, but in general available for limited time.	24×7×365
Customer interaction	Face-to-face	Screen-to-face
Business Scope	Limited to particular area.	Worldwide reach
Information exchange	No uniform platform for exchange of information.	Provides a uniform platform for information exchange.
Nature of purchase	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
Payment	Cash, cheque, credit card, etc.	Credit card, fund transfer, Cash in Delivery, Payment Wallets, UPCI application etc.

4. Write short notes on the concept of M–Commerce.

M-Commerce is the buying and selling of goods and services through wireless handheld devices such as Mobile Telephone and Personal Digital Assistants (PDAs). Mobile Commerce deals about the explosion of applications and, services that are becoming accessible from Internet–enabled mobile devices. It is also known as next–generation e–commerce. It enables Users to access the Internet without needing to find a place to plug in. The key growth in the mobile e-Commerce sector in recent years has been in through so-called Apps. Apps, short for Mobile Applications, are small piece of software developed specifically for the operating systems of handheld devices such as mobile

phones, PDAs and Tablet computers. Mobile Apps can come preloaded on handheld devices or can be downloaded by users from the app stores over the Internet.

5. What are the components of E–Commerce?
The major components of E–Commerce are as under: -

Point	Description
User	User is the Consumer / Buyer, i.e. any Individual / Entity using the e–Commerce platform / mechanism.
Vendors	E–Commerce Vendor refers to the Entity that provides the required goods and services to the User. Example: Flipkart, Amazon, etc.
Technology	Technology Infrastructure refers to the Computers, Servers, Database, Mobile Apps, Digital Libraries, Data Interchange, etc. enabling the e–commerce transactions.
Internet / Network	Faster Net Connectivity contributes significantly to the success of e–Commerce trade of an Entity. Net Connectivity can be through traditional as well as new technology.
Web Portal	◆ Web Portal provides the Application Interface through which the User interacts with the Vendor to perform the e–commerce transactions. ◆ Web Portals can be accessed through Desktops / Laptops / PDA / Mobiles / Smart TVs, etc. ◆ The simplicity and clarity of content on the Web Portal leads to better customer experience of buying a product online.
Payment Gateway	◆ Payment Gateway represents the manner through which the Customer makes payment to the e– Commerce Vendors. ◆ Payment Gateway is a critical component of e–commerce set–up, which assures the Seller, of the receipt of money from the Buyer of goods / services. ◆ Payment Methods include Credit / Debit Card Payments, Online Bank Payments, Payment Wallet of ◆ Vendor / Third Party, Cash on Delivery (COD), Unified Payments Interface (UPI), etc.

6. Explain the role of E–Commerce Vendors in promoting e–Commerce/ e–Business.
Role of E–Commerce Vendors in promoting e–Commerce/ e–Business: E-commerce vendors needs to ensure following for better, effective and efficient transaction.

a. **Suppliers and Supply Chain Management:** These being another important component of the whole operations. For effectiveness, they need to ensure that -

i. They have enough and the right goods suppliers.
ii. They (suppliers) are financially and operationally safe.
iii. Suppliers are able to provide real-time stock inventory.
iv. The order to deliver time is very short.

b. **Warehouse operations:** When a product is bought, it is delivered from the warehouse of e-commerce vendor. This place is where online retailers pick products from the shelf, pack them as per customer's specification / pre-decided standards and prepare those products to be delivered. These operations have become very critical to the success of the whole e- commerce business. Many e-commerce companies are investing huge amounts of money in automating the whole warehouses.

c. **Shipping and returns:** Shipping is supplementary and complementary to whole warehouse operations. Fast returns have become Unique Selling Preposition (USP) for many e-commerce vendors, so these vendors need very effective and efficient return processing.

d. **E-Commerce catalogue and product display:** Proper display of all products being sold by vendor including product details, technical specifications, makes for a better sales conversion ratio. These help customers gauge the products/services being sold. A good catalogue makes a lot of difference to whole customer experience.

7. What are the items covered in the Technology Infrastructure in E–Commerce?
Technology Infrastructure in E–Commerce comprises the following: –

Point	Description
Computers, Servers and Database	• These are the backbone for the success of the venture. Big e- commerce organization invest huge amount of money/time in creating these systems. They store the data / program used to run the whole operation of the organization. • As cloud computing is increasingly being used, many small / mid- sized e-commerce originations have started using shared infrastructures.
Mobile Apps	• Mobile Devices (Tablet Computers, Smart Phones, etc.) have Operating Systems and Application Software, and can be used to perform online transactions. • Mobile Devices may operate on many Operating Systems like Android, iOS, BlackBerry OS, Windows Mobile, etc.
Digital Library	• A Digital Library is a special library with a focused collection of digital objects. • Digital Library can store text, visual material, audio material, video material, in electronic media formats, along with means for organizing, storing, and retrieving the files and media contained in the library collection.

Data Interchange	• Data Interchange is an electronic communication of data. • For ensuring the correctness of data interchange between different parties in e–commerce, (viz. User, Vendor, Payment Gateway, Bank, etc.) business–specific protocols are being used.

8. Briefly describe the workflow in E–Commerce.

The workflow in E–Commerce: -

Step	Activities
Customers login	Few e-commerce merchants may allow same transactions to be done through phone, but the basic information flow is e- mode.
Product / Service Selection	Customer selects products / services from available options
Customer Places Order	Order is placed for selected product / service by customer. This step leads to next important activity PAYMENT GATEWAY.
Payment Gateway	Here customer makes a selection of the payment method. In case payment methods is other than cash on delivery (COD), the merchant gets the update from payment gateway about payment realization from customer. In case of COD, e- commerce vendor may do an additional check to validate customer.
Dispatch and Shipping Process	This process may be executed at two different ends. First if product / service inventory is managed by e-commerce vendor, then dispatch shall be initiated at merchant warehouse. Second, many e-commerce merchants allow third party vendors to sale through merchant websites. For example: FLIPKART states that it has more than 1 lac registered third party vendors on its website.
Delivery Tracking	Another key element denoting success of e-commerce business is timely delivery. Merchants keep a track of this. All merchants have provided their delivery staff with hand held devices, where the product / service delivery to customers are immediately updated.
COD tracking	In case products are sold on COD payment mode, merchants need to have additional check on matching delivery with payments.

9. What are the Policy Areas to be defined in E–Commerce?

Policy areas to be defined in E-commerce: -

Area	Description
Billing	• Process of Billing, • Format of Bill, details to be provided in the Bill, treatment of applicable Indirect Taxes (GST), etc
Product guarantee / warranty	• Proper display of product guarantee / warranty online as well as documents sent along with the products.

Shipping	• Shipping Time, • Place of Shipping • Frequency of Shipping • Mode of Shipping • Packing at the time of Shipping, etc.
Delivery	Policy needs to be defined for: • Which mode of delivery to be chosen? • When deliveries to be made? • Where deliveries to be made?
Return	Policy for return of goods need to be put in place defining: • Which goods to be accepted in return? • The number of days within which returns can be accepted • The process of verifying the authenticity of products received back. • The time within which buyer shall be paid his/her amount back for goods returned.
Payment	Policy guidelines need to be created for the following payment related issues: • Mode of payment. • For which products, specific payment mode shall be there. Organization restricts cash on delivery for few consumable products.

10. Explain the terms – (1) Network Architecture, and (2) Client Server Technology.

Network Architecture: Network Architecture refers to the layout of Network, of – (i) Hardware, (ii) Software, (iii) Connectivity, (iv) Communication Protocols, and (v) Mode of Transmission. Network Architecture Diagram provides a full picture of the established network with detailed view of all the resources accessible.

Client Server Technology: Client / Server (C/S) technology refers to computing technologies in which the hardware and software components (i.e. Clients and Servers) are distributed through the Network.

11. Explain the terms – (1) Single Tier Architecture, (2) Two Tier Architecture, (3) Three Tier Architecture.

Single Tier Architecture: A single computer that contains a Database and a front–end Interface (GUI) to access the Database is known as Single Tier System. All components required for a Software Application or Technology is put on a Single Server or Platform.

Two Tier Architecture: In a Two–Tier Architecture, the Presentation Layer or Interface runs on a Client, and the Data Layer or Data Structure is stored on a Server. The User System Interface is usually located in the User's desktop environment and the Database Management Services are kept in the Server which is a more powerful machine that services many Clients.

Three Tier Architecture: Three–Tier Architecture is a Client–Server Architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms.

12. Explain how and why the Three–Tier Architecture is used in E–Commerce.

Three - Tier architecture is a software design pattern and well-established software architecture. Its three tiers are the Presentation Tier, Application Tier and Data Tier. Three-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms. The three-tier architecture can be explained below:

Presentation Tier: Occupies the top level and displays information related to services available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.

Application Tier: This tier is pulled from the Presentation tier. It controls application functionality by performing detailed processing. This refers to the Application Server and Back End Server, and includes various Parties – (a) E–Commerce Vendor/Seller, (b) Reseller, if any, (c) Logistics Partner.

Database Tier: This tier houses the database servers where information is stored and retrieved. Data in this tier is kept independent of application servers or business logic. The Data Tier includes the data persistence mechanisms (database servers, file shares, etc.) and the data access layer that encapsulates the persistence mechanisms and exposes the data. This covers the Information Storehouse /Database, where all data relating to Customer Orders, Products, Prices, etc. are stored. This covers the Information Storehouse /Database, where all data relating to Customer Orders, Products, Prices, etc. are stored.

The following are the needs for Three-Tier Systems:

- Clear separation of user-interface-control and data presentation from application-logic.
- Dynamic load balancing.
- Change management.

13. What are the Risks in e–Commerce?

Risk is possibility of loss. The same may be result of intentional or un-intentional action by individuals. Risks associated with e-commerce transactions are high compared to general internet activities. These include the following:

(i) **Privacy and Security:** There are often issues of security and privacy due to lack of personalized digital access and knowledge.

(ii) **Quality issues:** There are quality issues raised by customers as the original product differs from the one that was ordered.

(iii) **Delay in goods and Hidden Costs:** When goods are ordered from another country, there are hidden costs enforced by Companies.

(iv) **Needs Access to internet and lack of personal touch:** The e-commerce requires an internet connection which is extra expensive and lacks personal touch.

(v) **Security and credit card issues:** There is cloning possible of credit cards and debit cards which poses a security threat.

(vi) **Infrastructure:** There is a greater need of not only digital infrastructure but also network expansion of roads and railways which remains a substantial challenge in developing countries.

(vii) **Problem of anonymity:** There is need to identify and authenticate users in the virtual global market where anyone can sell to or buy from anyone, anything from anywhere.

(viii) **Repudiation of contract:** There is possibility that the electronic transaction in the form of contract, sale order or purchase by the trading partner or customer maybe denied.

14. List the Control Objectives in e–Commerce.

Control Objectives in e–Commerce include the following –

(i) To recognize the significance of Information as a Critical Asset to the Entity,

(ii) To prevent loss from incorrect decision making,

(iii) To recognize the criticality and value of all IT Resources, viz. Hardware, Software and Personnel,

(iv) To prevent Cost of Data Loss,

(v) To avoid Computer Abuse and its related costs,

(vi) To maintain privacy and integrity of data shared through the Network amongst various Participants,

(vii) To safeguard IT Assets from un–authorized access

(viii) To ensure System Effectiveness, i.e. the ability to meet substantial User requirements, and

(ix) To ensure System Efficiency, i.e. to optimize the use of various IS Resources (machine time, peripherals, system software and Labour).

15. To manage risks in e–Commerce environment, Controls should be implemented by all Parties in the e–Business Chain. Explain this statement.

In an e-business environment, controls are necessary for all persons in the chain, including-

(i) Users: This is important to ensure that the genuine user is using the e-commerce/ m-commerce platform. There is risk if user accounts are hacked and hackers buy products / services.

(ii) Sellers / Buyers / Merchants: These people need to proper framework in place to ensure success of business. Many e-commerce businesses have lost huge amount of money as they did not have proper controls put in place. These include controls on:

1) Product catalogues

2) Price catalogues

3) Discounts and promotional schemes

4) Product returns

5) Accounting for cash received through Cash on Delivery mode of sales.

(iii) Government: Governments across the world and in India have few critical concerns vis-à-vis electronic transactions, namely:

1) Tax accounting of all products / services sold.

2) All products / services sold are legal. There have been instances where narcotics drugs have found to be sold and bought through electronic means.

(iv) Network Service Providers: They need to ensure availability and security of network. Any downtime of network can be disastrous for business.

(v) Technology Service Providers: These include all other service provider other than network service provider, for example, cloud computing back-ends, applications back-ends and like. They are also prone to risk of availability and security.

(vi) Logistics Service Providers: Success or failure of any e-commerce / m-commerce venture finally lies here. Logistics service providers are the ones who are finally responsible for timely product deliveries.

(vii) Payment Gateways: E-commerce vendors' business shall run only when their payment gateways are efficient, effective and foolproof.

16. Each Participant should have policies, practices and procedures in place to protect from e–commerce / m–commerce related risks. Explain this statement.

1) Educating the participant about the nature of risks:

1) Each Participant (and its Employees / Staff) should be properly educated and trained about the nature of risks in e– Business. It is easier to prevent risks and handle incidents, with proper awareness, education and training.

2) The frequency & nature of education programs, and the eligibility of participants in those programs should be defined properly.

2) Communication of organizational policies to its customers: To avoid customer dissatisfaction and disputes, the Entity's Policies on the following should be clearly defined and properly communicated to the Customers through the Website, by appropriate links on the Homepage –

1) Privacy Policies,

2) Information Security Policies,

3) Shipping and Billing Policies,

4) Policies in relation to handling special scenarios, e.g. "Payment Failed",

Order Details not received by Vendor, etc.

5) Refund Policies.

3) Ensure Compliance with Industry Body Standards: All e–Commerce Participants should comply with the applicable Rules / Regulations (e.g. FEMA, GST) and also the Standards if any, established by the Industry Body / Regulatory Authority (e.g. RBI).

4) Protect your e-Commerce business from intrusion:

1) Viruses: Check your website daily for viruses, the presence of which can result in the loss of valuable data.

2) Hackers: Use software packages to carry out regular assessments of how vulnerable your website is to hackers.

3) Passwords: Ensure employees change these regularly and that passwords set by former employees of your organization are defunct.

4) Regular software updates: Your site should always be up to date with the newest versions of security software. If you fail to do this, you leave your website vulnerable to attack.

17. List a few Control Considerations in managing Key Cyber Security Risks in e–Commerce.

Key Cyber Security Risks can be addressed through various Controls, including –

1) Proper definition of a Network Diagram detailing Servers, Databases, Hubs, Routers, Internal and External.

2) Networks, their Interconnects / Interfaces, etc.

