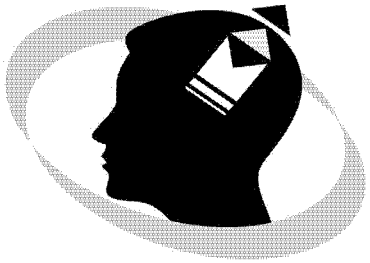
CA - INTER
COURSE MATERIAL

Quality Education
beyond your imagination...

SUBJECT CODE: 7A, MATERIAL NO: 36
FAST TRACK MATERIAL ON
ENTERPRISE INFORMATION SYSTEMS _39e



MASTER MINDS™

CA • CMA • CS • MEC • CEC

GUNTUR | RAJAHMUNDRY | KURNOOL | VIZAG | NELLORE

HYDERABAD | VIJAYAWADA | TIRUPATHI

Cell: 98851 25025 / 26

Visit us @ www.mastermindsindia.com | Mail: mastermindsinfo@ymail.com

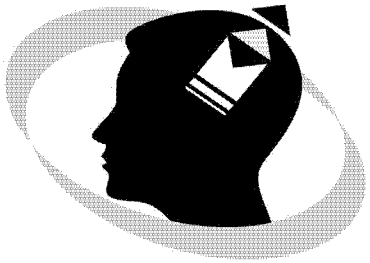
Facebook Page: Masterminds For CA | Youtube Channel: Masterminds For CA

INDEX

CA - INTER
COURSE MATERIAL

Quality Education
beyond your imagination...

PART A – CLASSNOTES



MASTER MINDS

CA • CMA • CS • MEC • CEC

GUNTUR | RAJAHMUNDRY | KURNOOL | VIZAG | NELLORE

HYDERABAD | VIJAYAWADA | TIRUPATHI

Cell: 98851 25025 / 26

Visit us @ www.mastermindsindia.com | Mail: mastermindsinfo@ymail.com

Facebook Page: Masterminds For CA | Youtube Channel: Masterminds For CA

1. AUTOMATED BUSINESS PROCESSES

ENTERPRISE BUSINESS PROCESSES

Q.No.1. Define Business Processes? What are the Categories of Business Processes?

Business Process: A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal.

Categories of Business Processes:

1. Operational Processes
2. Supporting Processes
3. Management Processes

Q.No.2. What is the difference between Operational Processes, Supporting Processes and Management Processes? (Or) Define the terms Operational Processes, Supporting Processes and Management Processes?

1. **OPERATIONAL PROCESSES (OR PRIMARY PROCESSES):** These processes deliver value to the customer by helping to produce a product or service. *Examples: Generating revenue - Order to Cash cycle, Procurement - Purchase to Pay cycle.*
2. **SUPPORTING PROCESSES (OR SECONDARY PROCESSES):** Supporting Processes back core processes and functions within an organization. One key differentiator between operational and support processes is that support processes do not provide value to customers directly.
   Examples: Accounting, Human Resource (HR) Management .
3. **MANAGEMENT PROCESSES:** Management processes measure, monitor and control activities related to business procedures and systems. Like supporting processes, management processes do not provide value directly to the customers. *Examples: internal communications, governance, strategic planning, budgeting.*

AUTOMATED BUSINESS PROCESSES

Q.No.3. Define the term Business Process Automation? Explain its objectives?

Business Process Automation (BPA):

a) It can be defined as removing the human element from existing business processes by automating the repetitive or standardized process components.

b) In other words, BPA is the tactic, that helps the business to automate processes to operate efficiently and effectively.

OBJECTIVES OF BPA:

- **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.

Q.No.4. Explain Benefits of Automating Business Process?

BENEFITS OF AUTOMATING BUSINESS PROCESS:

1. **Quality & Consistency:** Ensures that every action is performed identically - resulting in high quality, reliable results.

2. **Time Saving:**
   a) Automation reduces the number of tasks employees would otherwise need to do manually.
   b) It frees up time to work on items that add genuine value to the business.
3. **Visibility:** Automated processes are controlled and consistently operate accurately within the defined timeline. It gives visibility of the process status to the organisation.
4. **Improved Operational efficiency:**
   a) Automation reduces the time it takes to achieve a task.
5. **Governance & Reliability:** The consistency of automated processes means stakeholders can rely on business processes to operate and offer reliable processes to customers, maintaining a competitive advantage.
6. **Reduced Turnaround Times:** Eliminate unnecessary tasks and realign process steps to optimize the flow of information throughout production, service, billing and collection. This reduces the turnaround times for both staff and external customers.
7. **Reduced Costs:** Manual tasks, given that they are performed one-at-a-time and at a slower rate than an automated task, will cost more.

Q.No.5. What are the steps to be taken while implementing Business Process Automation?

Step 1: Define why we plan to implement a BPA: The primary purpose for which an enterprise implements automation may vary from enterprise to enterprise.

Step 2: Understand the rules / regulation under which enterprise needs to comply with: understand the rules of engagement, which include the rules, adhering to regulations and document retention requirements.

Step 3: Document the process, we wish to automate: At this step, all the documents that are currently being used need to be documented.

Step 4: Define the objectives/goals to be achieved by implementing BPA: Once the above steps have been completed, entity needs to determine the key objectives of the process improvement activities.

Step 5: Engage the business process consultant: To achieve BPA, decide which company/ consultant to partner with.

Step 6: Calculate the RoI for project: The right stakeholders need to be engaged and involved to ensure that the benefits of BPA are clearly communicated and implementation becomes successful.

Step 7: Developing the BPA: the consultant develops the requisite BPA.

Step 8: Testing the BPA: Once developed, it is important to test the new process to determine how well it works.

ENTERPRISE RISK MANAGEMENT

Q.No.6. Define the term Enterprise Risk Management? Write short notes on ERM?

Enterprise Risk Management (ERM):

It may be defined as a process, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

1. The primary objective of Enterprise Risk Management (ERM) is that every entity, whether for profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders.
2. ERM provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

3. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

Q.No.7. What are the Benefits of Enterprise Risk Management?

Benefits of ERM are:

1. **Align risk appetite and strategy:** Risk appetite is the degree of risk, Management considers the entity's risk appetite first in evaluating strategic alternatives.
2. **Link growth, risk and return:** ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
3. **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses - risk avoidance, reduction, sharing and acceptance.
4. **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.
5. **Identify and manage cross-enterprise risks:** Management needs to not only manage individual risks, but also understand interrelated impacts.
6. **Provide integrated responses to multiple risks:** Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.

Q.No.8. Explain the Components of Enterprise Risk Management?

Components of ERM are:

1. **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.
2. **Objective Setting:** 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 .
3. **Event Identification:** Potential events that might have an impact on the entity should be identified.
4. **Risk Assessment:** Identified risks are analyzed to form a basis for determining how they should be managed.
5. **Risk Response:** Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.
6. **Control Activities:** Policies and procedures are established and executed to help ensure that the risk responses management selected are effectively carried out.
7. **Information and Communication:** Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective communication also should occur in a broader sense, flowing down, across and up the entity.

A. **Monitoring:** The entire ERM process should be monitored, and modifications made as necessary.

Q.No.9. Explain the Framework of Enterprise Risk Management?

Framework of ERM:

1. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.

2. Management selects a risk response strategy for specific risks identified and analyzed, which may include:
   i) **Avoidance:** exiting the activities giving rise to risk.
   ii) **Reduction:** taking action to reduce the likelihood or impact related to the risk.
   iii) **Alternative Actions:** deciding and considering other feasible steps to minimize risks.
   iv) **Share or Insure:** transferring or sharing a portion of the risk, to finance it.
   v) **Accept:** no action is taken, due to a cost/benefit decision.

RISKS

Q.No.10. Define the term RISK? Explain Different types of Risks in Business Process Automation?

RISK:

As per International Organization for Standardization (ISO): **Risk** is uncertainty in achieving objectives. Risk can be positive or negative.

RISKS OF BUSINESS PROCESS AUTOMATION:

a) **Input & Access:** All input transaction data may not be accurate, complete and authorized.
b) **File & Data Transmission:** All files and data transmitted may not be processed accurately and completely, due to network error.
c) **Processing:** Valid input data may not have been processed accurately and completely due to program error or bugs.
d) **Output:** Is not complete and accurate due to program error or bugs and is distributed to unauthorized personnel due to weak access control.
e) **Data:** Master data and transaction data may be changed by unauthorized personnel due to weak access control.
f) **Infrastructure:** All data & programs could be lost if there is no proper backup in the event of a disaster and the business could come to a standstill.

Q.No.11. Explain Different types of Business Risks?

TYPES OF BUSINESS RISKS:

a) **Strategic:** Risk that would prevent an organization from accomplishing its objectives (meeting its goals).
b) **Financial:** Risk that could result in a negative financial impact to the organization (waste or loss of assets).
c) **Regulatory (Compliance):** Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.
d) **Reputational:** Risk that could expose the organization to negative publicity.
e) **Operational:** Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations.

CONTROLS in BPA

Q.No.12. Write about CONTROLS in BPA? Discuss the terms Internal Controls & Internal Control systems as per SA-315?

Control: It 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.

1. INTERNAL CONTROL as per SA-315:
   a) **Internal Controls** are a system consisting of specific policies and procedures designed to provide management with reasonable assurance that the goals and objectives it believes important to the entity will be met.
   b) "**Internal Control System**" means all the policies and procedures adopted by the management of an entity to assist in achieving management's objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud
2. EFFECTIVE INTERNAL CONTROL:
   a) The control environment sets the tone of an organization, influencing the control consciousness of its people.
   b) The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's internal control and its importance in the entity.
   c) Evaluating the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements.

Q.No.13. Discuss the Components of Internal Controls, as per SA315?

The five components are as follows:

1. CONTROL ENVIRONMENT: The Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.
2. RISK ASSESSMENT: Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.
3. CONTROL ACTIVITIES: Control Activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
   a) **Segregation of Duties (SOD)** is the process of assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets.
   b) **General Controls** apply to all systems - from mainframe to client/server to desktop computing environments.
   c) **Application Controls** are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing.
4. INFORMATION & COMMUNICATION:
   a) **Information** is necessary for the entity to carry out internal control responsibilities in support of the achievement of its objectives.
   b) **Communication** is the continual, iterative process of providing, sharing, and obtaining necessary information.
5. MONITORING OF CONTROLS: Ongoing evaluations, separate evaluations, or combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component is present and functioning.

Q.No.14. Explain the Limitations of Internal Control System?

Internal control systems are subject to certain inherent limitations, such as:

a) Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.

b) The possibility of circumvention of internal controls through collusion with employees or with parties outside the entity.

c) The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.

d) Manipulations by management with respect to transactions or estimates and judgments required in the preparation of financial statements.

DIAGRAMMATIC REPRESENTATION OF BUSINESS PROCESSES

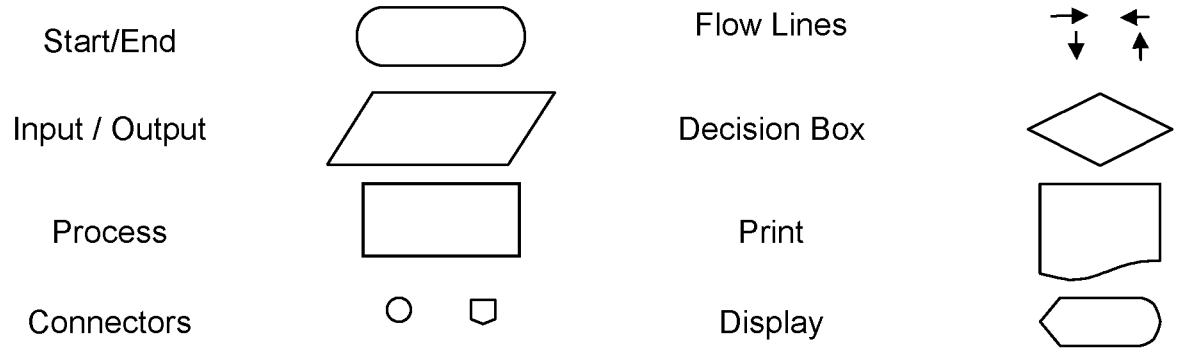
Q.No.15. Discuss the concept of Flowcharts?

INTRODUCTION TO FLOWCHARTS:

1. A Flowchart is a diagram prepared by the programmer of the sequence of steps involved in solving a problem.
2. It is an essential tool for programming and illustrates the strategy and thread of logic followed in the program.
3. A flowchart helps the programmer avoid fuzzy thinking and accidental omissions of intermediate steps.
4. They help visualize what is going on and thereby help understand a process, and perhaps also find flaws, bottlenecks, and other less-obvious features within it.
5. Flowcharts may be divided into

Types of Flowchart	Explanation
Document Flowchart	This flowchart traces the physical flow of documents through an organization – that is, the flow of documents from the departments, groups, or individuals who first created them to their final destinations.
System Flowchart	This typically depicts the electronic flow of data and processing steps in an Information System. While Document Flowcharts focus on tangible documents, system flowchart concentrates on the computerized data flows of Information systems.
Program Flowchart	It is most detailed and is concerned with the logical/arithmetic operations on data within the CPU and the flow of data between the CPU on the one hand and the input/output peripherals on the other.