3) Listing of the Entity's Digital Assets, their physical locations, and the IT Managers responsible for their protection.

4) Policy and Procedure Document of the criticality of the Digital Assets, the use of those digital assets, any direct impact on the Financial Statements of the company, access restrictions to those assets.

5) Periodical Review of Access Rights to all IT Resources to ensure that the access to the Users is commensurate with their functional roles and responsibilities.

6) Communication of IT Security Policy to all Staff, detailing the procedures to be adhered to when accessing IT

7) Systems / resources, e.g. Password Security, restricted use of Internet, etc.

18. Give examples of Legal Issues that are unique to E–Commerce transactions.

Some unique issues which may not arise in normal commercial transactions, may

arise in e–Commerce / m–Commerce transactions. Some examples are as follows

Event	**Legal questions out of event**
Product ordered by 'A' delivered to 'B'. (For example: a DEO). 'A' had made payment online.	1) What if 'B' accepts the products and starts using? 2) 'A' had ordered the product to gift to spouse on his/her birthday. What of the mental agony caused? 3) The product is a medicine necessary of treatment of 'A's dependent parents. In case of any complication to 'A's parent due to delayed delivery who bears the additional medical costs?
Service ordered by **'A'** not provided by online vendor. For example: **'A'** courier company does not collect an important document.	1) Who bears the loss that may be incurred by 'A'?
'A' auction website sales in-advertently sales products which cannot be sold at all, or sale of those products is illegal. For example: Guns/ Narcotics Drugs.	1) What is the legal liability if seller of products? 2) What is legal liability of buyers of such products? 3) What is the legal liability of auction web- site?
'A' downloads a software from a server in USA. **'A'** is in state of MP and then he sells the software to a person in Mumbai or Sells the same to another person in Singapore.	1) Whether such a download is import? 2) If 'A' re-exports can s/he claim benefits under customs?

19. List the prominent legislations that have an impact on E–Commerce.

Following commercial laws are applicable to e-commerce and m-commerce transactions.

a. **Income Tax Act, 1961:** Income Tax Act, has detailed provisions regarding taxation of income in India. In respect of e-commerce / m-commerce transactions, the issue of deciding place of origin transaction for tax purpose is critical.

b. **Companies Act, 2013:** Companies Act, 2013, regulates the corporate sector. The law defines all regulatory aspects for companies in India. Most of the merchants in e-commerce / m-commerce business are companies, both private and public.

c. **Foreign Trade (Development and Regulation) Act, 1992:** An Act to provide for the development and regulation of foreign trade by facilitating imports into, augmenting exports from, India and for matters connected therewith or incidental thereto. Amazon has recently allowed Indian citizens to purchase from

its global stores. All these shall be regulated through above law.

d. **The Factories Act, 1948:** Act to regulate working conditions of workers. The act extends to place of storage as well as transportation. Most of the merchants in e-commerce / m-commerce business need to comply with provisions of the act.

e. **The Goods and Services Tax (GST) Law:** This Law requires each applicable business, including e-commerce/ m-commerce, to upload each sales and purchase invoice on one central IT infrastructure, mandating reconciliations of transactions between business, triggering of tax credits on payments of GST, facilitating filling of e-returns, etc.

f. **Indian Contract Act,1872:** The Act defines constituents of a valid contract. In case of e-commerce / m-commerce business, it becomes important to define these constituents.

g. **The Competition Act, 2002:** Law to regulate practices that may have adverse effect on competition in India. Competition Commission have been vigilant to ensure that e-commerce / m-commerce merchants do not engage in predatory practices.

h. **Consumer Protection Act, 1986:** The law to protect consumer rights has been source of most of litigations for transaction done through e-commerce and m-commerce.

20. List the advantages and disadvantages of Digital Payments.

Advantages of digital payments: -

(i) Easy and convenient: Digital payments are easy and convenient. Person do not need to take loads of cash with themselves.

(ii) Pay or send money from anywhere: With digital payment modes, one can pay from anywhere anytime.

(iii) Discounts from taxes: Government has announced many discounts to encourage digital payments. User get 0.75% discounts on fuels and 10% discount on insurance premiums of government insurers.

(iv) Written record: User often forgets to note down his / her spending, or even if nothing is done it takes a lot of time. These are automatically recorded in passbook or inside E-Wallet app. This helps to maintain record, track spending and budget planning.

(v) Less Risk: Digital payments have less risk if used wisely. If user losses mobile phone or debit/credit card or Aadhar card, no need to worry a lot. No one can use anyone else's money without MPIN, PIN or fingerprint in the case of Aadhar. It is advised that user should get card blocked, if lost.

Disadvantages of digital payments: -

(i) Difficult for a Non-technical person: As most of the digital payment modes are based on mobile phone, the internet and cards. These modes are somewhat difficult for non-technical persons such as farmers, workers etc.

(ii) The risk of data theft: There is a big risk of data theft associated with the digital payment. Hackers can hack the servers of the bank or the E-Wallet a customer is using and easily get his/her personal information. They can

use this information to steal money from the customer's account.

(iii) Overspending: One keeps limited cash in his/her physical wallet and hence thinks twice before buying anything. But if digital payment modes are used, one has an access to all his/her money that can result in overspending.

21. Briefly explain a few methods of Digital Payments.

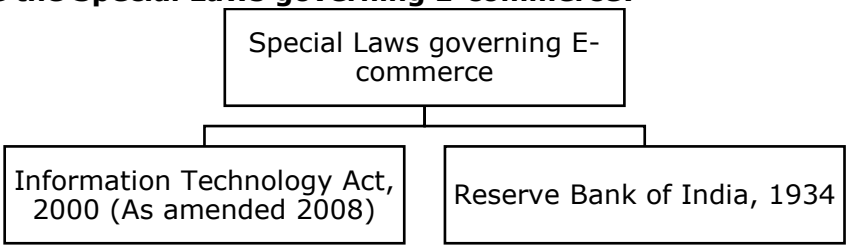
1) **UPI Apps:**
   - Unified Payment Interface (UPI) is a system that powers multiple Bank Accounts (of Participating Banks), several banking services features like fund transfer, and merchant payments in a single mobile application.
   - UPI is a payment mode which is used to make fund transfers through the Mobile App.
   - Some examples of UPI Apps are BHIM, SBI UPI App, HDFC UPI App, iMobile, Phone Pe App, etc.

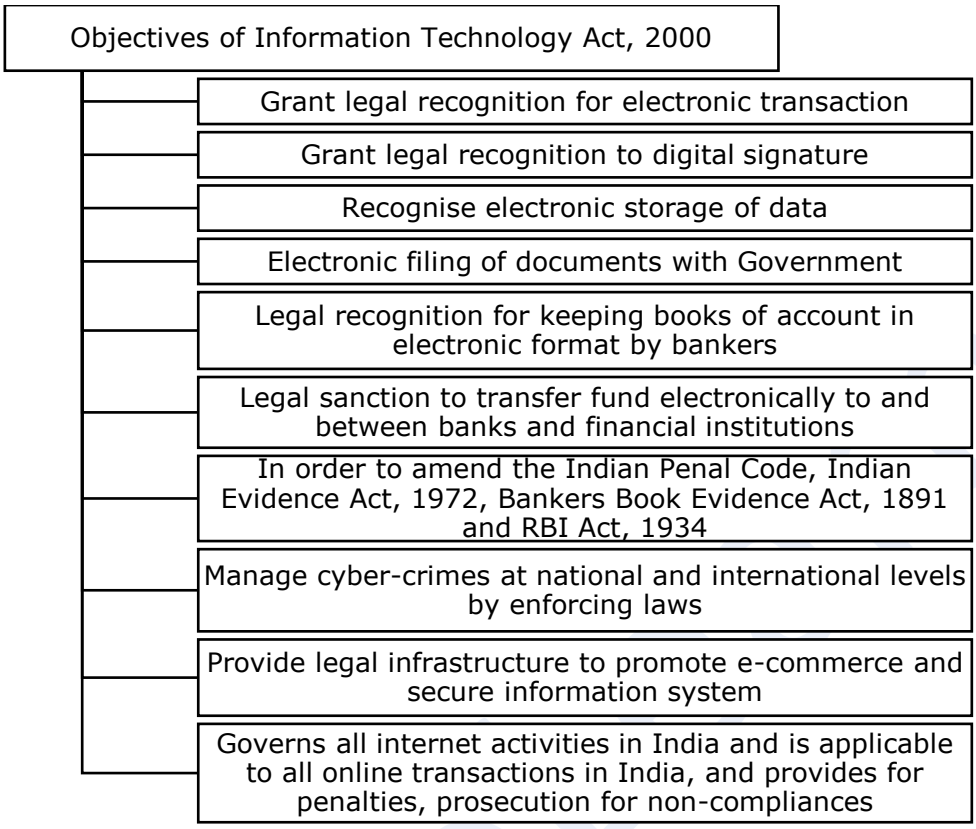
2) Immediate Payment Service (IMPS):
   - Immediate Payment Service (IMPS) is an instant inter–Bank Electronic Fund Transfer Service that can be transacted through Mobile Phones.
   - IMPS is also being extended through other channels such as ATM, Internet Banking, etc.

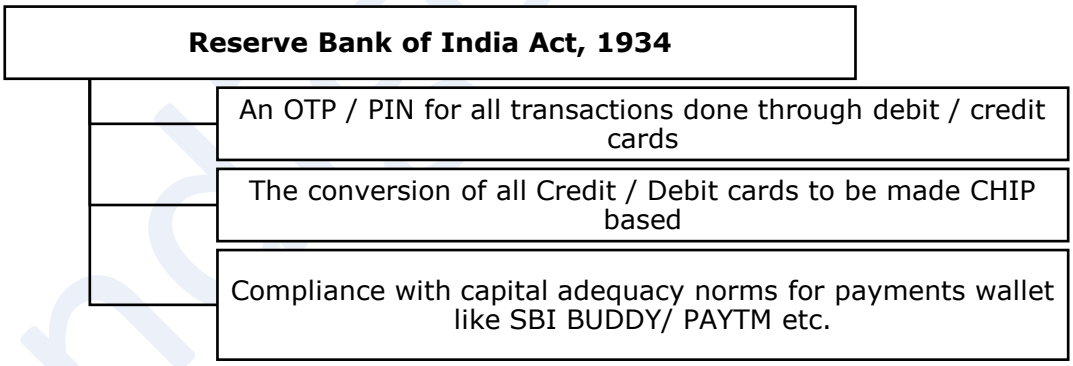
3) Mobile Apps:
   - BHIM (Bharat Interface For Money) is a Mobile App developed by the National Payments Corporation of
   - India (NPCI) based on UPI.
   - BHIM facilitates e–payments directly through Banks and supports all Indian Banks which use that platform. BHIM is built on the IMPS infrastructure and allows the User to instantly transfer money between the Accounts of any two parties.
   - BHIM works on all Mobile Devices and enables users to send or receive money to other UPI Payment Addresses by scanning QR Code or using Account Number with Indian Financial Systems Code (IFSC) Code or MMID (Mobile Money Identifier) Code for Users who do not have a UPI–based Bank Account.

4) Aadhar Enabled Payment Service(AEPS):
   - AEPS is an Aadhaar based digital payment mode. Customer needs only his or her Aadhaar number to pay to any merchant.
   - AEPS allows bank to bank transactions
   - It means the money you pay will be deducted from your account and credited to the payee's account directly.
   - Customers will need to link their AADHAR numbers to their bank accounts. APES once launched can be used at POS terminals also.

22. What are the Special Laws governing E-commerce?







23. Explain the Trends in E-commerce.

The latest trends in e-commerce are as follows:

i. **Content:** The content of the web should be such which not only attracts the customers' attention but also helps in engaging them. Shoppable videos for customers instead of using images and content would enable them to shop for products and services directly from videos.

ii. **Social Commerce:** The latest trend is the inclusion of e-commerce in social networks, such as Facebook, Twitter, YouTube, etc. Social media platforms offer innovative methods to reach first-time and new generation customers, engage and reward existing customers and showcase the best to offer.

iii. **Mobile Commerce:** The user is moving from desktop to mobile computing. 55% of the online traffic is generated from mobile devices and still it is on the increase. The creation of mobile application for e-commerce site is the latest trend to drive many online shoppers who use mobile apps for online shopping.

iv. **Biometrics:** Serious security issues such as hacking, spamming, online fraud and theft of confidential data are still holding back many online users from purchasing products online. Biometric verification is a recent e-commerce technology trends that measure the physical characteristics of users such as fingerprints, palm, face, or voice to solve security issues. With the use of biometrics, there will be no more stolen or forgotten password problem, also this enhanced security measures will make forging difficult for intruders.

v. **Artificial Intelligence:** Another trend in e-commerce is the use of Chatbot, a fully automated chat agent that will answer all the questions of consumers and act as a first point of contact. Chatbots commonly known as messenger bots is a piece of software that can be used by a retailer to chat with customers via text or voice. Well-designed chatbots can offer personalized assistances, enhance the user experience, process orders, track shipments, provide product suggestion, automates processes, and lot more.

vi. **Predictive Analysis:** The use of predictive analysis tools is increasing to predict the online customers' behavior. By segmenting the customers in different categories, the company can optimize its e-mail communication in order to increase conversions by offering-
   - the right customer
   - the right product
   - in the right way and
   - at the right time.

   The analytical approach would lead to an increase in the number of new customers. Predictive analysis tools help in predicting customers' buying habits, as well as their tastes and preferences, both quantitative and qualitative.

24. Explain Mobile Banking & Cryptocurrency

Mobile Banking: It is a service provided by a bank or other financial institution that allows its customers to conduct different types of financial transactions remotely using a mobile device such as a mobile phone or tablet. It uses software, usually called an app, provided by the banks or financial institution for the purpose. Each Bank provides its own mobile banking App for Android, Windows, and iOS mobile platform(s).

Cryptocurrency: Cryptocurrency is a digital currency produced by a public network, rather than any government, that uses cryptography to ensure that payments are sent and received safely. A cryptocurrency is a medium of exchange wherein records of individual coin ownership are stored in a computerized database using strong cryptography.

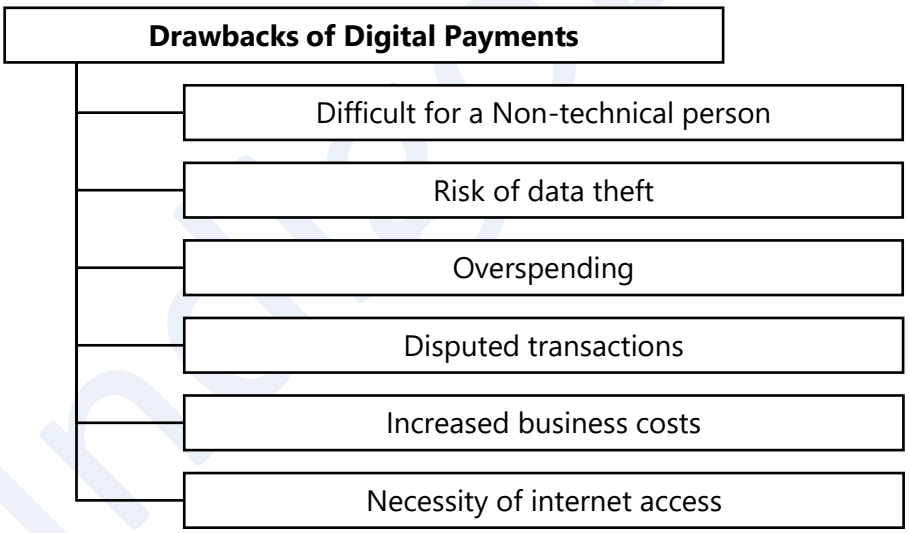
Cryptocurrency is called so because all the data is ensured with strong cryptography. The strong cryptography makes it almost impossible to counterfeit or double spend. The other digital currencies such as DigiCash utilizes a Trusted Third Party approach in which a third party verifies and facilitates the transactions. Cryptocurrency is completely decentralized, which means that there are no servers involved and no central controlling authority.

Cryptocurrency is stored in a digital wallet either on the computer or on other hardware. The first cryptocurrency was Bitcoin which was launched in 2009. The other cryptocurrencies prevailing in the world today include Litecoin, Peercoin, Namecoin, as well as Ethereum.

25.Explain E-Rupi

- e-Rupi based on UPI systems to ensure seamless transfer of benefits to the citizens in a "leak-proof" manner.
- It is an e-voucher, which will be delivered to beneficiaries in the form of a QR code and SMS-string-based voucher through which funds will be directly transferred to their bank account.
- These vouchers are person- and purpose-specific.
- e-RUPI is easy, safe, and secure as it keeps the details of the beneficiaries completely confidential.
- The entire is relatively faster and at the same time reliable, as the required amount is already stored in the voucher.
- Any government agency and corporation can generate e-RUPI vouchers via their partner banks.

26. List out the drawbacks of Digital payments.



Ch:4(b) Emerging Technologies

1. **Outline the concept of Virtualization. What are its major applications?**
    - **Virtualization** means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.
    - Virtualization refers to technologies designed to provide a layer of abstraction between computer hardware systems and the software running on them.
    - The core concept of Virtualization lies in Partitioning, which divides a single physical server into multiple logical servers. Once the physical server is divided, each logical server can run an operating system and applications independently.
    - Virtualization allows its' users to manipulate their systems' operating systems into thinking that a group of servers is a single pool of computing resources and conversely, allows its users to run multiple operating systems simultaneously on a single machine.

2. **What are the different types of Virtualization?**

    Common Types of Virtualization:

    1) Hardware Virtualization:

    - Hardware Virtualization or Platform Virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system.
    - Software executed on these virtual machines is separated from the underlying hardware resources.
    - The basic idea of Hardware virtualization is to consolidate many small physical servers into one large physical server so that the processor can be used more effectively.
    - The software that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Manager.

    2) Network Virtualization:

    - Network Virtualization is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time.
    - This allows a large physical network to be provisioned into multiple smaller logical networks and conversely allows multiple physical LANs to be combined into a larger logical network.
    - This behavior allows administrators to improve network traffic control, enterprise and security.
    - Network virtualization involves platform virtualization, often combined with resource virtualization.

    3) Storage Virtualization:

- Storage Virtualization is the apparent pooling of data from multiple storage devices, even different types of storage devices, into what appears to be a single device that is managed from a central console.
- Storage virtualization helps the storage administrator perform the tasks of backup, archiving, and recovery more easily and in less time by disguising the actual complexity of a Storage Area Network (SAN).
- Administrators can implement virtualization with software applications or by using hardware and software hybrid appliances.
- Storage virtualization is sometimes described as "abstracting the logical storage from the physical storage.

3. Write short notes on the concept of "Grid Computing".

- Grid Computing is a computer network in which each computer's resources are shared with every other computer in the system.
- It is a distributed architecture of large numbers of computers connected to solve a complex problem.
- It is a special kind of distributed computing. In distributed computing, different computers within the same network share one or more resources.
- In the ideal grid computing system, every resource is shared, turning a computer network into a powerful supercomputer.
- Processing Power, Memory and Data Storage are all community resources that Authorized Users can tap into and use for specific tasks. Every Authorized Computer would have access to enormous processing power and storage capacity.
- Every authorized computer would have access to enormous processing power and storage capacity.

4. What are the major applications of Grid Computing?
Application Areas of Grid Computing:

- Civil engineers collaborate to design, execute, & analyze shake table experiments.
- An insurance company mines data from partner hospitals for fraud detection.
- An application service provider offloads excess load to a compute cycle provider.
- An enterprise configures internal & external resources to support e- Business workload.
- Large-scale science and engineering are done through the interaction of people, heterogeneous computing resources, information systems and instruments, all of which are geographically and organizationally dispersed.

5. What are the Resources that can be "pooled" in Grid Computing?

The resources which are "pooled" or linked in a Grid include the following –

Computation:

Computing Cycles provided by the Processors of the Machines on the grid can be pooled together. This possible even if Processors vary in speed, architecture,

software platform, and other factors like memory, storage, and connectivity, etc. There primary ways to exploit the Computation Resources of a Grid are –

- To run an existing application on an available machine on the Grid rather than locally,
- To use an application designed to split its work in such a way that the separate parts an execute in parallel on different Processors, and
- To run an application, that needs to be executed many times, on many different machines in the Grid.

Storage:

- A grid providing an integrated view of data storage is sometimes called a Data Grid.
- Each machine on the grid usually provides some quantity of storage for grid use, even if temporary.
- Storage can be memory attached to the Processor or it can be Secondary Storage, using Hard Disk Drives or other permanent Storage Media.
- More advanced file systems on a grid can automatically duplicate sets of data, to provide redundancy for increased reliability and increased performance.

Communications:

- Communications within the grid are important for sending jobs and their required data to points within the grid.
- If only a limited Bandwidth available for communications, it can limit the utilization of the Grid.
- Higher Speed Networks may also be provided to meet the demands of jobs transferring larger amounts of data.

Software and Licenses:

- Instead of installing costly Software in each Node, it is possible to have Software installed for the Grid as a whole.
- Multi–User Licenses can be purchased to permit access by many Nodes at the same time.
- A License Management Software keeps track of how many Nodes are concurrently using the software, within the limits of the license.

Special equipment, capacities, architectures, and policies:

- Platforms on the grid will often have different architectures, operating systems, devices, capacities, and equipment.
- Each of these items represents a different kind of resource that the grid can use as criteria for assigning jobs to machines.

6. List the advantages of Grid Computing.

Advantages of Grid Computing as follows:

1) Making use of Underutilized Resources:

- In most organizations, there are large amounts of underutilized computing resources including even the server machines.

- Grid computing (more specifically, a data grid) can be used to aggregate unused storage into a much larger virtual data store, possibly configured to achieve improved performance and reliability over that of any single machine.

2) Resource Balancing:

- Grid offers resource balancing effect by scheduling grid jobs on machines with low utilization.
- This feature of grid computing handles occasional peak loads of activity in parts of a larger organization.
- If the grid is already fully utilized, the lowest priority work being performed on the grid can be temporarily suspended or even cancelled and performed again later to make room for the higher priority work.

3) Parallel CPU Capacity:

- The potential for usage of massive parallel CPU capacity is one of the most common visions and attractive features of a grid.
- A CPU-intensive grid application can be thought of as many smaller sub-jobs, each executing on a different machine in the grid.
- To the extent that these sub-jobs do not need to communicate with each other, the more scalable the application becomes.

4) Virtual resources and virtual organizations for collaboration:

- Grid computing provides an environment for collaboration among a wider audience.
- The users of the grid can be organized dynamically into several virtual organizations, each with different policy requirements.
- The grid can help in enforcing security rules among them and implement policies, which can resolve priorities for both resources and users.

5) Access to additional resources:

- In addition to CPU and storage resources, a grid can provide access to other resources as well.
- if a user needs to increase their total bandwidth to the Internet to implement a data mining search engine, the work can be split among grid machines that have independent connections to the Internet.

6) Reliability:

- High-end conventional computing systems use expensive hardware to increase reliability.
- The machines also use duplicate processors in such a way that when they fail, one can be replaced without turning the other off.
- All of this builds a reliable system, but at a great cost, due to the duplication of expensive components.

7) Management:

- The grid offers management of priorities among different projects.
- Aggregating utilization data over a larger set of projects can enhance an organization's ability to project future upgrade needs.
- When maintenance is required, grid work can be rerouted to other machines without crippling the projects involved.

7. What are the security factors to be considered in Grid Computing?

Following aspects should be considered in defining the Security Architecture: –

- **Single Sign-on:** A user should authenticate once and they should be able to acquire resources, use them, and release them and to communicate internally without any further authentication.
- **Protection of Credentials:** User passwords, private keys, etc. should be protected.
- **Interoperability with local security solutions:** Access to local resources should have local security policy at a local level. Despite of modifying every local resource there is an inter-domain security server for providing security to local resource.
- **Exportability:** The code should be exportable i.e. they cannot use a large amount of encryption at a time. There should be a minimum communication at a time.
- **Support for secure group communication:** In a communication, there are number of processes which coordinate their activities. This coordination must be secure and for this there is no such security policy.
- **Support for multiple implementations:** There should be a security policy which should provide security to multiple sources based on public and private key cryptography.

8. Write short notes on the concept of "Cloud Computing".

a) Cloud Computing, simply means the use of computing resources as a service through networks, typically the Internet.

b) Internet is generally visualized as "Clouds". Hence, use of Internet–based computing is called Cloud Computing.

c) Cloud Computing is a combination of both software based and hardware-based computing resources, provided through a Network Service.

d) Cloud Computing is designed to enable Users –

- ♦ to have anytime access to a shared pool of applications and resources,
- ♦ to access data using a simple front–end interface such as a Web Browser, and
- ♦ to develop, deploy and manage their resources on the Internet / Cloud, i.e. virtualization of resources.

9. List the objectives of Cloud Computing.

The objectives of cloud–based Computing are as under –

1) To bring all available IT resources in an eco–friendly and cost–saving way,
2) To ensure and improve IT services as accessible and available from anywhere ["Anywhere Access" (AA)],
3) To enlarge / upgrade / upscale the activities to match evolving business needs in a cost–effective manner,
4) To integrate IT–infrastructure and to create a manageable environment,
5) To reduce costs relating to Hardware and IT Energy / Power consumption.

10. Briefly describe the features of Cloud Computing.

Features of Cloud Computing:

1) Elasticity and Scalability:

- Cloud computing gives us the ability to expand and reduce resources according to the specific service requirement.
- we may need a large number of server resources for the duration of a specific task.
- We can then release these server resources after we complete our task.

2) Pay-per-Use:

- We pay for cloud services only when we use them, either for the short term or for a longer duration.

3) On-demand:

- Because we invoke cloud services only when we need them, they are not permanent parts of the IT infrastructure.
- This is a significant advantage for cloud use as opposed to internal IT services.
- With cloud services, there is no need to have dedicated resources waiting to be used, as is the case with internal services.

4) Resiliency:

- The resiliency of a cloud service offering can completely isolate the failure of server and storage resources from cloud users.
- Work is migrated to a different physical resource in the cloud with or without user awareness and intervention.

5) Multi Tenancy:

- Public cloud service providers often can host the cloud services for multiple users within the same infrastructure.
- Server and storage isolation may be physical or virtual depending upon the specific user requirements.

6) Workload Movement:

- Cloud-computing providers can migrate workloads across servers both inside

the data center and across data centers.

- This migration might be necessitated by cost or efficiency considerations

11. What are the advantages of Cloud Computing? (Any 8 points)

Major advantages of Cloud Computing include–

1) **Achieve economies of scale:** Volume output or productivity can be increased even with fewer systems and thereby reduce the cost per unit of a project or product.
2) **Reduce spending on technology infrastructure:** Data and information can be accessed with minimal upfront spending in a pay- as-you-go approach, which is based on demand.
3) **Globalize the workforce:** People worldwide can access the cloud with Internet connection.
4) **Streamline business processes:** Getting more work done in less time with less resources are possible.
5) **Reduce capital costs:** Not required to spend huge money on hardware, software, or licensing fees.
6) **Pervasive accessibility:** Data and applications can be accesses anytime, anywhere, using any smart computing device, making our life so much easier.
7) **Monitor projects more effectively:** It is feasible to confine within budgetary allocations and can be ahead of completion cycle times.
8) **Less personnel training is needed:** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9) **Minimize maintenance and licensing software:** As there is too much of premise computing resources, maintenance becomes simple and updates and renewals of software systems rely on the cloud vendor or provider.
10) **Improved flexibility:** It is possible to make fast changes in our work environment without serious issues at stake.

12. Differentiate between Grid Computing and Cloud Computing.

Aspect	Grid Computing	Cloud Computing
Meaning	**Grid Computing** is the provisioning of IT resources through a Control Server, to	**Cloud Computing** refers to provisioning of IT– resources as a service through the Internet.

	multiple locations, using web–services.	
Structure	This uses Software to divide and carve out pieces of program, as a large system image, to many computer nodes.	Resources are maintained in the Cloud / Internet for easy access, without installation of Software in the User Device.
Device use	Generally, access to Grid Computing is through one type of device only, e.g. only Desktop PCs, or only Laptops, etc.	Access to Cloud applications can be from a variety of devices – Desktop, Laptop, Smartphones, etc.
Point of failure	Sometimes, if one part of the Software in a Node fails, the application in other Nodes relying on such Node / Software, also fail. However, this can be avoided using certain Passover technologies.	Data is stored in the Cloud / Internet, which can be retrieved as per Users requirement. Failure of one node, will not affect other nodes.
Data storage	Suitable only for large volumes of data. Not economical if the data size is small.	Suitable for any size of data storage starting from 1 Byte to several Terabytes.
Cost	Higher Cost of Investment and Operating Expenses, due to need for large system images, and associated hardware to operate and maintain them.	Comparatively lower investment and operating expenses, in areas of Hardware, Software, Training, Data Storage, etc.
Focus	A computational Grid focuses mainly on computationally intensive operations.	Cloud Computing offers two types of service levels / instances – Standard and High–CPU.

13. What are the different types of Cloud Computing Environment?

Based on their deployment & usage, the Cloud Computing Environments may be classified as-

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

(ii) **Private Clouds:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called Internal Clouds or Corporate Clouds. Private Clouds can either be private to the organization and managed by the single organization or can be managed by third party.