FLOWCHART SYMBOLS:



Q.No.16. Discuss Advantages of Flowcharting?

ADVANTAGES OF FLOWCHARTS:

a) **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.

b) **Effective Analysis:** 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.

c) **Communication:** Flowcharts aid in communicating the facts of a business problem to those whose skills are needed for arriving at the solution.

d) **Documentation:** Flowcharts serve as a good documentation which aid greatly in **future** program conversions.

e) **Efficient coding:** Instructions coded in a programming language may be checked against the flowchart to ensure that no steps are omitted.

f) **Program Debugging:** They help in detecting, locating and removing mistakes.

g) **Efficient program maintenance:** The charts help the programmer to concentrate attention on that part of the information flow which is to be modified.

Q.No.17. Discuss Limitations of Flowcharting ?

LIMITATIONS OF FLOWCHART:

a) **Complex logic:** Flowchart becomes complex and clumsy where the problem logic is complex.

b) **Modification:** If modifications to a flowchart are required, it may require complete re-drawing.

c) **Reproduction:** Reproduction of flowcharts is often a problem because the symbols used in flowcharts cannot be typed.

d) **Link between conditions and actions:** Sometimes it becomes difficult to establish the linkage between various conditions and the actions to be taken.

e) **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.

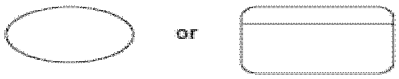
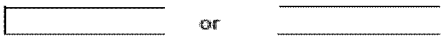
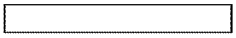
Q.No.18. Explain about Data Flow Diagrams (DFDs)? Explain Major components of DFD? Explain the concept of DFD with some example?

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

MAJOR COMPONENTS OF DFD:

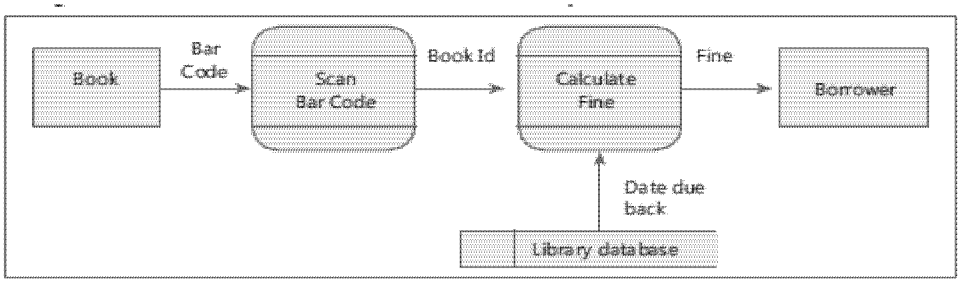
1. **Entity:**
   a) An *entity is* the source or destination of data.
   b) Entities are often represented as rectangles.
2. **Process:**
   a) The process is the manipulation or work that transforms data, performing computations, making decisions (logic flow), or directing data flows based on business rules.
   b) *In other words, a process receives input and generates some output.* Processes can be drawn as circles or a segmented rectangle on a DFD,
3. **Data Store:**
   a) A data store is where a process stores data between processes for later retrieval by that same process or another one. Files and tables are considered data stores.
   b) Data stores are usually drawn as a rectangle with the right hand side missing
4. **Data Flow:**
   a) Data flow is the movement of data between the entity, the process and the data store.
   b) Data flow is represented by an arrow, where the arrow is annotated with the data name.

MAIN SYMBOLS:

Meaning	Symbols
Process	
Data Store	
Entity	
Data Flow	

Example

Given below Fig. is a simple scenario depicting a book borrowed from a library being returned and the fine calculated, due to delay?



- The book is represented as an external entity and the input is the bar code.
- The process is the scanning of the bar code and giving an output of the Book ID.
- The next process calculates the fine based on accessing the "library database" and establishing the "due back" date.
- Finally, the fine is communicated to the borrower who is also shown as an external entity.

RISKS & CONTROLS FOR SPECIFIC BUSINESS PROCESSES

Q.No.19. How CONTROLS for specific business processes could be implemented?

BUSINESS PROCESSES - CONTROLS: In computer systems, controls should be checked at three levels, namely Configuration, Master & Transaction level.

1. **Configuration:** Configuration is the methodical process of defining options that are provided. Configuration will define how software will function and what menu options are displayed.

   Some examples are given below:

   Control on parameters: Creation of Customer Type, Vendor Type, year-end process

2. **Masters:** **Masters** refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory, Finance etc. The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed.

   Some examples are given here:

   a) **Vendor Master:** Credit period, vendor bank account details, etc.

   b) **Customer Master:** Credit limit, Bill to address, Ship to address, etc.

3. **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.

   For example:

   a) Sales transactions

   b) Purchase transactions

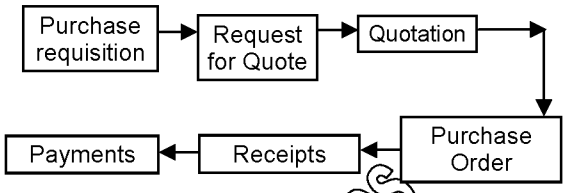
   c) Stock transfer transactions

Q.No.20. Discuss Procure to Pay (P2P) life cycle in detail? How Risks and Controls are implemented for P2P Transactions?

Procure to Pay (Purchase to Pay or P2P) is the process of obtaining and managing the raw materials needed for manufacturing a product or providing a service.

PROCURE TO PAY (P2P) LIFE CYCLE:

a) **Purchase requisition:** A document is prepared requesting the purchase department to place an order with the vendor specifying the quantity and time frame.
b) **Request for quote:** An invitation is sent to the vendors to join a bidding process for specific products.
c) **Quotation:** The vendors provide cost quotations for the supply of products.
d) **Purchase order:** A commercial document is issued to the vendor specifying the type, quantity and agreed prices for products.
e) **Receipts:** The physical receipt of goods and invoices.
f) **Payments:** The payments are made against the invoices.



Procure to Pay (P2P) - Risks and Controls:

Masters:

Risks and Control Objectives (Masters-P2P)

Risk	Control Objective
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.

Transactions:

Risks and Control Objectives (Transactions - P2P)

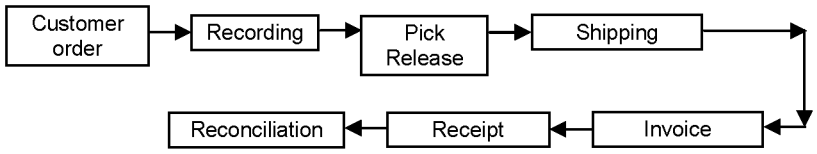
Risk	Control Objective
Unauthorized purchase requisitions are ordered.	Purchase orders are placed only for approved requisitions.
Purchase orders are not entered correctly in the system.	Purchase orders are accurately entered.
Amounts are posted in accounts payable for goods or services not received.	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.

Q.No.21. Discuss Order to Cash (O2C) life cycle in detail? How Risks and Controls are implemented for O2C Transactions?

a) **Order to Cash (OTC or O2C) is a set of business processes that involve receiving and** fulfilling customer requests for goods or services.

ORDER TO CASH (O2C) LIFE CYCLE:

a) **Customer Order:** A purchase order received from a customer specifying the type, quantity and agreed prices for products.
b) **Recording:** Availability of the items is checked and customer order is booked.
c) **Pick release:** The items are moved from the warehouse to the staging area.
d) **Shipping:** The items are loaded onto the carrier for transport to the customer.
e) **Invoice:** Invoice of the transaction is generated and sent to the customer.
f) **Receipt:** Money is received from the customer against the invoices.
g) **Reconciliation:** The bank reconciliation of all the receipts is performed.



Order to Cash (O2C) - Risks and Controls:

Masters:

Risks and Control Objectives (Masters-O2C)

Risk	Control Objective
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.

Transactions:

Risks and Control Objectives (Transactions-O2C)

Risk	Control Objective
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 sale.	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.

Q.No.22. Discuss Inventory Cycle in detail? How Risks and Controls are implemented?

The **Inventory Cycle** is a process of accurately tracking the on-hand inventory levels for an enterprise. An inventory system should maintain accurate record of all stock movements to calculate the correct balance of inventory.

PHASES OF THE INVENTORY CYCLE FOR MANUFACTURERS:

1. **Ordering phase:** The amount of time it takes to order and receive raw materials.
2. **Production phase:** The work in progress phase relates to time it takes to convert the raw material to finished goods ready for use by customer.
3. **Finished goods and delivery phase:** The finished goods that remain in stock and the delivery time to the customer. The inventory cycle is measured in number of days.

INVENTORY CYCLE - RISKS AND CONTROLS:

Masters:

Risks and Control Objectives (Masters-Inventory)

Risk	Control Objective
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.

Transactions:

Risks and Control Objectives (Transactions-Inventory)

Risk	Control Objective
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.
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.

Q.No.23. Discuss Human Resources cycle in detail? How Risks and Controls are implemented?

The **Human Resources** 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:

1. **Recruiting and on-boarding:** Recruiting is the process of hiring a new employee. On boarding is the process of getting the successful applicant set up in the system as a new employee.
2. **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. Career planning is the stage at which the employee and her supervisors work out her long-term career goals with the company.
3. **Career Development:** 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.
4. **Termination or Transition:** Some employees will leave a company through retirement after a long and successful career. The role of HR in this process is to manage the transition by ensuring that all policies and procedures are followed.

HUMAN RESOURCES - RISKS AND CONTROLS:

Configuration:

Risks and Control Objectives (Configuration-Human Resources)

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.

Masters:

Risks and Control Objectives (Masters-Human Resources)

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.

Q.No.24. Discuss the Advantages of Cyber Laws?

ADVANTAGES OF CYBER LAWS:

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects which are as follows:

a) 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.

b) Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

c) Digital signatures have been given legal validity and sanction in the Act.

d) The Act now allows Government to issue notification on the web thus heralding e-governance.

e) 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.

Q.No.25. Give some examples of Common Cyber-crime scenarios that can be prosecuted under the IT Act 2000 (amended via 2008)?

Examples of Common Cyber-crime scenarios:

a) **Harassment via fake public profile on social networking site:** A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labeled as person of 'loose character'. This leads to harassment of the victim.

b) **Email Account Hacking:** If victim's email account is hacked and obscene emails are sent to people in victim's address book.

c) **Credit Card Fraud:** Unsuspecting victims would use infected computers to make online transactions.

d) **Web Defacement:** The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.

e) **Cyber Terrorism:** Many terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.

f) **Online sale of illegal Articles:** Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet.

g) **Phishing and Email Scams:** Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity (e.g. Passwords, credit card information).

Q.No.26. Discuss the term Privacy that can be prosecuted under the IT Act 2000?

The main principles on data protection and privacy enumerated under the IT Act, 2000 are:

a) Defining 'data', 'computer database', 'information', 'electronic form', 'originator', 'addressee' etc.

b) Creating civil liability if any person accesses or secures access to computer, computer system or computer network

c) Creating criminal liability if any person accesses or secures access to computer, computer system or computer network

d) Declaring any computer, computer system or computer network as a protected system

e) Imposing penalty for breach of confidentiality and privacy

Q.No.27. Discuss the term Cybercrime that can be prosecuted under the IT Act 2000?

1. Cybercrime also known as computer crime is a crime that involves use of a computer and a network.
2. 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.
3. The United Nations Manual on the Prevention and Control of Computer Related Crime classifies such crimes into following categories:
   - **a)** Committing of a fraud by manipulation of the input, output, or throughput of a computer based system.
   - **b)** Computer forgery, which involves changing images or data stored in computers,
   - **c)** Deliberate damage caused to computer data or programs through virus programs or logic bombs,
   - **d)** Unauthorized access to computers by 'hacking' into systems or stealing passwords.

Q.No.28. Discuss the key terms regarding IT Act, 2000 (as amended in 2008)?

The IT Act, 2000 defines the terms that are useful to technically understand the concept of Cyber Crime.

DEFINITIONS:

1. "**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. "**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. "**Computer Network**" means the interconnection of one or more Computers or Computer **systems** or Communication device through-The use of satellite, microwave, terrestrial line, wire, wireless or other communication media;
4. "**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. "**Information**" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

Q.No.29. Discuss the term Sensitive Personal Data Information regarding IT Act, 2000?