(iii) **Community Clouds:** 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. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

(iv) **Hybrid Clouds:** 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. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

14. Write short notes on – (a) Public Clouds, (b) Private Clouds, (c) Community Clouds, and (d) Hybrid Clouds.

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

   Features:

   (i) **Scalable,** since Public Clouds have higher resources, and Service Providers ensure that all requests are granted.

   (ii) **Affordable,** since Public Cloud is offered to the public on a pay–as–you–go basis (e.g. per hour, etc.), and hence, low cost of usage / deployment.

   (iii) **Less Secure** than other deployment Models, since Public Cloud is offered by a Third Party who have full control over the Cloud.

   (iv) **Highly Available**, i.e. access from any part of the world with proper permission, without much geographical or other access restrictions.

   (v) **Stringent SLAs,** since the Service Provider's business reputation and customer strength are largely dependent on the Cloud Services, SLAs are followed strictly and violations are avoided.

2) **Private Clouds:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called Internal Clouds or Corporate Clouds. Private Clouds can either be

private to the organization and managed by the single organization or can be managed by third party.

Features:

(i) **More Secure** since the Private Cloud is deployed and managed by the Entity itself, and lower chance of data leakage.

(ii) **Better Control,** since the Entity need not rely on anybody else for control of the Private Cloud.

(iii) **Weak SLAs,** since in a Private Cloud, Formal SLAs do not exist or are weak as it is between the Entity and User of the same Entity.

3) **Community Clouds:** 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. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Features:

(i) **Collaborative & Distributive:** No single Company has full control over the whole cloud. This is usually distributive and hence better co–operation provides better results.

(ii) **Partially Secure:** Only a few organizations share the Cloud, so there is a possibility that the data can be leaked from one organization to another, however it is safe from the external world.

(iii) **Cost Effective:** Community Cloud becomes cost effective since it is shared by many organizations.

4) **Hybrid Clouds:** 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. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

Features:

(i) **Scalable:** Hybrid Cloud with the help of its Public Cloud counterpart is also scalable.

(ii) **Partially Secure:** The Private Cloud is considered as secured and Public Cloud has high risk of security breach. The Hybrid Cloud is thus partially secure.

(iii) **Stringent SLAs:** SLAs are more stringent than the Private Cloud, and might be on the lines provided by the Public Cloud Service Providers.

(iv) **Complexity:** Cloud Management is complex as it involves more than one type of deployment models, with high number of Users.

15. Cloud Computing has its disadvantages. Explain.

Drawbacks of Cloud Computing:

1) If Internet connection is lost, the link to the cloud and thereby to the data and applications is lost.
2) Security is a major concern as entire working with data and applications depend on other cloud vendors or providers.
3) Although Cloud computing supports scalability (i.e. quickly scaling up and down computing resources depending on the need), it does not permit the control on these resources as these are not owned by the user or customer.
4) Depending on the cloud vendor or provide, customers may have to face restrictions on the availability of applications, operating systems and infrastructure options.
5) Interoperability (ability of two or more applications that are required to support a business need to work together by sharing data and other business-related resources) is an issue wherein all the applications may not reside with a single cloud vendor and two vendors may have applications that do not cooperate with each other.

16. Explain the various Models of Cloud Computing Environment in brief.

Infrastructure as a Service (IaaS):

- **IaaS**, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand.
- This allows users to maximize the utilization of computing capacities without having to own and manage their own resources.
- The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs) and design virtual infrastructure, network load balancers etc., based on their needs.
- The IT architects need not maintain the physical servers as it is maintained by the service providers.

Platform as a Service (PaaS):

- In traditional application development, the application will be developed locally and will be hosted in the central location.
- In stand-alone application development, the application will be developed by traditional development platforms result in licensing - based software, whereas PaaS changes the application development from local machine to online.
- Typical PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases.
- Examples of PaaS: Google App Engine, Windows Azure Compute, etc.

Software as a Service (SaaS):

- SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.
- The end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure.

- SaaS changes the way the software is delivered to the customers.
- SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure.

Instance	Description
Testing as a Service (TaaS)	• Provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.
API as a Service (APIaaS)	• Allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
Email as a Service (EaaS)	• Provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

17. Different instances of Iaas

Instance	Description
Network as a Service (NaaS)	• Provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. • It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis. • Allows network architects to create virtual networks; virtual network interface cards (NICs), virtual routers, virtual switches, and other networking components. • Allows the network architect to deploy custom routing protocols and enables the design of efficient in-network services, such as data aggregation, stream processing, and caching. NaaS providers operate using three common service models: Virtual Private Network (VPN), Bandwidth on Demand (BoD) and Mobile Virtual Network (MVN).
Storage as a Service (STaaS)	• Provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. • It is an ability given to the end users to store the data on the storage services provided by the service provider.

	• STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center.
Database as a Service (DBaaS)	• Provides users with seamless mechanisms to create, store, and access databases at a host site on demand. • It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis. • The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.

18. What are the other cloud service models?

Instance	Description
Communication as a Service (CaaS)	• It is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. • This approach eliminates the large capital investments. Examples are: Voice over IP (VolP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.
Data as a Service (DaaS)	• Provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. • Data encryption and operating system authentication are commonly provided for security. DaaS users have access to high-quality data in a centralized place and pay by volume or data type, as needed. • However, as the data is owned by the providers, users can only perform read operations on the data. DaaS is highly used in geography data services and financial data services.
Security as a Service (SECaaS)	• It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. • It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats.
Identity as a Service (IDaaS)	• It is an ability given to the end users; typically, an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third-party service provider. • Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

19. What is Mobile Computing?

- Mobile Computing refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link.
- Mobile Computing is the use of portable computing devices in conjunction with mobile communications technologies to enable users to access the Internet and data on their home or work computers from anywhere in the world.
- Mobile Voice technology (i.e. Cell Phones Network) is extended to Mobile Computing, where data is being sent and received across the Network, on a wireless platform.
- An extension of this technology is the ability to send and receive data across these cellular networks.

20. List a few benefits of Mobile Computing.

Benefits of Mobile Computing:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real- time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledge base at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

21. What are the components of Mobile Computing?

The key components of Mobile Computing are as follows:

Mobile Communication:

- This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on.
- This would include communication properties, protocols, data formats and concrete technologies.

Mobile Hardware:

- This refers to the various Mobile Devices or Device Components that receive or access the service of mobility.
- It includes Portable Laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on.
- At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network.

Mobile Software:

- It is the actual program that runs on the Mobile Hardware and deals with the characteristics and requirements of Mobile Applications.
- It is the operating system of that Device, i.e. essential to make the Device operate.
- Mobile Applications (called Apps), are developed by organizations for use by customers.
- However, Apps could represent risks, in terms of flow of data, personal identification risks, introduction of malware and access to personal information of Mobile Owner.

22. How does Mobile Computing work?

Mobile Computing operates similar to an Employee's Desktop PC access the Organization's applications, except that the User's Device is not physically connected to the organization's system.

- The user enters or access data using the application on hand-held computing device.
- Using one of several connecting technologies, the new data are transmitted from hand-held to site's information system where files are updated and the new data are accessible to other system user.
- Now both systems (hand-held and site's computer) have the same information and are in sync.
- The process works the same way starting from the other direction.

23. List a few limitations of Mobile Computing.

1) **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and **E**nhanced **D**ata Rates for **G**SM **E**volution and 3G, 4G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

2) **Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

3) **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

4) **Transmission interferences:** Weather, terrain and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

5) **Potential health hazards:** People who use mobile devices while driving is often distracted from driving, and are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.

6) **Human interface with device:** Screens and keyboards tend to be small,

which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

24. Write short notes on the concept of Green Computing or Green IT.

- Green Computing or Green IT refers to the study and practice of environmentally sustainable computing or IT.
- In other words, it is the study and practice of establishing/ using computers and IT resources in a more efficient and environmentally friendly and responsible way.
- The objective of Green computing is to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste.
- Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

25. User Habits play a significant role in Green IT. Explain.

For effective implementation of Green Computing, Government Regulation as well as well–informed work habits of Computer Users are necessary. Some such steps for Green IT include

- Use energy–efficient Central Processing Units (CPUs), Servers and Peripherals.
- Switch Off the CPU and all peripherals during extended periods of inactivity.
- Switch–on and Switch–off energy–intensive peripherals such as Laser Printers, according to need of use.
- Use Liquid Crystal Display (LCD) Monitors rather than Cathode Ray Tube (CRT) monitors.
- Use Notebook Computers rather than Desktop Computers whenever possible.
- Use the power–management features to turn off Hard Drives and displays after several minutes of inactivity.
- Minimize the use of paper and properly recycle waste paper.
- Dispose off e–waste according to applicable law and regulations.
- Employ alternative energy sources for power supply to Workstations, Servers, Networks and Data Centers.
- Plan work so as to handle all computer–related tasks in one go, instead of alternating between paperwork and system–work. Switch off Computer in durations of paperwork.

26. List a few Best Practices in Green IT.

Some of such steps for Green IT include the following:

1) **Develop a sustainable Green Computing plan:**
   - On-going communication about and campus commitment to green IT best practices to produce notable results.
   - Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans;
   - Use cloud computing so that multiple organizations share the same computing resources thus increasing the utilization by making more efficient use of hardware resources.
2) **Recycle:**

- Dispose e-waste according to central, state and local regulations;
- Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and
- Recycle computers through manufacturer's recycling services.

3) Make environmentally sound purchase decisions:

- Purchase of desktop computers, notebooks and monitors based on environmental attributes;
- Provide a clear, consistent set of performance criteria for the design of products;
- Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

4) Reduce Paper Consumption:

- Reduce paper consumption by use of e-mail and electronic archiving;
- Use of "track changes" feature in electronic documents, rather than red line corrections on paper;
- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

5) Conserve Energy:

- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;

27. Write short notes on the "Bring Your Own Device" (BYOD) Concept.

- 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 to connect to the corporate network to access information and application.
- The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours.
- Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

28. What are the threats associated with BYOD Concept?

Risks associated in implementation of BYOD are generally classified into four broad areas:

1) **Network Risks:**

- In BYOD Environment, the Employer has no control the over the number of devices and systems used, traffic handled, and data exchanged over the Internet / Intranet.
- Network Security Risk increases in case of Virus attack, and when there is a need for scanning all systems in the Network.

- If a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation.
- In addition to this, the network security lines become blurred when BYOD is implemented.

2) **Device Risks:**
   - In BYOD Environment, Loss of Employee's Personal Devices which contains sensitive corporate information, can cause financial and reputational embarrassment to an organization.
   - Data from stolen or lost devices can provide easy access to Company emails, Company trade secrets and confidential data from a misplaced device.
3) **Application Risks:**
   - Employees' Mobiles and Smart Devices are not generally protected by Security Software available with the Entity.
   - Also, there is a lack of clarity in identifying 'who is responsible for device security 'the organization or the User'.
4) **Implementation Risks:**
   - It is normally exemplified and hidden in 'Weak BYOD Policy'.
   - Corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse.
   - This risk relates to the possibility of lack of proper BYOD Policy or poor communication thereof, device misuse, and consequent loss of valuable Corporate Knowledge and Data.
   - This risk can be overcome through measures like – (i) adherence to a robust BYOD Implementation Policy, (ii) an effective Employee education / training program.

29. Write short notes on Web 3.0.

- The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction.
- Web 3.0 seeks to achieve a more connected open & intelligent web applications using the concepts of natural language processing, machine learning, machine reasoning and autonomous agents.
- Web 3.0 Application uses Content Management Systems along with Artificial Intelligence.
- These systems are capable of answering the questions posed by the Users, because the application is able to think on its own and find the most probable answer, depending on the context, to the query submitted by the User.

30. Write short notes on Internet of Things (IoT) Concept.

The **Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to- computer interaction.

Applications: Some of the applications are as follows:

- Home Appliances are connected to create a "virtual home", so that all activities at home can be monitored through the Mobile Phone / Hand–held devices held by the Owner while s/he is at office.
- Office Appliances are connected through intranet, so that many statistical information on Resource Usage can be obtained effectively, e.g. Number of Pages printed in Office Printer, etc.
- Governments can keep track of resource utilizations / extra support needed.
- Wearables: Just like smart homes, wearables remain another important potential IoT application like Apple smartwatch.
- Connected Car: Connected car technology is a vast and an extensive network of multiple sensors, antennas, embedded software, and technologies that assist in communication to navigate in our complex world.

31. Write short notes on Artificial Intelligence (AI) and Machine Learning Concepts.

Artificial Intelligence (AI): The ability described above when exhibited by machines is called as Artificial intelligence (AI). It is intelligence exhibited by machines.

For example:

1) This technology is being used in autonomous vehicles, the google car.
2) Apple online assistant Siri is supposed to use it.

Applications: Artificial Intelligence is being used in the following applications:

- Autonomous vehicles (such as drones and self-driving cars);
- Medical diagnosis, in cancer research. Predicting the chances of an individual getting ill by a disease;
- Creating art (such as poetry);
- Proving mathematical theorems;
- Playing games (such as Chess or Go), and predicting the outcomes. Say which number on a lottery ticket may win;
- Search engines (such as Google search);
- Online assistants (such as Siri);

Machine Learning: Machine Learning is a type of Artificial Intelligence (AI) that provides computers with the ability to learn without being explicitly programmed.

The process of machine learning is similar to that of data mining. For example:

1) Machine learning has been used for image, video, and text recognition, as well as serving as the power behind recommendation engines. Apple SIRI is a good example.
2) This technology is being is being used in autonomous vehicles, the google car.

Applications: Virtually all applications were in AI using Machine learning so that some value is added. It includes specifically following application:

- Autonomous vehicles (such as drones and self-driving cars),

- Medical diagnosis, in cancer research. Predicting the chances of an individual getting ill by a disease.
- Playing games (such as Chess or Go), and predicting the outcomes. Say which number on a lottery ticket may win.
- Search engines (such as Google search),
- Online assistants (such as Siri).

32. Explain Pertinent issues related to Cloud computing

As an emerging technology, cloud computing involves several issues. Some of the pertinent issues related to cloud computing are:

Threshold Policy	• The main objective of implementing threshold policy is to inform cloud computing service consumers and providers what they should do. • Quite often, this policy does not exist. The only legal document between the customer and service provider is the Service Level Agreement (SLA). • This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do. • However, there is no standard format for the SLA, and as such, there may be services not documented in the SLA that the customer may be requiring in future.
Interoperability	• If a company enters a contract with one cloud computing vendor, it may find it difficult to change to another computing vendor that has proprietary APIs (application programming interfaces) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. • Once a company is locked in with one cloud provider, it is not easy to move an entire infrastructure to other clouds.
Hidden Costs	• Such costs may include higher network charges for storage and database applications, or latency issues for users who may be located far from cloud service providers.
Unexpected Behaviour	• An application may perform well at the company's internal data centre. It does not necessarily imply that the application will perform the same way in the cloud. • Therefore, it is essential to test its performance in the cloud for unexpected behaviour. • Testing may include checking how the application allocates resources on sudden increase in demand for resources and how it allocates unused resources.
Security Issues	• Cloud computing infrastructures use new technologies and services, most of which have not been fully evaluated with respect to security. • The important security issues with cloud computing are the management of the data might not be fully trustworthy; the risk of malicious insider attacks in the cloud; and the failing of cloud services.