1. **Sensitive Personal Data Information (SPDI):** Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under section 43A of the Information Technology Act 2000 define a data protection framework for the processing of digital data by Body Corporate.
2. **Scope of Rules:** Currently the Rules apply to Body Corporate and digital data. As per the IT Act, Body Corporate is defined as "Any company and includes a firm, sole proprietorship engaged in commercial or professional activities."
3. **Definition of Personal and Sensitive Personal data:** Rule 2(i) defines personal information as "information that relates to a natural person which likely to be available with a body corporate, is capable of identifying such person."

   Rule 3 defines sensitive personal information as:

   a) *Passwords*

   b) *Financial information*

   c) *Physical/physiological/mental health condition*

   d) *Biometric information*
4. **Consent:** Rule 5(1) requires that Body Corporate should, prior to collection, obtain consent in writing through letter or fax or email from the provider of sensitive personal data regarding the use of that data.

2. FINANCIAL AND ACCOUNTING SYSTEMS

INTRODUCTION

Q.No.1. What is a System? Define the terms INTEGRATED (ERP) and NON-INTEGRATED Systems?

1. The word "system" can be explained as, "a set of detailed methods, procedures and routines created to carry out a specific activity, perform a duty, or solve a problem".
2. An **Integrated System** that has combined different functions together in order to work as one entity and maintaining data in a centralized manner.
3. A **Non-Integrated System** is a system of maintaining data in a decentralized way. In case of non-integrated systems, separate database is maintained by each department separately.

Q.No.2. Discuss the features of Master Data and Non-Master Data?

Every accounting systems stores data in two ways: Master Data and Non-Master Data

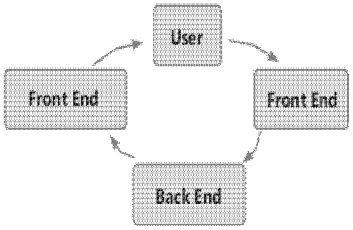
1. MASTER DATA:
   - **a)** Relatively permanent data not expected to change frequently.
   - **b)** Master data is generally not typed by the user, it is selected from the available list.
   - **c)** Master data entry is usually done less frequently say once a year or when there is a need to update.
   - ***d)*** *Eg.:* ***Accounting Master Data, Inventory Master Data, Payroll Master Data, Statutory Master Data***

2. NON-MASTER DATA:
   a) Non-permanent data and expected to change frequently. It is also called Transaction Data
   b) Non-master data is typed by the user and not selected from available list as it is a non-permanent and it keeps on changing again and again.
   c) *E.g.: Date recorded in each transaction is expected to change again and again and will not be constant in all the transactions.*

Q.No.3. Discuss the Working of any accounting software?

FRONT END & BACK END:

a) **Front End** - It is part of the overall software which actually interacts with the user who is using the software.
b) **Back End** - It is a part of the overall software which does not directly interact with the user, but interact with Front End only.



Working of any accounting software: If a user wants to have some information from the system, i.e. Balance Sheet.

a) User will interact with Front End part of the software and request front end to generate the report.
b) Front End will receive the instruction from user and pass it on to the back end.
c) Back End will process the data, generate the report and send it to the front end.
d) *Front end will now display the information to user.*
e) *This is how the process gets completed each and every time.*

Reasons for separating software in to parts like front end and back end

Function	Reason for Software usage
Domain Expertise	Front end software is meant for handling requests from users. Back end software is meant for storing and handling the data.
Presentation	Front end software interacting with a user is meant for presenting information in proper format, different colors, bold, italic letters, tables, charts, etc. Back end software is not meant for it.
User Experience	Front end software should guide a user to the desired report or feature.
Speed	Separate back end software is used for handling data only. This reduces the load and increases speed of operations.
Language	Back end speaks in technical language not understood by a layman. Front end can speak in languages such as user's language and technical language.

Q.No.4. Discuss the terms Installed Applications and Web Applications? And explain the advantages and disadvantages?

a) **Installed Applications** are programs installed on the hard disc of the user's computer.
b) **Web Applications** are installed on a web server and it is accessed using a browser and internet connection.

There are some advantages as well as disadvantages of both types of applications as discussed.

Particulars	Installed Application	Web Application
Installation & Maintenance	it needs to be installed on every computer one by one. Maintenance and updating of software may take lot time and efforts.	As software is installed on only one computer, i.e. on web server. Maintenance and updating of software becomes extremely easy.

Accessibility	As software is installed on the hard disc of the user's computer, It cannot be used from any computer.	it is used through browser and internet, it can be used from any computer in the world 24 x 7.
Mobile Application	Using the software through mobile application is difficult in this case.	Using mobile application becomes very easy as data is available 24 x 7.
Data Storage	Data is physically stored on the hard disc of the user's server. Hence user will have full control over the data.	Data is not stored in the user's server. It is stored on a web server. Hence user will not have any control over the data.
Data Security	user shall have the full physical control over the data and he/she can ensure that it is not accessed without proper access.	Data security is a big challenge in case of web application because It is maintained on a web server.
Performance	A well written installed application shall always be faster than web application.	As data is picked from web server using internet, speed of operation may be slower.
Flexibility	Installed applications shall have more flexibility and controls as compared to web application.	Web applications do not even compare to the flexibility of desktop applications.

Q.No.5. Discuss how Integrated Enterprise Resource Planning Systems support business?

1. An ERP system supports most of the business system that maintains in a single database the data needed for a variety of business functions such as Manufacturing, Supply Chain Management, Financials, Projects, Human Resources and Customer Relationship Management and Financial & Accounting Systems.
2. An ERP system is based on a common database and a modular software design.
3. The common database can allow every department of a business to store and retrieve information in real-time. The information should be reliable, accessible, and easily shared.
4. The modular software design should mean a business can select the modules they need, mix and match modules from different vendors, and add new modules of their own to improve business performance.
5. *Some of the well-known ERPs in the market today include SAP, Oracle, MFG Pro, MS Axapta etc.*

Q.No.6. Discuss the Advantages of an ERP System? Give some examples of Open Source ERP software?

a) Ability to customize an organization's requirements;
b) Integrate business operations with accounting and financial reporting functions;
c) Increased data security and application controls;
d) Build strong access and segregation of duties controls;
e) Automate many manual processes thus eliminating errors;
f) Process huge volumes of data within short time frames; and

Free and Open Source ERP software

S. No.	ERP Software	S. No.	ERP Software
1	Adempiere, a Java based ERP-System which started as a fork of Compiere	11	Open BlueLab
2	Compiere, a Java based ERP-System	12	Open bravo, a Java based ERP-System
3	Dolibarr, a PHP based ERP system	13	Open ERP (formerly Tiny ERP)
4	ERPS, a Python based ERP system	14	Open taps (Java based)

5	GNU Enterprise	**15**	Orange HRM
6	GRR (software), a PHP/MySQL - based, web- accessed free ERP system	**16**	Post books from XTuple
7	JFire, a Java based ERP-System from NightLabs	**17**	SQL-Ledger
8	Kuali Foundation	**18**	Stoq
9	LedgerSMB	**19**	Web ERP
10	OFBiz		

Q.No.7. Discuss the features of an Ideal ERP System?

1. An **Ideal ERP System** is that system which caters all types of needs of an organization and provides right data and right point of time to right users for their purpose.
2. These software modules can include the following:
   a) **Manufacturing:** Some of the functions include engineering, capacity, workflow management, quality control, bills of material, manufacturing process, etc.
   b) **Financials:** Accounts payable, accounts receivable, fixed assets, general ledger and cash management, etc.
   c) **Human Resources:** Benefits, training, payroll, time and attendance, etc.
   d) **Supply Chain Management:** Inventory, supply chain planning, supplier scheduling, claim processing, order entry, purchasing, etc.
   e) **Projects:** Costing, billing, activity management, time and expense, etc.
   f) **Customer Relationship Management (CRM):** The rationale behind this approach is to improve services provided directly to customers and to use the information in the system for targeted marketing.
   g) **Data Warehouse:** Data warehouse is a repository of an organization's electronically stored data. Data warehouses are designed to facilitate reporting and analysis.

RISKS AND CONTROLS

Q.No.9. Discuss several RISKS and CONTROLS of ERP Environment?

Risks and corresponding Controls

Aspect	Risk Associated	Control Required
Data Access	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.
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.
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.
Change in process	As the overall system is integrated, a small change in process for one department may require lot of efforts and money.	All the processes must be documented carefully in the beginning of implementation itself.
Staff Turnover	As the overall system is integrated and connected with each other department, it becomes complicated and difficult to understand.	This can be controlled and minimized with help of proper staff training system.

System Failure	As everybody is connected to a single system, 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.

Q.No.10. Discuss the terms RBAC and RAC controls in ERP?

a) **Role Based Access Control (RBAC)**

i) RBAC is sometimes referred to as Role-Based Security.

ii) It is a policy neutral access control mechanism defined around roles and privileges.

iii) The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.

iv) RBAC can be used in large organizations .

b) **Rules-based Access Control (RAC)**

i) RAC takes into account the data affected, the identity attempting to perform a task, and other triggers governed by business rules.

ii) RAC uses specific rules that indicate what can and cannot happen between a subject/ user and an object. A manager, for example, has the ability to approve his/her employees' hours worked.

iii) RAC can be used in small to medium sized organizations.

BUSINESS PROCESS MODULES AND THEIR INTEGRATION

Q.No.11. What is a Business Process? Explain how to manage a process.

1. **Business Process:** In the systems engineering arena, a **Process** is defined as a sequence of events that uses inputs to produce outputs.
   a) A Business Process consists of a set of activities that are performed in coordination in an organizational and technical environment.
2. To manage a process:
   a) The first task is to **define**. This involves defining the steps in the process.
   b) Once the process is mapped and implemented, **performance measures** can be established. Establishing measurements creates a basis to improve the process.
   c) The last piece describes the **organizational setup** that enables the standardization of and adherence to the process throughout the organization.

Q.No.12. Write about Human Resource Business Process Module of ERP?

HUMAN RESOURCE MODULE:

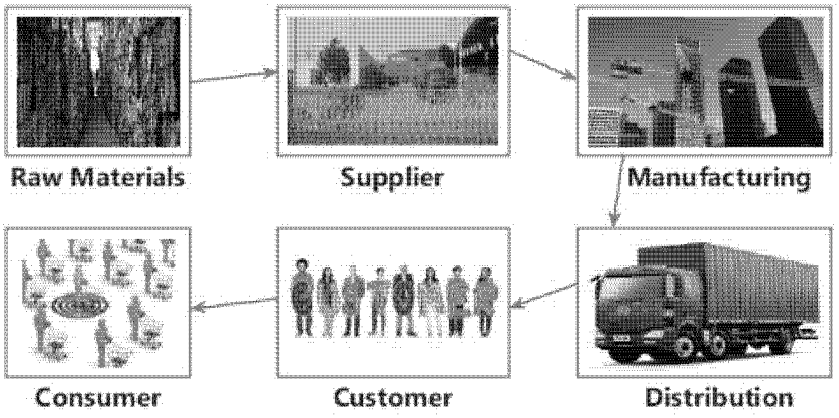
1. This module enhances the work process and data management within HR department of enterprises.
2. Right from hiring a person to evaluating one's performance, managing promotions, compensations, handling payroll and other related activities of an HR is processed using this module.
3. This department maintains total employee database such as every aspect of business transaction is taken care of by defining the master shifts master, PF ESI (Employees' State Insurance) master, leave, holiday, loans, employee master, operations and sub-operations masters etc.
4. *Only authorized person will be eligible to access information from this module.*

Q.No.13. Write about Supply Chain Module of ERP?

SUPPLY CHAIN MODULE:

a) This module provides extensive functionality for logistics, manufacturing, planning, and analytics.

b) Enterprises can optimize their supply chain for months in advance; streamline processes such as supply network, demand, and material requirement planning; create detailed scheduling; refine production integration, and maximize transportation scheduling.



Q.No.14. Write about Customer Relationship Management Module of ERP? Explain its benefits?

CRM: Customer Relationship Management is a system which aims at improving the relationship with existing customers, finding new prospective customers, and winning back former customers.

KEY BENEFITS OF A CRM MODULE ARE:

a) **Improved customer relations:** By using this strategy, all dealings involving servicing, marketing, and selling products to customers can be carried out in an organized and systematic way.

b) **Increase customer revenues:** With the help of CRM software, you can ensure that the product promotions reach a different and brand new set of customers, and not the ones who had already purchased your product, and thus effectively increase your customer revenue.

c) **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, based on their previous purchases.

d) **Better internal communication:** The sharing of customer data between different departments will enable you to work as a team. it will help in increasing the company's profitability and enabling better service to customers.

e) **Optimize marketing:** CRM will also give you an idea about the most profitable customer groups, and by using this information you will be able to target similar prospective groups, at the right time. In this way, you will be able to optimize your marketing resources efficiently.