	• Maintaining confidentiality is one the major issues faced in cloud systems because information is stored at a remote location which can be accessed by the service provider. Data confidentiality can be preserved by encrypting data. • Cloud systems share computational resources, storage, and services between multiple customer applications in order to achieve efficient utilization of resources while decreasing cost. • However, this sharing of resources may violate the confidentiality users' IT Assets. It must be ensured that there a degree of isolation between these users.
Legal Issues	• Cloud systems need to adhere to several regulatory requirements, privacy laws and data security laws. • These laws vary from country to country and cloud users have no control over where their data is physically located.
Software Development in Cloud	• From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. • The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security. • The project manager must keep in mind the applications should be upgraded frequently.
Bugs in Large-Scale Distributed Systems	• One of the difficult challenges in Cloud Computing is removing errors in these very large-scale distributed systems.

33. What is blockchain technology?

Blockchain referred to as Distributed Ledger Technology (DLT) is a shared, peer-to-peer, and decentralized open ledger of transactions system with no trusted third parties in between.

Every entry is permanent and cannot be changed or altered and all the transactions are fully irreversible.

The decentralised network refers to the network which is not controlled by any bank, corporation, or government. A blockchain generally uses a chain of blocks, with each block representing the digital information stored in public database

34. Applications of Blockchain Technology

- Financial Services

  Blockchain can be used to provide an automated trade lifecycle in terms of the transaction log of any transaction of asset or property - whether physical or digital such as laptops, smartphones, automobiles, real estate, etc. from one person to another.

- Healthcare

  Blockchain provides secure sharing of data in healthcare industry by increasing the privacy, security, and interoperability of the data by eliminating the interference of third party and avoiding the overhead costs.

- Government

  Blockchain improves the transparency and provides a better way to monitor and audit the transactions relating to land registration, vehicle registration and management, e-voting etc.

- Travel Industry

  Blockchain can be applied in money transactions and in storing important documents like passports/other identification cards, reservations and managing travel insurance, loyalty, and rewards thus, changing the working of travel and hospitality industry.

- Economic Forecasts

  Blockchain makes possible the financial and economic forecasts based on decentralized prediction markets, decentralized voting, and stock trading, thus enabling the organizations to plan and shape their businesses.

35. Risks and controls associated with Blockchian

- With the use of blockchain, organizations need to consider risks with a wider perspective as different members of a particular blockchain may have different risk appetite/risk tolerances that may further lead to conflict when monitoring controls are designed for a blockchain.

  There may be questions about who is responsible for managing risks if no one party is in-charge and how proper accountability is to be achieved in a blockchain.
- The reliability of financial transactions is dependent on the underlying technology and if this underlying consensus mechanism has been tampered with, it could render the financial information stored in the ledger to be inaccurate and unreliable.
- In the absence of any central authority to administer and enforce protocol amendments, there could be a challenge in the establishment of development and maintenance of process control activities and in such case, users of public blockchains find difficult to obtain an understanding of the general IT controls implemented and the effectiveness of these controls.

- As blockchain involves humongous data getting updated frequently, risk related to information overload could potentially challenge the level of monitoring required. Furthermore, to find competent people to design and perform effective monitoring controls may again prove to be difficult.

Controls

- Instead of traditional manual techniques, computerized continuous monitoring techniques shall be used to perform ongoing evaluations, considering the large volume of data processed and the frequency at which these transactions are getting processed.
- Suitable data analytics procedures shall be developed to identify and obtain relevant and quality data from the blockchain so that it can then be processed into information that subsequently can be used to support management's business processes and reporting objectives.
- Communication methods shall be developed to ensure that operational changes and updates relating to the use of blockchain are communicated to appropriate personnel so that internal control related responsibilities are carried out in proper manner.
- The unique aspects of blockchain such as consensus protocols, smart contracts, and private keys, as well as factors relating to the ongoing health, governance, and overall reliability of the blockchain in use; shall be assessed thoroughly.
- Both internal and external auditors shall be engaged in discussions during the development or identification of a blockchain so as to make the management understand the typical auditability issues associated with using blockchain. Subsequently, processes can be established to mitigate against those issues so that the appropriate information and support for transactions is available.

Ch:5 Core Banking Systems

1. List the major features of Banking Business.

The key features of a banking business are as follows:

1) The custody of large volumes of monetary items, including cash and negotiable instruments, whose physical security should be ensured.

2) Dealing in large volume (in number, value and variety) of transactions.

3) Operating through a wide network of branches and departments, which are geographically dispersed.

4) Increased possibility of frauds as banks directly deal with money making it mandatory for banks to provide multi-point authentication checks and the highest level of information security.

2. Write short notes on the following activities of Banks

(a) Acceptance of Deposits,

(i) Banks accept Deposits from their Customers, which is the source of money for the purpose of lending.

(ii) Deposits may be made by Customers in various schemes for pre–defined / specified periods.

(iii) Banks accept deposits in various forms, e.g. Term Deposits, Savings Bank Deposits, Current Account Deposits, Recurring Deposit, Saving–cum–Term Deposit, etc.

(iv) Banks offer various innovative products and schemes, to mobilise Deposits

(b) Granting of Advances – (Funded Limits),

(i) Advances constitute the major revenue–generating activity of Banks.

(ii) In respect of Business Sector, Advances may be in different forms – (a) Cash Credit, (b) Bill Purchasing / Discounting, (c) Overdrafts, (d) Term Loans, etc.

(iii) In respect of Retail Sector, Advances may be towards Vehicles, Housing, Education, etc.

(iv) Banks may also provide special facilities like issuance of Commercial Papers, ECB (External Commercial Borrowing) on behalf of Bank/ Borrower, securitization of Credit Sales, etc.

(v) Many Banks have specialized Centres to handle the Advances function, e.g. Corporate Banking Branch, SME Advances Branch, etc.

(c) Letter of Credits and Guarantees – (Non–Funded Limits),

(i) Issuing Letters of Credit and Guarantees are the major Non–Funded Limits granted by Banks to customers engaged in business, industrial and commercial activities.

(ii) A Letter of Credit (LC) is an Undertaking by a Bank to the Payee (the Buyer) any amount up to the limit specified in the LC, provided the terms and conditions mentioned in the LC are complied with.

(iii) A Bank may provide Guarantees for the performance of contractual obligations undertaken by their Customers, or satisfactory performance of goods supplied by them, or for submission by Customers to Government Agencies, or to Suppliers of goods, etc. in lieu of any Security Deposit.

(d) Collections,

(i) Customers can deposit instruments like Cheques, Drafts, Pay Orders, Travelers Cheques, Dividend and Interest Warrants, Tax Refund Orders, etc. drawn in their favour and Trade Bills drawn by them on their Buyers with their Bank for collection.

(ii) Banks collect the proceeds of these instruments, on behalf of the customer.

(iii) Collection Services are also extended for Term Deposit Receipts, instruments issued by Post Offices, e.g. National Savings Certificates, Postal Orders, etc.

(e) Clearing,

(i) Clearing, i.e. collecting instruments on behalf of Customers, is done through Clearing House Mechanism.

(ii) A Clearing House settles the inter–Bank transactions among the local participating Member Banks and Post Offices.

(iii) Clearing Houses generally adopt the electronic means, viz. MICR (Magnetic Ink Character Recognition) Code for its operations.

(iv) MICR Code is a 9–digit code comprising relevant information about the transaction and the Bank. MICR technology allows machines to read and process cheques, and complete voluminous transactions within a short time.

(v) Using Core Banking System (CBS), Banks/Branches, honour and pay instruments of other Branches beyond their Clearing Zone payable at par by the designated Branch of that Centre.

(f) Remittances,

(i) Remittances involve transfer of funds from one place to another.

(ii) Remittances are handled by Banks through – (a) Demand Draft (DD)

/ Bankers' Cheque / Pay Orders, (b) Telegraphic / Mail Transfers (TT/MT), (c) Electronic Funds Transfer (NEFT / RTGS transfer).

(g) Credit Cards,

(i) Credit Cards permit Customers to draw / avail an "Advance" from the Bank while making a purchase, and settle the amount to the Bank after the specified credit period. Sometimes, Cash Withdrawal is also permitted on a Credit Card.

(ii) Generally, Credit Cards issued by Banks are linked to one of the International Credit Card Networks (VISA, Master, etc.)

(h) Debit Cards,

(i) Debit Card facilitates Customers to pay at any authorized outlet, or to withdraw money from an ATM from their account. Debit Cards are networked with an Inter–Bank Network.

(ii) When a Debit Card is used for a transaction, the amount is immediately deducted from the Customer's Account Balance. There is no "Advance" or "Loan" given by the Bank in this case.

(i) Other Services.

Other Services rendered by Banks include –

(i) Retail Banking: These are Front–Office Operations that cover all operations which provide Direct Retail Services to Customers.

(ii) High Net–Worth Individuals (HNI): Banks provide special services to customers classified as High Net–Worth Individuals (HNI) based on value/volume of deposits/ transactions.

(iii) Back Operations: These cover all operations done at the Back Office of the Bank, and include General Ledger, Management Information Systems, Reporting, etc.

(iv) Specialized Services: Banks perform services like Insurance Broking, Claims, Underwriting, Life Insurance, Non–Life Insurance, etc, either by themselves, or by separate Entities / Subsidiaries.

(v) Risk Management: Risk Management is done at strategic, tactical, operational and technology areas of the Bank. Risk Management is managed as per the Bank's Policy, with detailed standards, procedures and guidelines provided for uniform implementation.

3. Give a few examples of IT Controls in Banks.

Some examples of internal controls in bank branch are given here:

1) Work of one staff member is invariably supervised/ checked by another staff member, irrespective of the nature of work (Maker-Checker process).

2) A system of job rotation among staff exists.

3) Financial and administrative powers of each official/ position is fixed and communicated to all persons concerned.

4) Branch managers must send periodic confirmation to their controlling authority on compliance of the laid down systems and procedures.

5) All books are to be balanced periodically. Balancing is to be confirmed by an authorized official.

6) Details of lost security forms are immediately advised to controlling so that they can exercise caution.

7) Fraud prone items like currency, valuables, draft forms, term deposit receipts, traveller's cheques and other such security forms are in the custody of at least two officials of the branch.

4. Write short notes on Implementing IT Controls in Banks. (May 2019)

Sample list of IT related controls are:

1) The system maintains a record of all log-ins and log-outs.

2) If the transaction is sought to be posted to a dormant (or inoperative) account, the processing is halted and can be proceeded with only with a supervisory password.

3) The system checks whether the amount to be withdrawn is within the drawing power.

4) The system flashes a message if the balance in a lien account would fall below the lien amount after the processing of the transaction.

5) Access to the system is available only between stipulated hours and specified days only.

6) Individual users can access only specified directories and files. Users should be given access only on a 'need-to-know basis' based on their role in the bank. This is applicable for internal users of the bank and customers.

7) Exception situations such as limit excess, reactivating dormant accounts, etc. can be handled only with a valid supervisory level password.

8) A user timeout is prescribed. This means that after a user logs-in and there is no activity for a pre-determined time, the user is automatically logged out of the system.

9) Once the end-of-the-day process is over, the ledgers cannot be opened without a supervisory level password.

5. Differentiate between General Controls and IT Application Controls, in the context of Banking Sector.

In the context of Banking Sector, Controls may be classified as under:

Point	General controls	Application controls
Meaning	These are controls which pervade across different layers of IT Environment and IT Systems.	These are controls which are implemented in an application, to prevent or detect and correct errors.
Scope	Their impact is macro in nature, i.e. at different levels of IT Environment.	They pertain to the scope of individual business processes or application systems (i.e. micro–impact.)
Purpose	1) To meet overall objectives of the IT System, 2) To manage IT related risks effectively, 3) To ensure that the Technology in use, supports the Business Objectives.	1) To ensure accurate and reliable processing, 2) To ensure that all transactions and data remains authorized, complete, accurate and valid during its input, update and storage.
Examples	1) IT Security Policy, 2) Business Continuity Plan 3) Change Management Documentation, etc	1) Only Transactions of the day will be processed by the System. 2) Excess Drawing permitted only if authorised.

6. All key modules of banking are all connected and related transactions are interfaces with central server. Explain.

All key modules of banking are all connected and related transactions are interfaces with central server are explained below:

1) **Back Office:** The Back Office is the portion of a company made up of administration and support personnel, who are not client-facing. Back-office functions include settlements, clearances, record maintenance, regulatory compliance, accounting, and IT services. Back Office professionals may also work in areas like monitoring employees' conversations and making sure they are not trading forbidden securities on their own accounts.

2) **Data Warehouse:** Banking professionals use data warehouses to simplify and standardize the way they gather data - and finally get to one clear

version of the truth. Data warehouses take care of the difficult data management - digesting large quantities of data and ensuring accuracy - and make it easier for professionals to analyse data.

3) **Credit-Card System:** Credit card system provides customer management, credit card management, account management, customer information management and general ledger functions; provides the online transaction authorization and service of the bank card in each transaction channel of the issuing bank; Support in the payment application; and at the same time, the system has a flexible parameter system, complex organization support mechanism and product factory-based design concept to speed up product time to market.

4) **Automated Teller Machines (ATM):** An Automated Teller Machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access most ATMs.

5) **Central Server:** Initially, it used to take at least a day for a transaction to get reflected in the real account because each branch had their local servers, and the data from the server in each branch was sent in a batch to the servers in the data centre only at the end of the day (EOD). All the bank's branches access applications from centralized data centres/servers, therefore, any deposits made in any branch are reflected immediately and customer can withdraw money from any other branch throughout the world.

6) **Branch Banking:** CBS are the bank's centralized systems that are responsible for ensuring seamless workflow by automating the frontend and backend processes within a bank. CBS enables single-view of customer data across all branches in a bank and thus facilitate information across the delivery channels.

7. What is CORE Banking System?

- **CORE** stands for **"Centralized Online Real–Time Environment"**.
- Core Banking System (CBS) is the set of basic software components that manage the services provided by a Bank to its Customers through its Branches and other points of transaction.
- A Bank's CBS functions as a heart (Circulatory System) and also its nervous system in the electronic world.
- CBS is the platform where Communication Technology and Information Technology are merged to suit the core needs of Banking.

8. Briefly describe a few Features of CBS.

The characteristics of CBS are:

1) There is a common database in a central server located at a Data Centre, which gives a consolidated view of the bank's operations.
2) Branches function as delivery channels providing services to its customers.
3) CBS is centralized Banking Application software that has several components which have been designed to meet the demands of the banking industry.
4) CBS is supported by advanced technology infrastructure and has high standards of business functionality.
5) Core Banking Solution brings significant benefits such as a customer is a customer of the bank and not only of the branch.
6) CBS is modular in structure and is capable of being implemented in stages as per requirements of the bank.

9. List a few technology components of CBS.

The key technology components of CBS are as follows:

- Database Environment
- Application Environment
- Cyber Security
  - Network Security and Secure Configuration
  - Application Security
  - Data Centre and Disaster Recovery Centre
  - Online transaction monitoring for fraud risk assessment

10. Write short notes on the following– (a)Infosys' Finacle, (b) Nucleus FinnOne, and (c) Oracle's Flexcube, (d) BaNCS, (e) bankMate.

(a) **Finacle:** Core banking software suite developed by Infosys that provides universal banking functionality covering all modules for banks covering all banking services.

(b) **FinnOne:** Web-based global banking product designed to support banks and financial solution companies in dealing with assets, liabilities, core financial accounting and customer service.

(c) **Flexcube:** Comprehensive, integrated, interoperable, and modular solution that enables banks to manage evolving customer expectations.

(d) **BaNCS:** A customer-centric business model which offers simplified operations comprising loans, deposits, wealth management, digital channels and risk and compliance components.

(e) **bankMate:** A full-scale Banking solution which is a scalable, integrated e-banking systems that meets the deployment requirements in traditional and non-traditional banking environments. It enables communication through any touch point to provide full access to provide complete range of banking services with anytime, anywhere paradigm.

11. CBS is based on Client–Server Architecture. Explain the Role of Client, Server and Branches in this regard.

Role of Client:

- User may be a Customer, or Staff at a Branch / Office.
- User–Actions and Controls are predominantly menu–driven.
- User is prompted by the Software to initiate an activity or to apply a control.
- User's actions are validated by the CBS, and the transaction is permitted / allowed accordingly.
- All operations that a Customer may do at any of the Branches of the Bank, are validated at those Branches. However, the accounting process is centralized at the Central Data Centre, and is updated at the Centralized Database.

Role of Server:

- Update of Database immediately when transactions are input and validated / authorised,
- Updating of parameters globally,
- System–generated Transactions, e.g. Application of Interest and Service Charges, Standing Instructions, Transfers, etc.
- Balancing/Reconciliation of Ledgers,
- Triggering and Generation of various kinds of Reports, etc.

Role of Branches:

- Beginning–Of–Day (BOD) Operations,
- Managing manual documents/vouchers, capturing data required for input into the software,
- Internal Authorization,
- End–Of–Day (EOD) Operations,
- Reviewing Reports for control and error correction.

12. The Technology Architecture of CBS has a four–layer Model. Describe briefly.

The Technology Architecture of CBS has a four–layer Model as under –

1) **Client:** A Client Device can be a Teller, ATM, POS, Mobile Phone, Telephone, WAP Client, Internet, TV Browser, Personal Digital Assistant (PDA), Branch Computer Terminal, etc.

2) **Channel Servers:** The above Clients connect to the Channel Servers. Channel Servers include Branch Server, Web Server, ATM/POS Switch, WAP or SMS Server, IVR Server, etc.

3) **Application Server:** Channel Servers route the Client Request to the Application Server (housed in the Central Data Centre). Application Server components include TP Monitors, Host Connect and Business

Intelligence.

4) **Host Server:** The Host Database Server houses the Execution Logic, and also has an appropriate DBMS (e.g. Oracle RDBMS).

13. Explain the various key aspects in-built into the architecture of the Core Banking System.

Some key aspects in-built into architecture of a CBS are as follows:

1) **Information flow:** This facilitates information flow within the bank and improves the speed and accuracy of decision-making. It deploys systems that streamline integration and unite corporate information to create a comprehensive analytical infrastructure.

2) **Customer centric:** Through a holistic core banking architecture, this enables banks to target customers with the right offers at the right time with the right channel to increase profitability.

3) **Regulatory compliance:** This holds the compliance in case bank is complex and expensive. CBS has built-in and regularly updated regulatory platform which will ensure compliance.

4) **Resource optimization:** This optimizes utilization of information and resources of banks and lowers costs through improved asset reusability, faster turnaround times, faster processing and increased accuracy.

14. Prepare a list of risks associated with Data Centre and Network Operations of Core Banking System.

Risks associated in respect of Data Centre and Network Operations of Core Banking System are:

- The transactions may not be recorded completely or accurately, and the related items will be inaccurately or incompletely recorded.
- Invalid items may be recorded or valid items may be inaccurately or incompletely recorded.
- Timely and adequate technical support may not be available and issues may not be resolved.
- User queries may not be timely and adequately resolved.
- Timely execution and complete processing and availability of data may not be ensured.
- Unavailability of applications or data backups in the event of a disaster.
- Backup may not be available if subject to some disaster, resulting in risk of data loss.
- Data may be lost and systems may not be recoverable in the event of a serious system failure.

15. Write short notes on the following Servers in a CBS IT Environment – (a) Application Server, (b) Internet Banking Application Server (c) ATM Channel Server, (d) Internet Banking Channel Server, (e) Database server, (f) Web Server, (g) Proxy Server, (h) Anti–Virus Software Server.

(a) Application Server:

- All the transactions of the Customer are processed by the Data Centre. The Application Server performs necessary operations and this update the account of the Customer in the Database Server.
- Generally, the Application Server is located at the Central Data Centre. Sometimes, the Application Server may be decentralized and located at a Regional Office or at Branch for easy and quick response.
- The Application Software in the Application Server should always be the latest version as accepted after adequate testing. The Testing process is such that –
  1) Changes are first made to a separate server called "Test Server".
  2) Programs are debugged and certified that the program is now amended as required and performs as is expected of it.
  3) The changed and latest Application Software is moved into the "Live" Application Server under proper authority.
  4) The earlier version of the Software is archived.
  5) The latest copy of the Software would always have a Backup Copy.

(b) Internet Banking Application Server:

- The Internet Banking Software which is stored in the IBAS (Internet Banking Application Server) authenticates the Customer with the login details stored in the IBCS (Internet Banking Channel Server).
- Authentication involves comparison of the details provided by the Customer, with the data already stored in the Data Server, to ensure that the Customer is genuine and is authorised to do Internet Banking.

(c) ATM Channel Server:

- This Server contains the details of ATM Account Holders (e.g. Account Number, Customer Name, Balance, etc.).
- Since ATMs are attached to the Central Network, the control is established through ATM Switch.
- A File containing the Account Balances of the Customers [called Positive Balance File (PBF)] is sent to the ATM Switch, by the Central Database.
- So, ATM Transactions continue to happen without any halt, even if the Central Database is busy or inaccessible due to EOD activities, etc.

- Once the Central Database Server becomes accessible, all the transactions that took place till such time as the
- This ensures – (a) continuity of ATM Operations, and (b) prompt updation of the Central Database.

(d) Internet Banking Channel Server:

- The Internet Banking Database Server as well as the IBCS Software stores the details as to Username, Passwords, Home Branch, etc. of all the Internet Banking Customers.
- The Internet Banking Customer should first log into the Bank's Website with the Username and Password.
- After verifying his credentials, the IBCS Server forwards his transaction request to the Application Server.

(e) Database Server:

- The Database Server of the Bank contains the entire data of the Bank.
- Data consists of – (a) Transaction Data and (b) Master Data.
- Direct Access is not permitted to the Database Server, so as to ensure Data Integrity.
- Access to the Database Server is permitted only for – (a) the Application Software, i.e. normal Application Server, (b) ATM Server, and (c) Internet Banking Application Server (IBAS).
- There is a designated role for maintenance of the Database, i.e. the Database Administrator (DBA).
- Every access to the Database is logged and monitored, including the activities of the DBA himself.

(f) Web Server:

- The Web Server is used to host all Web Services and Internet–related Software, using HTTP (Hypertext Transfer Protocol).
- All the Online Requests and Websites are hosted and serviced through the Web Server.
- User logs in and makes a request to the Web Server, which hosts the Internet Banking Website.
- Web Server uses HTTP to send the files that form the Web Pages to the Users.
- To protect the Web Server from unauthorized use, a Firewall is designed such that only traffic addressed to the Web Server through the Authorized Port is permitted.
- All Computers that host Websites must have Web Server Programs. Sometimes, there may be dedicated computers and appliances to function as Web Servers.

(g) Proxy Server:

- A Proxy Server is a Computer that offers a Computer Network Service to allow Clients to make indirect network connections to other network services.
- A Client connects to the Proxy Server, and then requests a connection, file, or other resource available on a different Server.
- The Proxy Server provides the resource either by connecting to the specified server or by serving it from a cache.
- Sometimes, the Proxy may alter the Client's request or the Server's response for various purposes.

(h) Anti–Virus Software Server:

- The Anti–Virus Server is used to host Anti–Virus Software.
- All the Software deployed are first scanned to prevent unnecessary consequences. This ensures that appropriate Virus/ Malware Scans are performed.

16. Application Software in a CBS Environment have 4 Gateways. Briefly explain them.

Application Software have 4Gatewaysthrough which the Bank / Entity can control the functioning, access and use the various menus and functions of the software –

1) Configuration:

- Configuration refers to the manner in which a Software is set–up for use.
- Configuration is thus the first step after Software Installation, and is a very significant step.
- It includes both Hardware and Software Parameters.
- Configuration will define how the Software will function and what menu options are displayed.
- CBS Configuration involves defining the various parameters as per the Bank's Policies, Practices, Procedures and Business Process Rules.
- CBS Configuration includes –
  - modifying the default parameters in Systems Software,
  - defining the workflow for each of the Products or Services,
  - setting up of different CBS Modules e.g. Advances, Deposits, Cash, Treasury, etc.
  - defining the Access Rules, User Creation, Rights, Password Procedures, etc.
  - specifying the manner of system–driven transactions, e.g. Interest Computation.

2) Masters:

- Masters refer to the setting parameters for various types of Product and Service Types as per the Software Modules used in the Bank.

- The Parameter Settings in the Masters will determine how the Software will process relevant transactions.
- After configuring the software, the Masters are set–up first time during installation.
- Masters are also called Standing Data, since they are changed only when – (i) there are changes in Business Processes, Values, etc. and (ii) they are authorised by appropriate levels of Management.
- Some examples of masters in context of CBS Software are as follows:
  - Customer Master: Customer type, details, address, PAN details,
  - Employee Master: Employee Name, Id, designation, level, joining details, salary, leave, etc.
  - Income Tax Master: Tax rates applicable, Slabs, frequency of TDS, etc.

3) Transactions:

- In CBS, Transactions refer to the actual transactions of various Products and Services.
- Some examples of transactions in the context of CBS software are given here:
  - Deposit transactions: opening of a/c, deposits, withdrawals, interest computation, etc.
  - Advances transactions: opening of a/c, deposits, withdrawals, transfers, closure, etc.
  - ECS transactions: Entry, upload, authorize/approve, update, etc.
  - General Ledger: Expense accounting, interest computation update, charges update, etc.

4) Reports:

- Information processed by the System is provided to Users through Reports.
- These reports could be used for monitoring the operations as also for tracking the performance or security.
- Some examples of reports are as follows:
  - Summary of transactions of day
  - Daily General Ledger (GL) of day
  - Activity Logging and reviewing
  - MIS report for each product or service
  - Reports covering performance/compliance;
  - Reports of exceptions, etc.

17. List a few Control Points in implementing CBS.

The deployment and implementation of CBS should be controlled at various stages to ensure that banks automation objectives are achieved:

1) **Planning**: Planning for implementing the CBS should be done as per strategic and business objectives of bank.

2) **Approval:** The decision to implement CBS requires high investment and recurring costs and will impact how banking services are provided by the

bank. Hence, the decision must be approved by the board of directors.

3) **Selection:** Although there are multiple vendors of CBS, each solution has key differentiators. Hence, bank should select the right solution considering various parameters as defined by the bank to meet their specific requirements and business objectives.

4) **Design and develop or procured:** CBS solutions used to be earlier developed in-house by the bank. Currently, most of the CBS deployment are procured. There should be appropriate controls covering the design or development or procurement of CBS for the bank.

5) **Testing:** Extensive testing must be done before the CBS is live. The testing is to be done at different phases at procurement stage to test suitability to data migration to ensure all existing data is correctly migrated and testing to confirm processing of various types of transactions of all modules produces the correct results.

6) **Implementation:** CBS must be implemented as per pre-defined and agreed plan with specific project milestones to ensure successful implementation.

7) **Maintenance:** CBS must be maintained as required. E.g. program bugs fixed, version changes implemented, etc.

8) **Support:** CBS must be supported to ensure that it is working effectively.

9) **Updation:** CBS modules must be updated based on requirements of business processes, technology updates and regulatory requirements;

10) **Audit:** Audit of CBS must be done internally and externally as required to ensure that controls are working as envisaged.

18. Explain the Business Process Flow of CASA Facility. Outline its Risks and related Controls.

Process flow of CASA facility:

a. **Customer request:** Customer – (a) approaches the Relationship Manager (RM) to apply for a CASA facility, or (b)applies for CASA facility through Internet Banking.

b. **Application:** Customer submits relevant documents, viz. Application, KYC Documents (PAN, Aadhaar, Driving License, Passport, etc.), either in physical self–attested or electronic form (e–KYC).

c. **Initial screening:** After initial screening for completeness, the RM forwards the documents to the Credit Team.

d. **Assessment:** The Credit Team – (a) verifies the documents, (b) assesses the financial and credit–worthiness of the Applicant Customer, and (c) updates the appropriate facilities in the Customer Account.

e. **Facilities:** CASA along with the requested facilities are provided to the Customer for daily operations. Facilities include Cheque Deposits / Withdrawal, Cash Deposit / Withdrawal, RTGS, NEFT, ECS, SMS Alerts, Internet Banking, etc.

Risks & controls in CASA process:

Risk	Key controls
Customer Master defined in CBS is not as per the Application / KYC	• Input Controls should be in place to check accuracy of data by comparing with Source Documents, immediately after its entry. • Access Rights to authorize the Customer Master in CBS should be restricted to Authorized Personnel.
Inaccurate Interest / Charges is calculated in CBS.	• Interest Allowed on Savings Account balances should be automatically computed in CBS as per the defined rules. • Charges for facilities, e.g. RTGS/NEFT, etc. should be automatically computed in CBS as per the defined rules.
Unauthorized Personnel approve the CASA transaction in CBS.	SoD to be maintained between the Initiator (Maker) and Authorizer (Checker) of the transaction for processing in CBS.
Inaccurate accounting entries are generated in CBS	Accounting Entries should be generated by CBS based on the facilities requested by the Customer, and defined configurations for those facilities in CBS.