REPORTING SYSTEM AND MIS

Q.No.15. Define the terms Report, Management Information System and MIS Report?

1. A **Report** simply means presentation of information in proper and meaningful way.
2. Two basic reports, i.e. **Balance Sheet** and **Profit & Loss Account.**
3. **Management Information System** is an integrated, user-machine system for providing information to support operation, management and decision-making functions in an organization.
4. An **MIS report** is a tool that managers use to evaluate business processes and operations.

Q.No.16. Discuss the important characteristics of MIS Reports?

Characteristics of MIS Reports:

a) **Relevant** - This is important because a report that includes unnecessary information might be ignored.

b) **Timely** - Managers need to know what's happening now or in the recent past to make decisions about the future.

c) **Accurate** - It's critical that numbers add up and that dates and times are correct. Managers and others who rely on MIS reports can't make sound decisions with information that is wrong.

d) **Structured** - Try to break long passages of information into more readable blocks or chunks and give these chunks meaningful headings.

DATA ANALYTICS & BUSINESS INTELLIGENCE

Q.No.17. Define the term Data Analytics? Explain various types of Data analytics applications?

1. **Data Analytics** is the process of examining data sets to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software.
2. Data Analytics can also be separated into quantitative data analysis and qualitative data analysis.
3. **The** quantitative data analysis involves analysis of numerical data
4. The qualitative approach focuses on understanding the content of non-numerical data like text, images, audio and video.
5. TYPES OF DATA ANALYTICS APPLICATIONS

a) **Data mining,** involves sorting through large data sets to identify trends, patterns and relationships; predictive analytics, which seeks to predict customer behavior, equipment failures and other future events;

b) **Text mining** provides a means of analyzing documents, emails and other text-based content.

c) **E-commerce** companies and marketing services providers do click stream analysis to identify website visitors who are more likely to buy a product or service based on navigation and page-viewing patterns.

d) **Mobile network operators** examine customer data to forecast churn so they can take steps to prevent defections to business rivals; to boost customer relationship management efforts, for marketing campaigns and equip call center workers with up- to-date information about callers.

e) **Healthcare organizations** mine patient data to evaluate the effectiveness of treatments for cancer and other diseases.

Q.No.18. What are the steps involved Inside the Data Analytics Process?

1. The analytics process starts with **data collection**, in which data scientists identify the information they need for analytics application and then work with data engineers and IT staffers to assemble it for use.
2. Data from different source systems may need to be **combined via data integration routines**, transformed into a common format.
3. The next step is to **find and fix data quality problems**. That includes running data profiling and data cleansing jobs to make sure that the information in a data set is consistent.
4. Additional data preparation work is then done to **manipulate and organize the data** for the planned analytics use, and data governance policies are applied to ensure that the data hews to **corporate standards** and is being used properly.

5. A data scientist builds an analytical model, using predictive modeling tools or other analytics software and programming languages such as Python, Scala, R and SQL.
6. The model is initially run against a partial data **set to test** its accuracy; finally, the model is run in production mode against the full data set.
7. The last step in the data analytics process is **communicating** the results generated by analytical models to business executives and other end users to aid in their decision-making.

Q.No.19. Discuss the term Business Intelligence (BI)? Explain its features or benefits?

1. **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.
2. The potential benefits of business intelligence programs include accelerating and improving decision making; optimizing internal business processes; increasing operational efficiency; driving new revenues;
3. BI data can include historical information, as well as new data gathered from source systems, enabling BI analysis to support both strategic and tactical decision-making processes.

BUSINESS REPORTING & XBRL

Q.No.20. Discuss the term Business Reporting? Why Business Reporting is Important?

1. **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.
2. Organizations conduct a wide range of reporting, including financial and regulatory reporting.
3. High-quality reports also promote better internal decision-making.
4. Effective and transparent business reporting allows organizations to present a cohesive explanation of their business and helps them engage with internal and external stakeholders, including customers, employees, shareholders, creditors, and regulators.

Q.No.21. What is XBRL? Discuss its importance in Reporting?

1. **Extensible Business Reporting Language (XBRL) -** an international standards-based business reporting language developed by accountants for financial reporting;
2. **XBRL** is a freely available and global standard for exchanging business information.
3. XBRL is used around the world, in more than 50 countries.
4. **XBRL** lets reporting information move between organizations rapidly, accurately and digitally.
5. **XBRL** is a standards-based way to communicate and exchange business information between business systems.

Q.No.22. What does XBRL do?

It allows unique tags to be associated with reported facts, allowing:

a) People publishing reports to do so with confidence that the information contained in them can be consumed and analyzed accurately.
b) People consuming reports to test them against a set of business and logical rules, to capture and avoid mistakes at their source.

c) People using the information to do so in the way that best suits their needs, including by using different languages, alternative currencies and in their preferred style.

d) People consuming the information to do so confident that the data provided to them conforms to a set of sophisticated pre-defined definitions.

Q.No.23. What is XBRL tagging?

1. **XBRL Tagging** is the process by which any financial data is tagged with the most appropriate element in an accounting taxonomy (a dictionary of accounting terms) that best represents the data in addition to tags that facilitate identification/classification (such as enterprise, reporting period, reporting currency, unit of measurement etc.).
2. Since all XBRL reports use the same taxonomy, numbers associated with the same element are comparable irrespective of how they are described by those releasing the financial statements.
3. Information in reports prepared using the XBRL standard is interchangeable between different information systems in entirely different organizations.
4. XBRL has the capability to allow the tagging of transactions that can themselves be **aggregated** into XBRL reports.

Q.No.24. Who uses XBRL?

XBRL is used in many ways, for many different purposes, including:

a) **REGULATORS:**
   i) Financial regulators that need significant amounts of complex performance and risk information about the institutions that they regulate.
   ii) Tax authorities that need financial statements and other compliance information from companies to process and review their corporate tax affairs.

b) **COMPANIES:** Companies that need to provide information to one or more of the regulators mentioned above.

c) **GOVERNMENTS:** Government agencies that are simplifying the process of businesses reporting to government and reducing red tape, by either harmonizing data definitions or consolidating reporting obligations (or both).

d) **DATA PROVIDERS:** Specialist data providers that use performance and risk information published into the market place and create comparisons, ratings and other value-added information products for other market participants.

e) **ANALYSTS AND INVESTORS:**
   i) Analysts that need to understand relative risk and performance.
   ii) Investors that need to compare potential investments and understand the underlying performance of existing investments.

f) **ACCOUNTANTS:** Accountants use XBRL in support of clients reporting requirements and are often involved in the preparation of XBRL reports.

Q.No.25. Explain the Important features of XBRL

Features of XBRL:

1. **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 of the terms.
2. **Testable Business Rules:** Business rules can be logical or mathematical, or both can be used to:

a) Stop poor quality information being sent to a regulator or third party.
b) Stop poor quality information being accepted by a regulator or third party.
c) Business reports that fail critical rules can be bounced back to the preparer for review and resubmission.

3. **Multi-lingual Support:** 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.
4. **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.

Q.No.26. Write about the importance of Basel III in Banking Sector?

1. **Basel III** is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector.
2. These measures aim to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source and to improve risk management and governance.
3. For measurement and assessment of banking risks, we need to bear in mind that many complex business relationships and risks cannot be quantified statistically through linear models of risk assessment. Hence, **Basel III, based on Artificial Intelligence is the best solution**
4. This improves the management of banking risks and banking risk prediction, and in- turn, the assessment of capital adequacy under Basel III.

APPLICABLE REGULATORY & COMPLIANCE REQUIREMENTS

Q.No.27. What is Regulatory Compliance?

1. In general, **Compliance** means conforming to a rule, such as a specification, policy, standard or law.
2. Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business.
3. Violations of regulatory compliance regulations often result in legal punishment, including interest, penalty and prosecution in some cases.
4. By and large we can classify the compliance and regulatory requirements in two types as under.
   a) **General** - Applicable to all irrespective of anything.
   b) **Specific** - Applicable to specific type of businesses only.

Q.No.28. Explain typical life cycle of an accounting transaction? (Or) Explain Book keeping life cycle in Business Process?

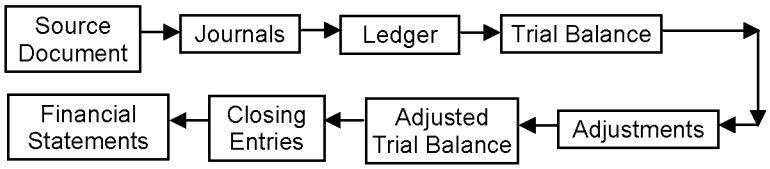
Accounting or Book keeping cycle covers the business processes involved in recording and processing accounting events of a company.

LIFE CYCLE OF AN ACCOUNTING TRANSACTION:

a) **Source Document:** Document the capture data from transactions.
b) **Journal:** Transactions are recorded into journals from the source document.
c) **Ledger:** Entries are posted to the ledger from the journal.
d) **Trial Balance:** Unadjusted trial balance containing totals from all account heads is prepared.
e) **Adjustments:** Appropriate adjustment entries are passed.
f) **Adjusted Trial balance:** The trial balance is finalized post adjustments.

g) **Closing entries:** Appropriate entries are passed to transfer accounts to financial statements.

h) **Financial statement:** The accounts are organized into the financial statements.



Q.No.29. Write about Financial Accounting Business Process Module of ERP?

1. 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.
2. The key features of this module.
   a) Tracking of flow of financial data across the organization in a controlled manner and integrating all the information for effective strategic decision making.
   b) Creation of Organizational Structure (Defining Company, Company Codes, business Areas, Functional Areas, Credit Control, Assignment of Company Codes to Credit Controls).
   c) Financial Accounting Global Settings (Maintenance of Fiscal Year, Posting Periods, defining Document types, posting keys, Number ranges for documents).
   d) General Ledger Accounting (Creation of Chart of Accounts, Account groups, defining data transfer rules, creation of General Ledger Account).
   e) Tax Configuration & Creation and Maintenance of House of Banks.
   f) Account Payables *(Creation of Vendor Master data and vendor-related finance attributes like account groups and payment terms).*

Q.No.30. Write about Controlling Module of ERP?

CONTROLLING MODULE: This module helps in analyzing the actual figures with the planned data and in planning business strategies. Two kinds of elements are managed in Controlling -**Cost Elements** and **Revenue Elements**. These elements are stored in the Financial Accounting module.

Key features are:

a) Cost Element Accounting (Overview of the costs and revenues that occur in an organization);

b) Cost Center Accounting;

c) Activity-Based-Accounting (Analyzes cross-departmental business processes);

d) Internal Orders;

e) Product Cost Controlling (Calculates the costs that occur during the manufacture of a product or provision of a service);

f) Profitability Analysis (Analyzes the profit or loss of an organization by individual market segments); and

Q.No.31. Write about Sales and Distribution Business Process Module of ERP?

SALES & DISTRIBUTION MODULE: It 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 are:

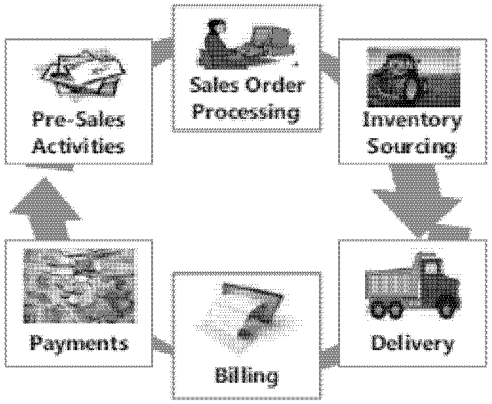
a) Setting up Organization Structure (creation of new company, company codes, sales organization, distribution channels, divisions, business area, plants, sales area, maintaining sales offices, storage location)

b) Assigning Organizational Units (Assignment of individual components created in the above activities with each other according to design like company code to company, sales organization to company code, distribution channel to sales organization, etc.)

c) Defining Pricing Components (Defining condition tables, condition types, condition sequences)

d) Setting up sales document types, billing types, and tax-related components

e) Setting up Customer master data records and configuration.

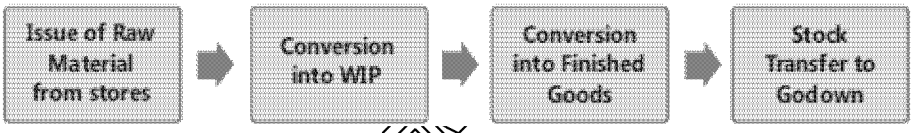


Q.No.32. Write about Production Planning Business Process Module of ERP?

Production Planning (PP) Module also consists of master data, system configuration and transactions in order to accomplish plan procedure for production.

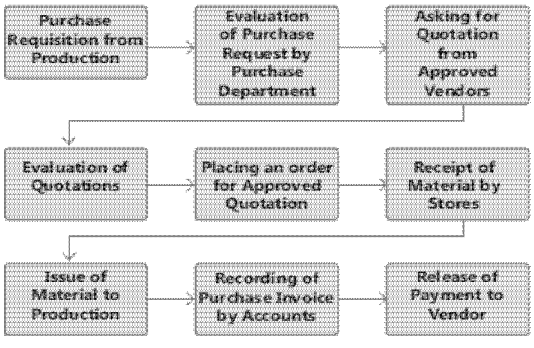
PP module collaborate with master data, sales and operations planning, distribution resource planning, material requirements planning, product cost planning and so on while working towards production management in enterprises.

The following picture discusses Production Planning Module.



Q.No.33. Write about Material Management Business Process Module of ERP?

1. **Material Management (MM) Module** as the term suggests manages materials required, processed and produced in enterprises.
2. Different types of procurement processes are managed with this system.
3. Some of the popular sub-components are vendor master data, consumption based planning, purchasing, inventory management, invoice verification and so on.
4. Material Management also deals with movement of materials via other modules like logistics, Supply Chain Management, sales and delivery, warehouse management, production and planning.



Q.No.34. Write about Quality Management Module of ERP?

QUALITY MANAGEMENT MODULE:

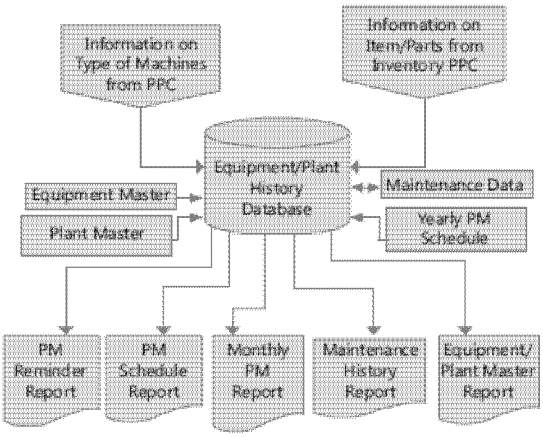
1. This quality management module helps an organization to accelerate their business by adopting a structured and functional way of managing quality in different processes.
2. Quality Management module collaborates in procurement and sales, production, planning, inspection, notification, control, audit management and so on.
3. Quality Management Process includes:

a) Master data and standards are set for quality management;
b) Set Quality Targets to be met;
c) Quality management plan is prepared;
d) Define how those quality targets will be measured;
e) Take the actions needed to measure quality;
f) Identify quality issues and improvements and changes to be made;
g) In case of any change is needed in the product, change requests are sent;
h) Report on the overall level of quality achieved; and
i) Quality is checked at multiple points, e.g. inwards of goods at warehouse, manufacturing, procurement, returns.

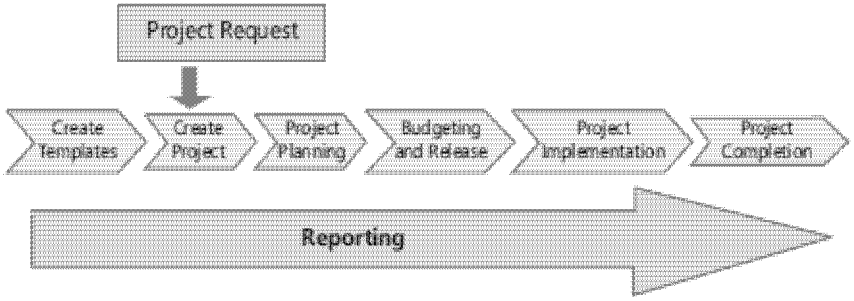
Q.No.35. Write about Plant Maintenance Module of ERP?

PLANT MAINTENANCE MODULE:

a) This is a functional module which handles the maintaining of equipment and enables efficient planning of production and generation schedules.
b) It supports cost-efficient maintenance methods, such as risk-based maintenance or preventive maintenance, and provides comprehensive outage planning and powerful work order management.



Q.No.36. Write about Project Systems Module of ERP?



PROJECT SYSTEMS MODULE

a) This is an integrated project management tool used for planning and managing projects.
b) It has several tools that enable project management process such as cost and planning budget, scheduling, requisitioning of materials and services.

Q.No.37. What is Data Warehouse? Explain the concept of Data Warehouse in brief?

a) Data warehouse is a repository of an organization's electronically stored data.

b) This is a module that can be accessed by an organizations customers, suppliers and employees.

c) Data warehouses are designed to facilitate reporting and analysis.

d) This classic definition of the data warehouse is to retrieve and analyze data, to extract, transform and load data, and to manage the data dictionary are also considered essential components

e) 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.

Q.No.38. What type of Questions should be asked by an auditor during ERP audit?

1. ERP systems should produce accurate, complete, and authorized information that is supportable and timely.
2. In a computing environment, this is accomplished by a combination of controls in the ERP System, and controls in the environment in which the ERP system operates.
3. Some of the questions auditors should ask during an ERP audit are:
   - **a)** Does the system process according to GAAP (Generally Accepted Accounting Principles) and GAAS (Generally Accepted Auditing Standards)?
   - **b)** Does it meet the needs for reporting, whether regulatory or organizational?
   - **c)** Were adequate user requirements developed through meaningful interaction?
   - **d)** Does the system protect confidentiality and integrity of information assets?
   - **e)** Does it have controls to process only authentic, valid, accurate transactions?
   - **f)** Are effective system operations and support functions provided?
   - **g)** Are all system resources protected from unauthorized access and use?
   - **h)** Are user privileges based on what is called "role-based access?"
   - ***i)*** *Is there an ERP system administrator with clearly defined responsibilities?*
   - ***j)*** *Is the functionality acceptable? Are user requirements met? Are users happy?*
   - ***k)*** *Have workarounds or manual steps been required to meet business needs?*

Q.No.39. Discuss the relationship/connection between Regulatory Compliance and Accounting Systems? And explain the pros and cons of having single software for accounting and tax compliance?

Most of the regulatory compliance requires accounting data and accounting data comes from accounting systems.

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.

Pros and Cons of having single software for Accounting and Tax Compliance

S. 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.

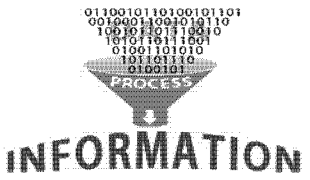
2	Features and facilities	Less - as this system is not an exclusive system for tax compliance, it may have limited features for tax compliance.	More - as this is an exclusive and specifically designed system for tax compliance, naturally more features and facilities shall exist in this system.
3	Time 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 system, reconciliation with accounting data is needed, possibility of mismatch of data is always there.
5	Cost	More - if tax compliance feature is not available in accounting system, getting it customized may require some amount of cost which may be higher than buying separate software.	Less - as this is specific purpose software, there shall be less complications and the cost also shall be less.

3A. INFORMATION SYSTEMS AND ITS COMPONENTS

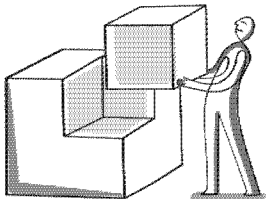
INTRODUCTION

Q.No.1. Explain the concepts 1) Information 2) System 3) Information System?

1. **Information:**
   a) Data is a raw fact and can take the form of a numbers or statement such as a date or a measurement which has some meaning.
   b) The processed data is called information.



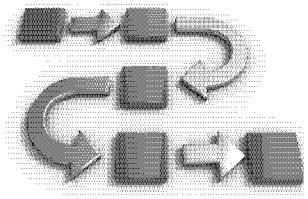
2. **System:**
   a) The system can be defined as "a group of mutually related, cooperating elements with a defined boundary; working on reaching a common goal by taking inputs and producing outputs in organized transformation process."
   b) Five Components of Generic systems are Input, Process, Output, Feedback and control.



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

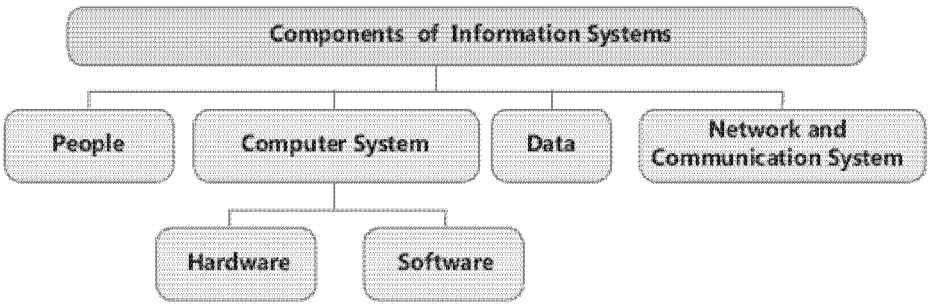
Q.No.2. What are the characteristics of Computer based information systems?

a) All systems work for predetermined objectives.
b) A System has number of interrelated and interdependent subsystems or components.
c) Every sub system depends on other subsystems for its inputs. No subsystem can function in isolation
d) If one subsystem or component fails in most of the cases whole system does not work.



Q.No.3. What are the main components of information system

.The components of Information System are:



a) People (End users and IS specialists)
b) Hardware (Machines and media)
c) Software (Programs and procedures)
d) Data (Data and knowledge bases)
e) Networks (Communications media and network support)

Q.No.4. What is meant by Hardware? What are the components of Hardware?

Hardware is the tangible portion of our computer systems, something we can touch and see.

It consists of following devices:

a) **Input Devices** are devices through which we interact with the systems. Some examples of input devices includes Keyboard, Mouse.

b) **Processing devices:** The Central Processing Unit (CPU or microprocessor) is the actual hardware that explains and executes the program instructions and coordinates how all the other hardware devices work together.

c) **Data Storage Devices** refers to the memory where data and programs are stored.

d) **Output Devices:** Computers systems provide output to decision makers to solve business problems, the desired output may be in visual, audio or digital forms. Most common examples of output devices are Speakers, Screen (Monitor), Printer etc.

Q.No.5. What is CPU? Explain different functional units of CPU?

1. The Central Processing Unit (CPU or microprocessor) is the actual hardware that explains and executes the program instructions and coordinates how all the other hardware devices work together.

2. The processor or CPU is like the brain of the computer.
3. The main function of CPU is to execute programs stored in memory.
4. It consists of three functional units:
   a) **Control Unit (CU):** CU controls the flow of data and instruction to and from memory, translates the instruction and controls which tasks to execute and when.
   b) **Arithmetic and Logical Unit (ALU):** Performs arithmetic operations such as addition, subtraction, multiplication, and logical comparison of numbers: Equal to, Greater than, Less than, etc.
   c) **Registers:** These are high speed memory units within CPU for storing small amount of data (mostly 32 or 64 bits). Registers could be:

i) **Accumulators:** They can keep running totals of arithmetic values.

ii) **Address Registers:** They can store memory addresses which tell the CPU as to where in the memory an instruction is located.

iii) **Storage Registers:** They can temporarily store data that is being sent to or coming from the system memory.

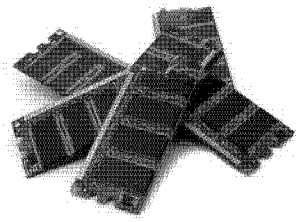
iv) **Miscellaneous:** These are used for several functions for general purpose.

Q.No.6. Explain different types of Data Storage Devices?

DATA STORAGE DEVICES refers to the memory where data and programs are stored. Various types of memory techniques/devices are given as follows:

a) **Internal Memory:** This includes Processor Registers and Cache Memory.

b) **Processor Registers:** Registers are internal memory within CPU, which are very fast and very small.

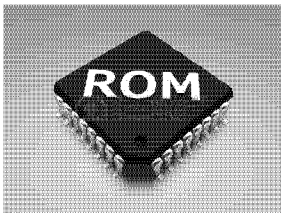


c) **Primary Memory/Main Memory:** These are devices in which any location can be accessed by the computer's processor in any order. These are primarily of two types:

i) **Random Access Memory (RAM):**

- Volatile in nature means Information is lost as soon as power is turned off.
- This is Read Write memory. Information can be read as well as modified.

ii) **Read Only Memory (ROM):**



- This is non-volatile in nature (contents remain even in absence of power).
- Information can be read not modified.

d) **Secondary Memory:** .

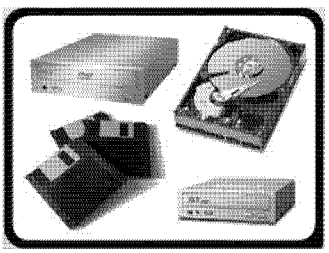
i) The secondary memory devices are non-volatility , available in large size and available in less cost.

ii) Ex: Pen Drives, Floppy drive,Hard Disk, CD, DVD

e) **Cache Memory: Refer Question 8.**

f) **Virtual Memory: Refer Question 9.**

Q.No.7. What is Cache Memory? Explain?



a) There is a huge speed difference between Registers and Primary Memory.

b) Cache memory can be used in order to bridge the speed differences between Registers and Primary memory.

c) Cache is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations.

d) These copies can be accesses by Processor/Registers more rapidly than main memory.