19. Explain the Business Process Flow of Credit Cards. Outline its Risks and related Controls.

Process Flow of Issuance of Credit Card Facility:

(a) Either the customer approaches the relationship manager to apply for a credit card facility or customer will apply the same through internet banking, the charges/rates for the facility are provided by the relationship manager basis the credit application made by the customer.

(b) Once the potential customer agrees for availing the facilities/products of the bank, the relationship manager request for the relevant documents i.e. KYC and other relevant documents of the customer depending upon the facility/product.

(c) The document received from the customers are handed over to the Credit team for sanctioning of the facilities/limits of the customers.

(d) Credit team verifies the document's, assesses the financial and credit worthiness of the borrowers and issues a credit limit to the customer in CBS and allots a credit card.

(e) Credit Card is physically transferred to the customer's address.

Process Flow of Sale - Authorization process of Credit Card Facility:

(a) Customer will swipe the credit card for the purchase made by him/her on the POS machine (Point of Sale) at merchant's shop/establishment.
(b) POS (Point of Sale) will process the transaction only once the same is authenticated.
(c) The POS (Point of Sale) will send the authentication request to the merchant's bank (also referred as 'acquiring bank') which will then send the transaction authentication verification details to the credit card network (such as VISA, MASTER CARD, AMEX, RUPAY) from which the data will be validated by the credit card issuing bank within a fraction of seconds.
(d) Once the transaction is validated, the approval message is received from credit card issuing bank to the credit card network which then flows to the merchant's bank and approves the transaction in the POS (Point of Sale) machine.
(e) The receipt of the transaction is generated and the sale is completed. The transaction made is charged during the billing cycle of that month.

Process Flow of Clearing & Settlement process of Credit Card Facility:

(a) The transaction data from the merchant is transferred to the merchant's bank. Merchant's bank clears settlement amount to Merchant after deducting Merchant fees. Merchant's bank, in turn now provides the list of settlement transactions to the credit card network which then provides the list of transactions made by the customer to the credit card issuing bank.
(b) The credit card issuing bank basis the transactions made, clears the amount to Merchant's bank but after deducting interchange transaction fees.
(c) At the end of billing cycle, card issuing company charges the customer's credit card account with those transactions in CBS.

Risk & Controls in Credit Card Process:

Risks	**Key control**
Credit Line setup is unauthorized and not in line with the Bank's policy	Credit Committee should check that the Financial Ratios, Net–Worth, Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is as per the Bank's Credit Risk Policy and that the Client can be given the Credit Line
Credit Line setup is unauthorized and not in line with the bank's policy.	Access Rights to authorize the Credit Limit in the Credit Card System should be restricted to Authorized Personnel.
Masters defined for the customer are not in	• Access Rights to authorize the Customer Master in the Credit Card System should be restricted to Authorized Personnel.

accordance with the Pre-Disbursement Certificate.	• SoDs should be in place in Credit Card System, so that a Maker cannot exercise Checker's rights also.
Credit Line setup can be breached.	• Controls should ensure that a transaction cannot be made if the aggregate Outstanding Amount exceeds the Credit Limit assigned to the Customer. • A "Denied" message is sent to the Intermediary, and also to the Customer.
Inaccurate Interest / Charge is calculated in the Credit Card system.	Interest on fund–based Credit Cards and Charges are automatically calculated in the Credit Card System as per the defined masters.
Inaccurate reconciliations are performed	Daily Reconciliation is made for the balances received from Credit Card Network with the transactions updated in the Credit Card System on Card Network Level.

20. Explain the Business Process Flow of Mortgage Loans. Outline its Risks and related Controls?

Business process flow of mortgage loan:

a. **Customer request:** Customer approaches the Relationship Manager (RM) or Loan Officer (LO) to apply for a Mortgage Loan.
b. **Discussion:** The RM/LO provides Loan Consulting to the Customer / Borrower, on various procedural and financial aspects of the Loan.
c. **Application:** Customer submits Loan Application, KYC Documents, Income Proof, details as to Existing Loans and Financial Obligations, Property proposed to be purchased, etc.
d. **Initial screening:** After initial screening and review of the Application and Documents, the RM/LO forwards the Application and Documents to the Credit Team.
e. **Credit assessment:** The Credit Risk Team evaluates various factors like – (i) Present and Proposed Incomes, (ii)Existing Loan Obligations, (iii) Past Credit History of the Applicant in terms of CIBIL Score, (iv) Ratios of Proposed EMIs to Net Disposable Income, (v) Number of Dependents, etc.
f. **Under writing team**: The Underwriting Team –(1) verifies the Applicant's Credit History and current employment information, (2) ensures that the Loan to be provided is within the lending guidelines, (3) provides a Conditional Approval, along with the list of documents to be obtained.
g. **Legal & valuation:** The Property proposed to be purchased is evaluated by the Legal and Valuation Team for – (1) Whether the Applicant will obtain a Clean Title to the property upon its purchase,

and can therefore affect a valid mortgage in favour of the Bank? (2) Whether the Value of the Property constitutes appropriate security for the Bank? (3) Whether Norms as to Approved Plan, Age of the Building, Construction Quality, Completion Certificate, Utility Connections, etc. are complied with?

h. **Operation team:** The Legal and Valuation Team sends its report to the Operations Team. The Operations Team generates the Offer Letter (Sanction Letter) to the Applicant, providing details as to Loan Amount, Rate of Interest, Period of Repayment (Tenor), Monthly Instalment, Address of Property, Processing Fees, Insurance Coverage, and other applicable terms and conditions.
i. **Customer acceptance:** Customer agrees to the Loan Agreement by signing the Offer Letter, and Loan Documents. All signed and executed documents are then sent to the Operations Team.
j. **Disbursement:** Operations Team disburses the Loan Amount (in one instalment or in tranches, as per the agreement), generally by a Demand Draft / Electronic Transfer in favour of the Seller of the Property – after ensuring conditions like TDS Remittance, Stamp Duty, Margin, etc.
k. **Security creation:** RM/LO follows up with the Customer for execution of related documents like Mortgage Deed, CERSAI Certification, etc. to ensure First Charge on the Property, in the Bank's favour.
l. **Servicing:** Customer carries out Loan Servicing activities (e.g. Interest Rate Change, EMI Change, pre–payments, foreclosure, etc.) through the Nodal Branch, or through online mode

Risk & Controls in Mortgage Loan Process:

Risk	Key control
Incorrect customer and loan details are captured which will affect the over- all downstream process.	There is secondary review performed by an independent team member who will verify loan details captured in core banking application with offer letter
Incorrect loan amount disbursed.	There is secondary review performed by an independent team member who will verify loan amount to be disbursed with the core banking application to the signed offer letter.
Interest amount is in-correctly calculated and charged.	Interest amount is auto calculated by the core banking application basis loan amount, ROI and tenure.
Unauthorized changes made to loan master data or customer data.	System enforced segregation of duties exist in the core banking application where the person putting in of the transaction cannot approve its own transaction and reviewer cannot edit

	any details submitted by person putting data.

21. Explain the Business Process Flow of Trade / Business Finance. Outline its Risks and related Controls.

Business process flow of Trade/Business Finance:

a. **Customer request:** Customer approaches the Relationship Manager (RM) to apply for a Mortgage Loan. Alternatively, the RM may identify potential customers and approach them with the details of the products/ facilities offered by the Bank and the charges/rates thereof.

b. Discussion: The RM provides Consulting to the Customer / Borrower, on various procedural and financial aspects of the Loan.

c. **Application:** Customer submits Loan Application, KYC Documents, Audited Financial Statements, Financial Projections, details as to Existing Loans and Financial Obligations, Project Details, etc.

d. **Initial screening:** After initial screening and review of the Application and Documents, the RM forwards the Application and Documents to the Credit Team.

e. **Credit assessment:** The Credit Risk Team evaluates various factors like – (i) Project Feasibility, (ii) Financial Strength of the Applicant, (iii) Past Credit History of the Applicant in terms of CIBIL Score, (iv) Key Financial Ratios, (v) Primary and Collateral Securities offered, etc.

f. Sanction Letter: Legal and Valuation Team seeks to Legal Clearance (i.e. validity of Title) and Valuation of the Properties offered as Primary and Collateral Security to the Bank. The Credit Team issues a Sanction Letter to the Customer, containing the details the terms of the facilities and the Credit Limits the customer is eligible.

g. Customer acceptance & PDC: Customer agrees to the Loan Agreement by signing the Offer Letter, and Loan Documents. Credit Team prepares a Pre–Disbursement Certificate (PDC) containing the details of all the facilities and limits approved for the customer, and sends it to the Disbursement Team. Disbursement Team creates Customer Account and Master in the Loan Disbursement System and updates the various credit limits sanctioned as per PDC.

h. **Security creation:** RM follows up with the Customer for execution of related documents like Mortgage Deed, CERSAI Certification, ROC Charge Creation, etc. to ensure a Charge in the Bank's favour.

i. **Disbursement:** Disbursement Team disburses the Loan Amount, by – (i) crediting the Account of the Customer, (ii) Funds Transfer in favour of Vendor (in case of Term Loans for Asset Acquisition), or (iii)permitting withdrawals by cheque up to specified limit (in case of CC/OD, etc.)

j. **Operations:** Customer carries out operations in the account, and Loan Servicing activities (e.g. Renewals, Interest Rate Change, foreclosure, etc.) in the normal manner.

Risk & Controls in Trade Finance:

Risk	Key control
Credit Line setup is unauthorized and not in line with the Bank's policy	Credit Committee should check that the Financial Ratios, Net–Worth, Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit Amount, etc. is as per the Bank's Credit Risk Policy and that the Client can be given the Credit Line
Credit Line as per CBS is not as per sanctioned limit	Access Rights to authorize the Credit Limit in the Loan System should be restricted to Authorized Personnel.
Facilities granted may be unauthorized / inappropriate	SoDs should be in place in Loan System, so that a Maker cannot exercise Checker's rights also.
Masters defined for the Customer are not as per the PDC.	• Access Rights to authorize the Customer Master in the Loan System should be restricted to Authorized Personnel. • SoDs should be in place in Loan System, so that a Maker cannot exercise Checker's rights also.
Credit Line setup can be breached.	• Controls should ensure that a transaction cannot be made if the aggregate • Outstanding Amount exceeds the Credit Limit assigned to the Customer
Inaccurate Interest/ Charges are calculated in the Loan Disbursal system	• Interest on Fund–Based Loans and Commission Charges for Non–Fund Based Loans are automatically calculated in the Loan Disbursal System as per the defined Masters. • Masters are regularly updated for changes in the Base Rate of Interest.

22. Explain the Business Process Flow of Treasury Operations. Outline its Risks and related Controls.

Business process flow of treasury operations:

a. **Pre-Deal Analytics:** Before entering into a Deal (for purchase or sale), Dealers check various aspects including – (a) Requirements of the Bank,

(b) Risk levels undertaken, (c) Counter–Party and Own Credit Limits, (d) Regulatory Compliance, e.g. Forex Deals, Board Resolution, International Swaps and Derivatives Association (ISDA) Agreement, Margin Requirements, etc.

b. **Entering into trade deals:** Dealers use the appropriate Trading /Communication Platform, e.g. Reuters' System, Telephonic Conversation, Brokers or another Private Channel, with the respective Counter–Party. All transactions in a Treasury Function are recorded through a system that tracks the flow of each transaction through its life cycle. The document that records the transaction is called a Deal Ticket.
c. **Ticket entry:** As soon as the deal is struck with the Counter–Party, the Deal Ticket is recorded in the Front Office System, and gets queued in for authorization.
d. **FO approval:** After the Deal Ticket has been created and recorded, it is approved by another User in the Front Office. Each User is assigned a financial limit, to approve Ticket Amounts within that limit.
e. **Middle office process:** If Deal Ticket details are found correct, the Deal Ticket as approved by FO, flows into the Treasury System. Middle Office now performs Pricing and Valuations on the Deal Ticket.
f. **Confirmation:** After FO Approval of the Deal Ticket and Pricing / Valuation in Middle Office, the Deal Ticket is verified by a User in the Back Office. After Back Office Verification, the deal is approved by another User in the Back Office, within the financial limits / delegated powers. This constitutes the Confirmation of the Deal Ticket.
g. **Settlement:** When a deal is complete, a Confirmation Letter containing the terms and conditions thereof is sent to the Counterparty. Generally, the External Confirmation from the Counterparty is received on the same day itself. Settlement of Securities / Funds is made by the Back-Office Team, based on the above.
h. **Reconciliation:** FOBO (Front Office/ Back Office) Reconciliation – to ensure the completeness and accuracy of trades/deals done for the day,

Risk & Controls in Treasury Operations

Risk	Key control
Unauthorized securities setup in systems such as Front office/Back office.	Appropriate Segregation of duties and review controls around securities master setup/ amendments.
Inaccurate trade is processed	Appropriate Segregation of duties and review controls to ensure the accuracy and authorization of trades.
Unauthorized confirmations are processed	Complete and accurate confirmations to be obtained from counter-party.
Insufficient Securities available for Settlement	Effective controls on securities and margins.

Incomplete and inaccurate data flow between systems.	Inter-system reconciliations, Interfaces and batch processing controls.
Insufficient funds are available for settlements	Controls at CCIL/NEFT/RTGS settlements to ensure the margin funds availability and the timely funds settlements.

23. Explain the Business Process Flow of Internet Banking.

Internet Banking Process is as under:

(a) Application:

- The Customer applies to the Bank for Internet Banking facility.
- The Customer is provided with a User ID and Password.
- The Password provided by the Bank is expected to be changed at the first log–in, and further log–ins are permitted only using the Password as changed by the Customer.

(b) Validation of User ID and password-Access control:

- User accesses the Bank's Internet Banking Website through a Browser.
- The Browser connects to the Bank's Website.
- Bank's Website and a facility for Log in User keys in the User ID and Password.
- Based on the confirmation with the Master Data at IBDS, the IBAS sends an acknowledgement to the Web Server. The Web Server displays the appropriate message.

(c) Internet Banking Transactions:

- If User ID and Password are properly validated, the Customer is permitted to perform the authorized transactions and service requests, e.g. Funds Transfer, Balance Enquiry, Tax Payment, Statement of Accounts, Password Change, etc.
- The Service requested is directed by the Web Server to the IBAS for processing.
- The Internet Banking Channel Server (IBCS) retrieves the data from the Central Database Server. The IBCS will be able to access the Central Database Server only through a Middleware and Firewall.
- The Web Server generates a dynamic web page for the service requested, e.g. Tax Payment Challan, Statement of Accounts, etc. and presents it to the Web Browser in an encrypted form.
- User may choose to log out, or may be automatically logged out after one service request.
- The Customer may also be permitted to have multiple service requests in one session itself.