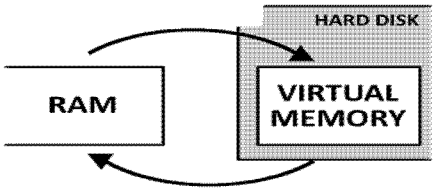
e) The cache acts as temporary memory and boosts processing power.

Q.No.8. Explain about Virtual Memory?

a) If a computer lacks the Random-Access Memory (RAM) needed to run a program or operation, OS uses virtual memory to compensate.

b) Virtual memory combines computer's RAM with temporary space on the hard disk.

c) When RAM runs low, virtual memory moves data from RAM to a space called a paging file. Moving data to and from the paging file frees up RAM to complete its work.



Q.No.9. What is software? What are different types of software's?

a) **Software** is defined as a set of instructions that tell the hardware what to do. Software is created through the process of programming.

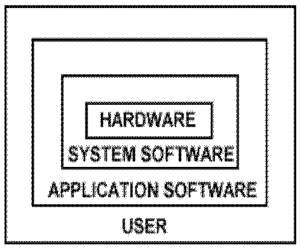
b) Software are two categories: **Operating Systems Software** and **Application Software.**

c) **Operating systems:** OS manage the hardware and create the interface between the hardware and the user.

d) **Application software:** Application software is the category of programs that do some processing/task for the user.

Q.No.10. What is Operating System (OS)? What are the activities executed by Operating system?

1. An **Operating System (OS)** is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs.
2. Some Operating systems used nowadays are Windows 7, Windows 8, Linux, UNIX, etc.
3. A variety of activities are executed by Operating systems:
   a) **Performing hardware functions:** Application programs to perform tasks must obtain input from keyboards, & display output on monitors. Operating system acts as an intermediary between the application program and the hardware.
   b) **User Interfaces:** An important function of OS is to provide user interface. Now a days, we are using Graphical User Interface (GUI) that uses icons, menus, graphics for interfacing such as Windows OS.
   c) **Hardware Independence:** OS provides Application Program Interfaces (API), which can be used by programmers to create application software, thus avoiding the need to understand the inner workings of OS and hardware. Thus, OS gives us hardware independence.
   d) **Memory Management:** Memory Management features of Operating System allow controlling how memory is accessed and maximize available memory & storage.



System Software Architecture

   e) **Task Management:** Task Management feature of Operating system helps in optimum utilization of resources. This facilitates a user to work with more than one application at a time.
   f) **Networking Capability:** Operating systems can provide systems with features & capabilities to help connect computer networks. Like Linux & Windows 8
   g) **Logical Access Security:** Operating systems provide logical security by authentication using a User ID and Password.
   h) **File management:** The operating system keeps a track of where each file is stored and who can access it, based on which it provides the file access.

Q.No.11. What is Application software? Explain different types, Advantages and Disadvantages of Application Software?

1. **Application software:** It is a collection of programs which designed for specific purpose.
2. **Different types:**
   a) **Application Suite:** Has multiple applications bundled together. E.g. MS Office has MS Word, MS Excel, MS Access, etc.
   b) **Enterprise Software:** Addresses an enterprise's needs and data flow in a huge distributed environment. E.g. ERP Applications like SAP.
   c) **Enterprise Infrastructure Software:** Provides capabilities required to support enterprise software systems. E.g. email servers, Security software.
   d) **Information Worker Software:** Addresses individual needs of individual projects within departments. E.g. Spreadsheets, CAAT (Computer Assisted Audit Tools) etc.
   e) **Content Access Software:** Used to access digital content and entertainment. E.g. Media Players, Adobe Digital etc.
   f) **Educational Software:** Holds contents adopted for use by students. E.g. Examination Test CDs
   g) **Media Development Software:** Addresses individual needs to generate and print electronic media for others to consume. E.g. Desktop Publishing, Video Editing etc.
3. **Benefits are as follows:**
   a) **Addressing User needs:** Application Software exactly meets the needs of the user. Since it is designed specifically with one purpose.
   b) **Less threat from virus:** The threat of viruses to the custom-made applications is very less because it provides security.
4. **Regular updates:** Licensed application software gets regular updates from the developer for security reasons

Disadvantages:

a) **Development is costly:** Developing application software to meet specific purposes can prove to be quite costly for developers.

b) **Infection from Malware:** application software is used and shared by many people online then it carries a computer virus or other malicious programs.

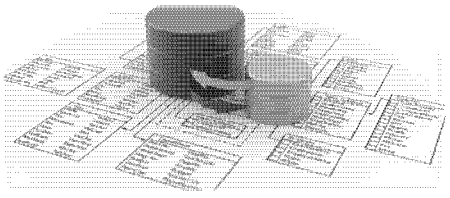
Q.No.12. What is data, database and Database management systems (DBMS)?

a) **Data:** Data are the raw bits and pieces of information with no clarity. Data can be quantitative or qualitative. Quantitative data is numeric. Qualitative data is descriptive.

b) **Database:** A database is an organized collection of related information.

c) **Database Management Systems (DBMS):** DBMS is a software system that helps in organizing, controlling and using the data needed by the application program.

EX: Oracle, MySQL, SQL Servers and DB2 etc.



Q.No.13. What is Database Model? What are different types of Database Models?

Database model is the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated.

Some database models are as:

a) Hierarchical Database Model,

b) Network Database Model,

c) Relational Database Model, and

d) Object Oriented Database Model

Q.No.14. What is Hierarchical Database Model? Explain?

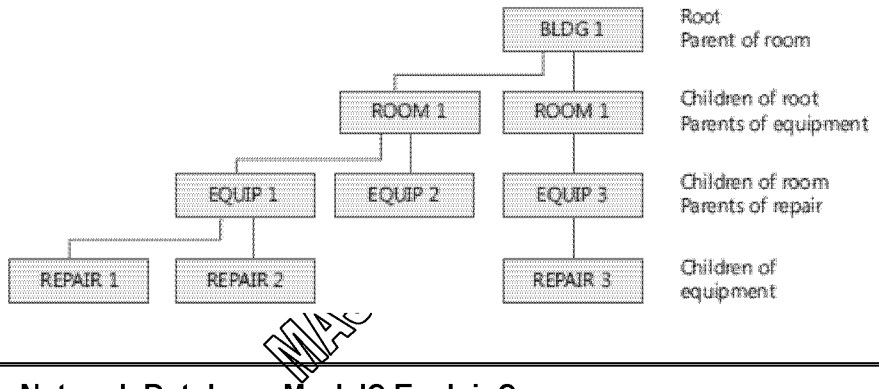
a) A hierarchically structured database is arranged logically in an inverted tree pattern.

b) All records in hierarchy are called Nodes. Each node is related to the others in a parent-child relationship.

c) Each parent record may have one or more child records, but no child record may have more than one parent record.

d) Thus, the hierarchical data structure implements one-to-one and one-to-many relationships.

e) The top parent record in the hierarchy is called the Root Record.



Q.No.15. What is Network Database Model? Explain?

a) A network database structure views all records in sets. Each set is composed of an owner record and one or more member records.

b) However, unlike the hierarchical mode, the network model also permits a record to be a member of more than one set at one time.

c) This feature allows the network model to implement the many-to-one and the many-to- many relationship types.

d) Network databases generally implement the set relationships by means of pointers that directly address the location of a record on disk. This gives excellent retrieval performance.

e) Unlike hierarchical data structures that require specific entrance points to find records in a hierarchy, network data structures can be entered and traversed more flexibly.

Q.No.16. What is Relational Database Model? Explain?

a) A **Relational Database** allows the definition of data and their structures, storage and retrieval operations and integrity constraints that can be organized in a table structure.

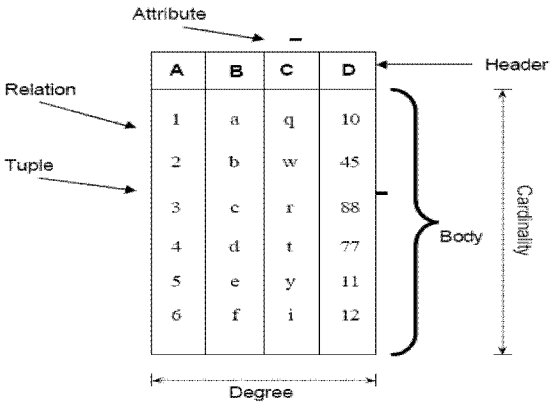
b) Three key terms are used extensively in relational database models: Relations, Attributes, and Domains.

c) A relation is a table with columns and rows. The named columns of the relation are called attributes, and the domain is the set of values the attributes can take.

d) For each table, one of the fields is identified as a Primary Key, which is the unique identifier for each record in the table.

e) Keys are commonly used to join or combine data from two or more tables.

f) Examples are Microsoft Access, MySQL, and Oracle.



Q.No.17. What is Object Oriented Data Base Model? Explain?

a) Objects are predefined set of program code that is used to perform a specific task.

b) It is based on the concept of objects and their interactions.

c) An **Object-Oriented Database** provides a mechanism to store complex data such as images, audio and video, etc.

d) An Object-Oriented Database Management System (OODBMS) helps programmers make objects created in a programming language behave as a database object.

e) An object-oriented database management system is a relational database designed to manage all these independent programs, using the data produced to quickly respond to requests for information by a larger application.

f) Expert Systems, Image Processing Systems, Multimedia Systems, Computer Aided Software Engineering (CASE) can use OODBMS to create or design several applications.

Q.No.18. What are the Major advantages and disadvantages of DBMS?

1. DISADVANTAGES

   a) **Permitting Data Sharing:** The same information can be made available to different users.

   b) **Minimizing Data Redundancy:** In a DBMS duplication of information or redundancy is, carefully controlled or reduced. so the cost of storing information on hard drives and other storage devices can be reduced.

   c) **Integrity can be maintained:** it can be maintained by having accurate, consistent, and up-to-date data. Updates to the data only made in one place in DBMS that ensures Integrity.

   d) **Program and File consistency:** File formats and programs are standardized that makes easy to maintain, because the same rules and guidelines are applied for all types of data.

   e) **User-friendly:** DBMS provides friendly interfacing which makes the data access and manipulation easier for the user.

   f) **Improved security:** Security constraints can be defined. Information should be protected or secured and it is accessible only to authorized personnel.

   g) **Achieving program/data independence:** In a DBMS, data does not reside in applications but data bases program & data are independent of each other.

   h) **Faster Application Development:** The data is already exists in databases, application developer has to think of only the logic required to retrieve the data in the way a user needs.

2. DISADVANTAGES

   a) **Cost:** Implementing a DBMS system can be expensive and time-consuming, especially in large enterprises. Training requirements alone can be quite costly.

   b) **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.

Q.No.19. Explain the concepts 1) Big Data 2) Data Mining?

a) **Big data:** The term refers to such massively large data sets that conventional database tools do not have the processing power to analyze them. For example, WalMart must process over one million customer transactions every hour.

b) **Data Mining:** Data Mining is the process of analyzing large data sets in a data warehouse to find previously unknown trends, patterns to make decisions.

Q.No.20. What is Data Warehouse? What are two primary schools of thought when designing a data warehouse and List out the Benefits of Data Warehouse?

1. The concept of the data warehouse is extract data from one or more of the organization's databases and load it into the data warehouse (which is itself another database) for storage and analysis. so the data warehouse must pull data from the existing databases on a regular, scheduled basis.
2. The two approaches of designing a data warehouse are:
   i) **The Bottom-Up Approach** starts by creating small data warehouses, called data marts. As these data marts are created, they can be combined into a larger data warehouse.
   ii) **The Top-Down Approach** suggests that we should start by creating an enterprise-wide data warehouse and then, create smaller data marts from the data warehouse.
3. **Benefits of Data Warehouse:**
   i) Developing a data warehouse forces an organization to better understand the data that it is currently collecting and, equally important, what data is not being collected.
   ii) A data warehouse provides a centralized view of all data being collected across the enterprise and provides a means for determining data that is inconsistent.
   iii) By having a data warehouse, snapshots of data can be taken over time. This creates a historical record of data, which allows for an analysis of trends.

Q.No.21. What is computer network? Discuss the types and issues of computer network?

1. **Computer Network** is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information.
2. Each component, namely the computer in a computer network is called a 'Node'.
3. Networks could be of two types:
   a) **Connection Oriented networks:** Wherein a connection is first established and then data is exchanged like it happens in case of telephone networks.
   b) **Connectionless Networks:** Where no prior connection is made before data exchanges.
4. Each of these networks is modeled to address the following basic issues:
   a) **Routing:** It refers to the process of deciding on how to communicate the data from source to destination in a network.
   b) **Bandwidth:** It refers to the amount of data which can be sent across a network in given time.
   c) **Resilience:** It refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.
   d) **Contention:** It refers to the situation that arises when there is a clash for some common resource in a network.

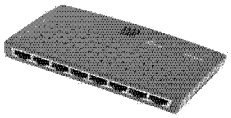
Q.No.22. Explain some technical concepts based on some simple principles.

Some technical concepts are:

a) **Packet:** When a device intends to send a message to another device, it breaks the message down into smaller pieces, called packets. Each packet has the sender's address, the destination address, a sequence number.

b) **Repeater:** A repeater regenerates the signal over the same network before the signal becomes too weak and extends the length of signal transmitted over the same network.

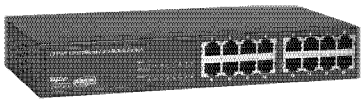
c) **Hub:** A simple network device that connects other devices to the network and sends packets to all the devices connected to it. *Hubs cannot filter data, so data packets are sent to all connected devices.*



d) **Bridge:** Bridge is a communications processor that connects two Local Area Networks (LANs) working on the same protocol. A bridge filters content by reading the MAC addresses of source and destination.

e) **MAC Address:** These are most often assigned by the manufacturer of a Network Interface Controller (NIC) and are stored in its hardware, such as the card's read-only memory.

f) **Switch:** A network device that connects multiple devices together and filters packets based on their destination within the connected devices.



g) **Router:** A device that receives and analyses packets and then routes them towards their destination

h) **Network Topology:**

i) The term 'Topology' defines the physical or logical arrangement of links and linking devices in a network.

ii) Common topologies are **Star Network, Bus Network, Ring Network and Mesh Network**

i) **Transmission Mode:**

i) It is used to define the direction of signal flow between two linked devices. There are three types:

ii) **Simplex** (wherein the data flows in only one direction- unidirectional),

iii) **Half-Duplex** (where in the data flows in one direction or the other, but not both at the same time) and

iv) **Full Duplex** (in which the data flows in both directions simultaneously).

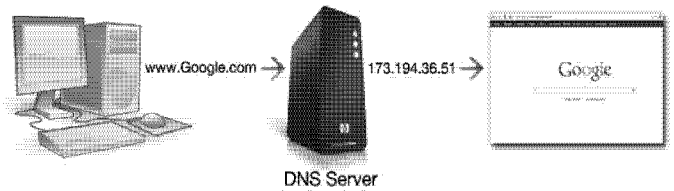
j) **Protocol:** In computer networking, a protocol is the set of rules that allow two (or more) devices to exchange information across the network.

k) **IP Address:**

i) Every device that communicates on the Internet, whether it be a personal computer, a tablet, a smartphone, or anything else, is assigned a unique identifying number called an IP (Internet Protocol) address.

ii) Presently we are using IPv4 (version 4), IPv6 standards Ex: domain wikipedia.org has the IP address of 107.23.196.166.

l) **Domain Name:** A Domain Name is a human-friendly name for a device on the Internet. For example, Wikipedia's domain name is wikipedia.org;



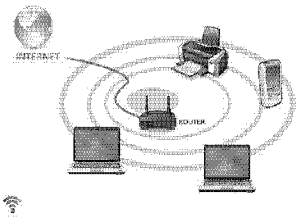
m) **Domain Name System (DNS):** When a request to access a device with a domain name is given, a DNS server is queried. It returns the IP address of the device requested, allowing for proper routing.

n) **Packet Switching:**

i) When a packet is sent from one device out over the Internet, it does not follow a straight path to its destination.

ii) Instead, it is passed from one router to another across the Internet until it is reaches its destination.

o) **Wi-Fi:**



i) Wi-Fi stands for wireless fidelity. Wi-Fi is a technology that takes an Internet signal and converts it into radio waves. These radio waves can be picked up within a radius of approximately 65 feet by devices with a wireless adapter.

p) **Voice over IP (VoIP):**

i) A growing class of data being transferred over the Internet is Voice Data.

ii) A protocol called VoIP enables sounds to be converted to a digital format for transmission over the Internet and then recreated at the other end. EX:Skype, Google Hangouts, Whatsapp calls).

INFORMATION SYSTEMS CONTROLS

Q.No.23. What is Controls? Explain the Need for Controls in Information Systems?

Control: Controls are defined as policies, procedures, practices, and organization structure ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected.

Need For Controls:

a) Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

b) A well designed information system should have controls built-in for all its sensitive or critical sections.

IS control procedure may include:

a) Strategy and direction

b) General Organization and Management

c) System Programming and technical support functions;

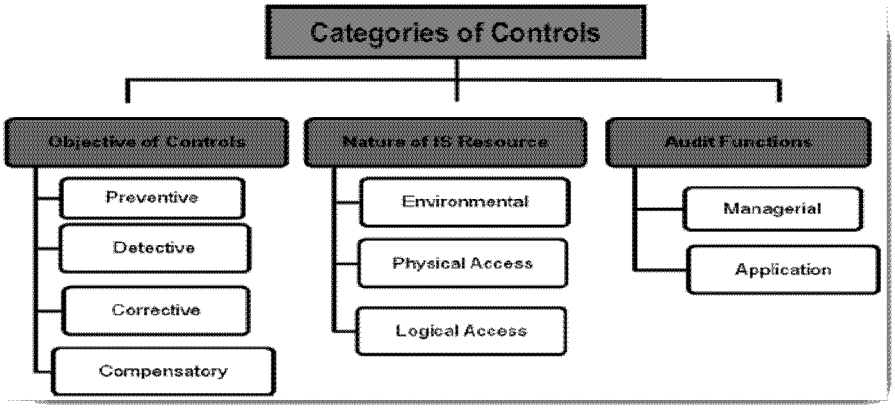
d) Quality Assurance Procedures

e) Physical Access Controls

f) Network and Communication

g) Database Administration

CLASSIFICATION OF INFORMATION SYSTEMS' CONTROLS



Q.No.24. Explain the Classification based on "Objective of Controls"?

The Classification based on "Objective of Controls" are:

1. **Preventive Controls:** These controls prevent errors, omissions, or security incidents from occurring. Some of the examples of Preventive Controls are:
   - **a)** Access control
   - **b)** Anti-virus software
   - **c)** Firewalls, Passwords.

Purpose	*Manual Control*	*Computerized Control*
Restrict unauthorized entry into the premises.	*Build a gate and post a security guard.*	*Use access control software, smart card, biometrics, etc.*
Restricted unauthorized entry into the software applications.	*Keep the computer in a secured location and allow only authorized person to use the applications.*	*Use access control, viz. User ID, password, smart card, etc.*

2. **Detective Controls:** Detective Controls detect errors or incidents that escape from preventive controls. *For example, a detective control may identify account numbers of inactive accounts*
3. **Characteristics of Detective controls:**
   - **a)** Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
   - **b)** Interaction with the preventive control to prevent such acts from occurring; and
   - **c)** Surprise checks by supervisor.
4. **Corrective Controls:** It is desirable to correct errors, omissions, or incidents once they have been detected. Ex: correction of data-entry errors.

Characteristics of the corrective controls:

- **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)** Correcting error arising from a problem

Q.No.25. Explain about Controls for Fire Damage in Environmental Controls?

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.

a) **Fire Damage:** It is a major threat to the physical security of a computer installation.

b) **Controls for Fire Damage:** Some of the major ways of protecting the installation against fire damage are as follows:

- **i)** Both automatic and manual fire alarms may be placed at strategic locations.
- **ii)** Manual fire extinguishers can be placed at strategic locations.
- **iii)** Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials should be used.

c) **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured.

d) **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).

e) **Wiring Placed in Electrical Panels and Conduit:** To reduce the risk of fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit.

Q.No.26. Explain about Power Spikes and it's controls in Environmental Controls?

Power Spikes: This is caused due to a very short pulse of energy in a power line.

Controls for Environmental Exposures:

The risk of damage due to power spikes can be reduced using Electrical Surge Protectors or stabilizer that are typically built into the Un-interruptible Power System (UPS).

a) **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.

b) **Voltage regulators and circuit breakers** protect the hardware from temporary increase or decrease of power.

c) **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 and should be easily accessible and yet secured from unauthorized people.

Q.No.27. Explain different controls for Water Damage in Environmental Controls?

a) **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.

b) **Controls for Water Damage:**

i) Wherever possible have waterproof ceilings, walls and floors;

ii) Ensure an adequate positive drainage system exists;

iii) Install alarms at strategic points within the installation;

iv) In flood areas have the installation above the upper floors but not at the top floor;

Q.No.28. Explain the controls for Pollution Damage in Environmental Controls?

a) **Pollution Damage and others:** The major pollutant in a computer installation is dust. Dust may cause either permanent damage or temporary failure.

b) **Controls for Environmental Exposures:**

i) **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.

ii) **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. stick wall paper on the entry door.

Q.No.29. Explain different Controls for Physical Exposures?

Physical Access Controls: These are the controls relating to physical security of the tangible IS resources. Such controls include

1. **Locks on Doors:**
   a) **Cipher locks (Combination Door Locks)** - Cipher locks are used in low security situations. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period, usually ten to thirty seconds.
   b) **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.
   c) **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.
2. **Physical Identification Medium:**
   a) **Personal Identification Numbers (PIN):** A secret number will be assigned to the individual, serves to verify the authenticity of the individual. Ex: ATM
   b) **Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card.
   c) **Identification Badges:** Special identification badges can be issued to personnel as well as visitors. *For easy identification purposes, their color of the badge can be changed.*
3. **Logging on Facilities:**
   a) **Manual Logging:** All visitors should sign in visitor's register indicating their name, company represented, their purpose of visit, and person to see.
   b) **Electronic Logging:**
      i) This feature is a combination of electronic and biometric security systems.
      ii) The users logging can be monitored and the unsuccessful attempts being highlighted.

Q.No.30. Explain other Controls for Physical Exposures?

Other means of Controlling Physical Access:

a) **Video Cameras:** Cameras should be placed at specific locations and monitored by security guards. The video supervision recording must be retained for possible future play back.
b) **Security Guards:** Extra security can be provided by appointing guards helped with CCTV feeds.
c) **Controlled Visitor Access:** A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.
d) **Bonded Personnel:** All service contract personnel, such as cleaning people and office boys, should be asked to sign a bond.
e) **Dead Man Doors:** These systems encompass a pair of doors that are typically found in room entries. The first entry door must close and lock, for the second door to operate, with the only one person permitted in the holding area.
f) **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.
g) **Computer Terminal Locks:** These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.
h) **Controlled Single Entry Point:** A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry.

Q.No.31. What is Logical Access Controls? Explain the Technical Exposures in Logical Access Controls?

Logical Access Controls: These are the controls relating to logical access to information resources such as data and programs is restricted to authorized users.

Technical exposures include the following.

a) **Data Diddling:** This involves the change of data before or after they entered the system.The worst part with this is that it occurs before computer security can protect the data.

b) **Bomb:** Bomb is a piece of bad code intentionally planted by an insider or supplier of a program. which is logical, time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately.

c) **Christmas Card:** On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half-finished work.

d) **Worm:** A worm does not require other program like a virus to relocate itself. Thus, a Worm program copies itself to another machine on the network.

e) **Rounding Down:** This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

f) **Salami Techniques:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted.

g) **Trap Doors:** Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data.

h) **Spoofing:** A spoofing attack involves forging one's source address. One machine is used to imitate the other in spoofing technique.

Q.No.32. Explain User Access Management and User Responsibilities in Logical Access Controls?

a) **User Access Management:**

   i) **User Registration:** Information about every user is documented.

   ii) **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities.

   iii) **User password management:** Allocations, storage, revocation, and reissue of password are password management functions.

   iv) **Review of user access rights:** Periodic review of access rights to check anomalies.

b) **User Responsibilities:**

   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. .

Q.No.33. Explain Network Access Control in Logical Access Controls?

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:

a) **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.

b) **Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks.

c) **Segregation of networks:** Based on the sensitive information handling function, network is isolated from the internet usage service

d) **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies.

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

f) **Firewall:** A **Firewall** is a system that acts as access control between two networks. It is a barrier between public and private network.

g) **Encryption:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks.

h) **Call Back Devices:** The call- back device requires the user to enter a password and then the system breaks the connection. If the user is authorized, the call back device dials the user's number to establish a new connection.

Q.No.34. Explain Operating System Access Control in Logical Access Controls?