- If there is no action from the User for some time, the system may log out automatically with the message as "Session Expired", and request for a fresh log–in.

24. Write short notes on e–Commerce Transaction Processing – i.e. Payment Process through Gateway.

- Here, the User logs in on the e–commerce Website Portal, places an order and selects the option of payment, e.g. through Cards, or through Internet Banking.
- For Payment through Internet Banking, the Merchant Site is directed to Bank's Merchant–Internet Banking Server.
- User must log in in the Bank's Server and authorize payment, through OTP (Online Transaction Password) received on the Registered Mobile, to complete the transaction.
- After this, the Customer is re–directed from the Bank's Site to Merchant's Site.

25. List a few IT risk related to CBS.

Some of the common IT risks related to CBS are as follows:

a) **Ownership of Data/ process:** Data resides at the Data Centre. Establish clear ownership.

b) **Authorization process:** Anybody with access to the CBS, including the customer himself, can enter data directly. What is the authorization process? If the process is not robust, it can lead to unauthorized access to the customer information.

c) **Authentication procedures:** Usernames and Passwords, Personal Identification Number (PIN), One Time Password (OTP) are some of the most commonly used authentication methods. However, these may be inadequate and hence the user entering the transaction may not be determinable or traceable.

d) **Several software interfaces across diverse networks**: A Data Centre can have as many as 75-100 different interfaces and application software. A data centre must also contain adequate infrastructure, such as power distribution and supplemental power subsystems, including electrical switching; uninterruptable power supplies; backup generators and so on. Lapse in any of these may lead to real-time data loss.

e) **Maintaining response time:** Maintaining the interfacing software and ensuring optimum response time and up time can be challenging.

f) **User Identity Management:** This could be a serious issue. Some Banks may have more than 5000 users interacting with the CBS at once.

g) **Access Controls**: Designing and monitoring access control is an extremely challenging task. Bank environments are subject to all types of attacks; thus, a strong access control system is a crucial part of a bank's

overall security plan. Access control, however, does vary between branch networks and head office locations.

h) Incident handling procedures: Incident handling procedures are used to address and manage the aftermath of a security breach or cyberattack. However, these at times, may not be adequate considering the need for real-time risk management.

i) Change Management: Though Change management reduces the risk that a new system or other change will be rejected by the users; however, at the same time, it requires changes at application level and data level of the database- Master files, transaction files and reporting software.

26. What is the sub–processes of "Information Security"? List a few risks and related controls?

In a CBS, "Information Security" includes the following sub– processes:

(a) Policies, Procedures, and Practices: This refers to the processes relating to approval and implementation of Information Security. These cover all key areas of securing information at various layers of information processing.

(b) User Security Administration: This refers to security for various Users of IT Systems, and covers how Users are created and granted access as per the Bank's Organization Structure and Access Matrix. User Security Administration ranges from creation to disabling of Users.

(c) Application Security: This refers to how security is implemented at various aspects of application. It covers configuration, setting of parameters and security for transactions through various Application Controls.

(d) Database Security: This refers to various aspects of implementing security for the Database Software.

(e) Operating System Security: This refers to the security for Operating System Software which is installed in the Servers, and the Systems which are connected to the Servers.

(f) Network Security: This refers to security at various layers of Network and Connectivity to the Servers.

(g) Physical Security: This refers to security implemented through Physical Access Controls.

Risks and related Controls relating to Information Security are as under –

Risks	Key IT control
1) Significant information resources may be modified inappropriately, disclosed without authorization, and/or	Super user access or administrator passwords are changed on system, installation and are available with administrator only. Password of super use or administrator is adequately protected.

unavailable when needed.	
2) Lack of management direction and commitment to protect information assets.	Security policies are established and management monitors compliance with policies.
3) Potential Loss of confidentiality, availability and integrity of data and system.	Vendor default passwords for applications systems, operating system, databases, and network and communication software are appropriately modified, eliminated, or disabled.
4) User accountability is not established.	All users are required to have a unique user id.
5) Security breaches may go undetected.	Access to sensitive data is logged and the logs are regularly reviewed by management.
6) Potential loss of confidentiality, availability and integrity of data and system	Physical access restrictions are implemented and administered to ensure that only authorized individuals can access or use information resources.

27. Write short notes on Application Software Controls in a CBS.

CBS, some Risks and related Controls relating to Application Software are as under –

Risks	**Key IT control**
1) Interest may be incorrectly computed leading to incorrect recording of income/expenditure.	Interest is automatically correctly computed. Digits are rounded off appropriately. Interest is accurately accrued.
2) Inappropriate assignment of rate codes resulting in violation of business rules and/ or loss of revenue.	The interest rate code is defaulted at the account level and can be modified to a rate code carrying a higher or lower rate of interest only based on adequate approvals.
3) Absence of appropriate system validations may result in violation of business rules.	System validations have been implemented to restrict set up of duplicate customer master records.
4) Inappropriate reversal of charges resulting in loss of revenue.	System does not permit reversal of the charges in excess of the original amount charged.
5) Multiple liens in excess of	System prevents a single lien from

the deposit value may result in inability to recover the outstanding in the event of adefault.	exceeding the deposit value. It prevents marking of multiple liens against the same deposit, thus preventing the total liens exceeding the deposit account.
6) Inappropriate security or controls over system parameter settings resulting in unauthorized or incorrect changes to settings.	Access for changes made to the configuration, parameter settings is restricted to authorized user and require authorization/ verification from another user.

28. Explain the process of Money Laundering.

Money Laundering is the process used by Criminals, by which the proceeds of crime is concealed and layered through multiple banking transactions, so that they appear to come from a legitimate source.

Stages of Money Laundering:

1) Placement:

- Proceeds derived from illegal activities are "placed" into the system. This means the movement of proceeds (e.g. Currency), from the scene of the crime to a place, or into a form, less suspicious and more convenient for the Criminal.

2) Layering:

- Layering involves sending the illegal money through various complex financial transactions, to change its form and make it difficult to track.
- This involves the use of several Shell Corporations, namesake "Charities", Offshore Banks, Countries with loose regulation and secrecy laws, and multiple Bank Transfers between different accounts in different names in different countries.
- Transactions (Deposits and Withdrawals) are made in varying amounts in various accounts, in various currencies, to change the form of "dirty" money, to obscure the audit trail, thus making it hard to trace. It also involves the purchase of Luxury Assets and Financial Instruments.

3) Integration:

- Integration involves conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations.
- Integration of the "cleaned" money into the economy is accomplished by the Launderer making it appear to have been legally earned. By this stage, it is exceedingly difficult to distinguish legal and illegal wealth.

- Examples: Fictitious "Export" Invoices, obtaining Domestic Loan against a Foreign Deposit, Purchasing of Property, Luxury Assets and complex Financial Instruments, etc.

29. Briefly describe the provisions of the Prevention of Money Laundering Act, in the context of Banks?

- Money–Laundering has the meaning assigned u/s 3 which provides as– Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in, any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property, shall be guilty of offence of Money–Laundering.
- Punishment will give under section 4 as follow- Whoever commits the offence of Money–Laundering shall be punishable with Rigorous imprisonment for a Minimum 3 years, Maximum 7 years and Fine.

30. Briefly describe the impact of Cybercrimes, in the context of Banks.

Cybercrime or Computer Crime involves use of a Computer and a Network. Cybercrimes are offences that are committed against Individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern Telecommunication Networks like Internet (Chatrooms, email, Notice Boards and Groups) and Mobile Phones.

Impact on Banking Sector: Banking Sector is prone to high risks by Cyber Criminals, since Banks deal with money. In modern technology, Frauds can be committed across geographical boundaries without leaving a trace. Hence, CBS / Banking Software should have high level of controls covering all aspects of Cyber Security.

Cyber–related Offences: The Information Technology Act, 2000 contains punishments in respect of various Cyber–related offences. The Act exposes Banks to both civil and criminal liability in case of non–compliance.

31. Write short notes on Sensitive Personal Data or Information, in the context of Banks.

Personal Information means any information that relates to a Natural Person, which, either directly or indirectly, in combination with other information available or likely to be available with a Body Corporate, is capable of identifying such person.

Sensitive Personal Data or Information (SPDI) of a Person means such Personal Information which consists of information relating to –

(a) Password,
(b) Financial Information such as Bank Account or Credit Card or Debit Card or other payment instrument details,
(c) Physical, Physiological and Mental Health Condition,
(d) Sexual Orientation,

(e) Medical Records and History,
(f) Biometric Information,
(g) Any detail relating to the above Clauses as provided to Body Corporate for providing service, and
(h) Any of the information received under above Clauses by Body Corporate for processing, stored or processed under lawful contract or otherwise.

Duties of Banks:

- To develop and properly communicate the "Bank's Privacy Policy",
- To establish managerial, technical, operational and physical security control measures that are commensurate with the Information Assets being protected with the nature of business,
- To train Employees in the proper handling of Personal Information,
- To enter into proper SLAs with Vendors for maintaining confidentiality of SPDI, in case of outsourced activities,
- To demonstrate that they have implemented security control measures as per their documented Information
- Security Programme and Information Security Policies, in the event of an Information Security Breach, etc.

32. Write short notes on Cyber Crime.

Cybercrimes is defined as: 'Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones.
Cybercrime also known as computer crime is a crime that involves use of a computer and a network. The computer may have been used in committing a crime, or it may be the target.
The United Nations Manual on the Prevention and Control of Computer Related Crime classifies such crimes into following categories:

- Committing of a fraud by manipulation of the input, output, or throughput of a computer-based system.
- Computer forgery, which involves changing images or data stored in computers,
- Deliberate damage caused to computer data or programs through virus programs or logic bombs,
- Unauthorized access to computers by 'hacking' into systems or stealing passwords, and,
- Unauthorized reproduction of computer programs or software piracy.
- Cybercrimes have grown big with some countries promoting it to attack another country's security and financial health.

33. What are the objectives of the Information Technology Act?

The objectives of the Act are –

1) To grant legal recognition for electronic commerce in place of paper-based methods of communication and storage of information. Electronic Commerce means the transactions carried out by means of Electronic Data Interchange and other means of electronic communication.
2) To give legal recognition to Digital Signature for authentication of any information or matter, which requires authentication under any law.
3) To provide for a regulatory regime to supervise the Certifying Authorities issuing Digital Signature Certificates.
4) To facilitate e–governance and electronic filing of documents with Government departments.
5) To facilitate and give legal sanction to Electronic Fund Transfers between Banks and Financial Institutions by amending the Reserve Bank of India Act, 1934.
6) To give legal recognition for keeping books of account by Bankers in electronic form by amending the Bankers' Book Evidence Act, 1891.
7) To provide for dealing with offences relating to electronic documents by amending the Indian Penal Code and the Indian Evidence Act, 1872.

34. List some important definitions in the Information Technology Act.

1) **Section 2(a)** "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
2) **Section 2(i)** "Computer" means any electronic, magnetic, optical or other high- speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
3) **Section 2(j)** "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
   i. the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
   ii. terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;
4) **Section 2(o)** "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic

or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

5) **Section 2(v)** "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer-generated micro fiche;

35. Write short notes on various damages to Computer System or Network u/s 43.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

a) accesses or secures access to such computer, computer system or computer network;
b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;
e) disrupts or causes disruption of any computer, computer system or computer network;
f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

36. Write short notes on Penalties & Adjudications under Chapter X of Information Technology Act.

Section 63. Punishment for false information or failure to give information, etc.

- Any person wilfully and maliciously giving false information and so causing an arrest or a search to be made under this Act shall on conviction be liable for imprisonment for a term which may extend to two years or with fine which may extend to fifty thousand rupees or both.
- If any person -
  a. being legally bound to state the truth of any matter relating to an offence under section 3, refuses to answer any question put to him by an authority in the exercise of its powers under this Act; or
  b. refuses to sign any statement made by him in the course of any proceedings under this Act, which an authority may legally require to sign; or
  c. to whom a summon is issued under section 50 either to attend to give evidence or produce books of account or other documents at a certain

place and time, omits to attend or produce books of account or documents at the place or time,

he shall pay, by way of penalty, a sum which shall not be less than five hundred rupees but which may extend to ten thousand rupees for each such default or failure.

Section 70. Offences by companies.

- Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to the company, for the conduct of the business of the company as well as the company, shall be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

  Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
- Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of any company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

37. Describe the 'Tampering with Computer Source Documents' u/s 65 of Information Technology Act 2000?

Offence:

- Knowingly or intentionally concealing, destroying or altering, or causes to conceal, destroy or alter any computer source code. Computer Source Code means the listing of programmes, computer commands, design & layout & programme analysis of computer resource in any form.

Penalty:

- Imprisonment up to 3 years, or
- Fine up to ₹2,00,000, or
- Both.

38. Briefly explain the following with respect to the Information Technology Act 2000:

[Section 66B] Punishment for dishonestly receiving stolen Computer Resource or Communication Device:

Offence:

- Dishonestly receiving or retaining any stolen Computer Resource or Communication Device knowing or having reason to believe the same to be stolen Computer Resource or Communication Device.

Penalty:

- Imprisonment up to three years, or
- Fine up to ₹1,00,000, or
- Both.

[Section 66C] Punishment for Identity Theft:

Offence:

- Fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person, shall be punished.

Penalty:

- Imprisonment up to 3 years **and** Fine up to ₹1,00,000.

[Section 66D] Punishment for cheating by Personation by using Computer Resource:

Offence:

- By means for any Communication Device or Computer Resource cheats by personating.

Penalty:

- Imprisonment up to 3 years **and** Fine up to ₹1,00,000.

[Section 66E] Punishment for Violation of Privacy:

Offence:

- Intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person.

Penalty:

- Imprisonment up to 3 years, or
- Fine up to ₹2,00,000, or
- Both.

Our Approach

We go to great lengths to ensure that we deliver a quality learning experience to our students. Right from pedagogy design to faculty selection, video recording and animation, at every stage our goal is to ensure that the final output is the BEST and it meets the requirements of the learners. It is our laser sharp focus on maintaining HIGH QUALITY and setting new benchmarks in the CA education domain, that make our efforts stand out and help our students to succeed in their examinations.

A Glimpse of our e-learning modules

START LEARNING TODAY

1 Go to https://www.indigolearn.com and click on Sign Up
2 Choose your courses & pay online
3 Start Learning Instantly

GET IT ON Google Play

Download our APP 1FIN

IndigoLearn

https://www.indigolearn.com | support@indigolearn.com | +91 9640 11111 0