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

b) **Terminal log-in procedures:** When the user enters user-id and password, the system compares the ID and password to a database of valid users and accordingly authorizes the log-in.

c) **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.

d) **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. If there is a match, the user is granted access.

e) **Discretionary Access Control:** The system administrator usually determines who is granted access to specific resources and maintains the access control list.

f) **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. For this Biometric Authentication should be employed.

g) **Password management system:** An operating system could enforce selection of good passwords and the password file should not be accessible to users.

h) **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.

Q.No.35. Explain Application and Monitoring System Access Control in logical controls?

a) **Information access restriction:** *A user can access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users.*

b) **Sensitive system isolation:** Based on the criticality of a system in an enterprise, it may even be necessary to run the system in an isolated or separated environment.

c) **Event logging:** All incoming and outgoing requests along with attempted access should be recorded in a transaction log.

d) **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential.

e) **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.

Q.No.36. What is Managerial Controls? Explain Top Management and Information Systems Management Controls in Managerial Controls?

Managerial Controls: The controls at this level provide a stable infrastructure in which IS can be built, operated, and maintained on a day-to-day basis.

Top Management and Information Systems Management Controls:

a) The senior managers who take responsibility for IS function in an organization face many challenges.

b) The major functions that a senior manager must perform are as follows:

i) Planning – determining the goals of the information systems function and the means of achieving these goals;

ii) Organizing – gathering, allocating, and coordinating the resources needed to accomplish the goals;

iii) Leading – motivating, guiding, and communicating with personnel.

iv) Controlling – comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

c) Top management must prepare two types of information systems plans for the information systems function: a Strategic plan and an Operational plan.

d) The strategic Plan is the long-run plan covering and Operational Plan is the short-plan covering.

Q.No.37. Explain Systems Development Management Controls in Managerial Controls?

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems.

The six activities discussed below deal with system development controls in IT setup.

a) System Authorization Activities: *Each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.*

b) User Specification Activities: *The user can create a detailed written descriptive document of the logical needs that must be satisfied by the system.*

c) Technical Design Activities: The technical design activities translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs.

d) Internal Auditor's Participation: The internal auditor should involve at every stage of the system development process to make conceptual suggestions regarding system requirements and controls.

e) Program Testing: All program modules must be thoroughly tested before they are implemented *to identify programming and logic errors.*

f) User Test and Acceptance Procedures: Just before implementation, the individual modules of the system must be tested as a unified whole then it is formally accepted by the user department(s).

Q.No.38. Explain Programming Management Controls in Managerial Controls?

Programming Management Controls: The program development life cycle comprises six major phases - Planning; Design; Control; Coding; Testing; and Operation and Maintenance

Phases of Program Development Life Cycle

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts can be used to monitor progress against plan.
Control	The Control phase has two major purposes: **a)** Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations **b)** Control should ensure software released for production use is authentic, accurate, and complete.

Design	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 and Threads approach).
Testing	Three types of testing can be: **a) Unit Testing** - which focuses on individual program modules; **b) Integration Testing** - Which focuses in groups of program modules **c) Whole-of-Program Testing** - which focuses on whole program.
Operation and Maintenance	Three types of maintenance can be used as: **a) Repair Maintenance** - in which program errors are corrected; **b) Adaptive Maintenance** - in which the program is modified to meet changing user requirements **c) Perfective Maintenance** - in which the program is tuned to decrease the resource consumption.

Q.No.39. Explain Data Resource Management Controls in Managerial Controls?

DATA RESOURCE MANAGEMENT CONTROLS

1. Data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented.
2. *Data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed.* .
3. The control activities involved as:
   a) **Definition Controls:** These controls are placed to ensure that the database always corresponds and comply with its definition standards.
   b) **Existence/Backup Controls:** Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases.
   c) **Access Controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, destroying the entity's data.
      i) User Access Controls through passwords and biometric Controls.
      ii) Data Encryption: Keeping the data in database in encrypted form.
   d) **Update Controls:** These controls restrict update of the database to authorized users in two ways:
      i) By permitting only addition of data to the database.
      ii) Allowing users to change or delete existing data.
   e) **Concurrency Controls:** These controls provide solutions and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.
   f) **Quality Controls:** These controls ensure the accuracy, completeness, and consistency of data maintained in the database.

Q.No.40. Explain Quality Assurance Management Controls in Managerial Controls?

1. Quality Assurance management is concerned with ensuring that the -

   Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.
2. The reasons for the emergence of Quality assurance in many organizations are as follows:

a) Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work.

b) Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work,

c) Organizations are becoming more concerned about their liabilities if they produce and sell defective software.

d) Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer,

Q.No.41. Explain Security Management Controls in Managerial Controls?

1. **Threat Identification:** A threat is some action or event that can lead to a loss. Some of the major threats and to the security of information systems and their controls are as discussed in the Table.

Major Security threats and their control measures

Threat	Controls
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed to mitigate losses from water damage
Energy Variations	Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities like BCP, DRP, Insurance etc. must be adapted to withstand structural damages that may occur due to earthquake, snow, wind etc.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Use anti-virus and anti-worm softwares.
Misuse of software, data and services	Use separate methods to observe the actions of information systems employees.
Hackers	Use logical access controls to mitigate losses from the activities of hackers.

2. **BCP (Business Continuity Planning) Controls:** These controls make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption.

3. A comprehensive Disaster Recovery Plan comprises four parts - **an Emergency Plan, a Backup Plan, a Recovery Plan** and a **Test Plan.**

Q.No.42. What are Application Controls? Explain Boundary Controls in Application Controls?

1. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage.

2. **Major Boundary Control are as follows:**

a) **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not have permission to access the respective system resource or file.

b) **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation .these can be used as a password boundary access control.

c) **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution independent to a user identification details, or a customer selected number.

d) **Identification Cards:** Identification cards are used to store information required in an authentication process.

e) **Biometric Devices:** Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.

Q.No.43. Explain Input Controls in Application Controls in brief?

1. Input Controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system.
2. Input controls are important since substantial time is spent on inputting data which involves human intervention and are therefore prone to errors and fraud.
3. Input control techniques are:
   a) Source Document Control
   b) Data Coding Controls
   c) Batch Controls
   d) Validation Controls

Q.No.44. Explain Source Document Controls in Input controls?

a) **Use pre-numbered source documents:** Source documents should come pre-numbered from the printer with a unique sequential number on each document. *Source document numbers used for tracing transactions through accounting records.*

b) **Use source documents in sequence:** Source documents should be distributed to the users and used in sequence. *This requires the adequate physical security be maintained over the source document inventory at the user site.*

c) **Periodically audit source documents:** Missing source documents should be identified by reconciling document sequence numbers. *Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors.*

Q.No.45. Explain Data Coding Controls in Input controls?

Two types of 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.

1. **Transcription Errors:** It is a special type of data entry error that is commonly made by human operators . These fall into three classes:
   a) **Addition errors** occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766
   b) **Truncation errors** occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327
   c) **Substitution errors** are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266
2. **Transposition Errors:** It is a simple error of data entry that occurs when two digits that are either individual or part of larger sequence of numbers are reversed (Transpose) when posting a transaction. There are two types of transposition errors.
   a) **Single transposition** errors occur when two adjacent digits are recorded as 21345 instead of 12345.
   b) **Multiple transposition** errors occur when non-adjacent digits are transposed. For example, 12345 are recorded as 32154.

Q.No.46. Explain Batch Controls in Input controls?

Batching is the process of grouping together transactions that bear some type of relationship to each other. Two types of batches that occur are as follows:

i) **Physical Controls:** These controls are groups of transactions that constitute a physical unit. *For example - source documents might be given to a data-entry clerk to be entered into an application system at a terminal.*

ii) **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous. *For example different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.*

To identify errors or irregularities in either a physical or logical batch, three types of control totals are as follows:

i) **Financial totals:** Grand totals calculated for each field containing money amounts.

ii) **Hash totals:** Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totaled.

iii) **Document/Record Counts:** Grand totals for number of documents in record in batch.

Q.No.47. Explain validation controls in input controls?

Input validation controls are intended to detect errors in the transaction data before the data are processed. There are three levels of input validation controls:

1. **Field Interrogation:** It involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation.
   a) **Limit Check:** The field is checked by the program against predefined limits to ensure that no input/output error has occurred.
   b) **Picture Checks:** These checks against entry into processing of incorrect/ invalid characters.
   c) **Valid Code Checks:** Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid.
   d) **Check Digit:**
      i) A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing.
   e) **Arithmetic Checks:** Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.
   f) **Cross Checks:** may be employed to verify fields appearing in different files to see that the result tally.
2. **Record Interrogation:** These are discussed as follows:
   a) **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?
   b) **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
   c) **Sequence Check:** If physical records follow a required order matching with logical records.
3. **File Interrogation:** These are discussed as follows:
   a) **Version Usage:** Proper version of a file should be used for processing the data correctly
   b) **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process.
   c) **Data File Security:** Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability.

d) **Before and after Image and Logging:** The application may provide for reporting of before and after images of transactions.

e) **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected.

f) **Parity Check:** When programs or data are transmitted, additional controls are needed. Used for detecting errors or correcting codes.

Q.No.48. Explain about Communication Controls in brief?

Communication Controls: Components in the communication subsystem are responsible for transporting data among all the other subsystems within a system

1. **Physical Component Controls:** These controls involve Transmission Media - wire Media or wireless Media, Modems, Port Protection Devices, Multiplexors.
2. **Line Error Controls:** Error Detection (using Parity Checking) and Error Correction (using forward Error Correcting Codes and Backward Error Correction) are the two major approaches under Line Error Controls.
3. **Flow Controls**: The simplest form of flow control is "Stop-and-Wait Flow Control" in which the sender transmits a frame of data only when the receiver is ready to accept the frame.
4. **Link Controls:** This involves two common protocols – HDLC (Higher Level Data Control) and SDLC (Synchronous Data Link Control);
5. **Topological Controls:** A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked. Some of the four basic topologies include Bus, Ring and Star Topology.
6. **Channel Access Controls**: These techniques fall into two classes – Polling methods and Contention methods. Polling techniques establish an order in which a node can gain access to channel capacity. whereas in Contention methods, nodes in a network must compete with each other to gain access to a channel.
7. **Internetworking Controls:** Internetworking is the process of connecting two or more communication networks together. Three types of devices are used to connect sub-networks in an Internet: Bridge, Router and Gateway.

Q.No.49. Explain different types of Processing Controls?

DIFFERENT TYPES OF PROCESSING CONTROLS ARE:

1. **Processor Controls:** The processor has three components:
   a) A Control unit, which fetches programs from memory and determines their type;
   b) An Arithmetic and Logical Unit, which performs operations; and
   c) Registers that are used to store temporary results and control information.
2. Four types of controls that can be used to reduce expected losses from errors and irregularities associated with Central processors.

Controls to reduce expected losses from errors and irregularities associated with Central processors

Control	Explanation
Error Detection and Correction	Occasionally, processors might crash. The causes could be design errors, manufacturing defects, damage.The failure might be transient, intermittent, and permanent. For the transient and intermittent errors,retries and re-execution might be successful whereas for permanent errors, the processor must halt and report the error.

Multiple Execution States	It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities.
Timing Controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.
Component Replication	In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected.

3. **Real Memory Controls:** This comprises the fixed amount of primary storage in which programs must be executed by the central processor. Real memory controls seek to protect areas of memory assigned to a cpu program from illegal access by another program.
4. **Virtual Memory Controls:** Virtual Memory exists when the addressable storage space is larger that the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.
5. **Data Processing Controls:** These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. (**Note:** Refer next question in detail)

Q.No.50. Explain different types of Data Processing Controls?

These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed.

i) **Run-to-Run Totals:** These helps in verifying data that is subject to process through different stages. A specific record probably the last record can be used to maintain the control total.

ii) **Reasonableness Verification:** Two or more fields can be compared and cross verified to ensure their correctness.

iii) **Edit Checks:** Edit checks like the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

iv) **Field Initialization:** Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e. setting all values to zero/blank before inserting the field or record.

v) **Exception Reports:** Exception reports are generated to identify errors in the data processed. *Such exception reports give the transaction code and why a particular transaction was not processed or what is the error in processing the transaction.*

Q.No.51. Explain Update Controls in Database Controls in detail?

1. Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called **Database Controls.**
2. Database Controls are two types: Update and Report controls
3. **Major Update Controls are:**
   a) **Sequence Check between Transaction and Master Files:** The correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records. If errors, in this stage are fail to observe, it leads to corruption of the critical data.
   b) **Ensure All Records on Files are processed:** While processing, the transaction file records mapped to the respective master file, and the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.
   c) **Process multiple transactions for a single record in the correct order:** Multiple transactions can occur based on a single master record .Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.

d) **Maintain a suspense account:** When mapping between the master records to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account.

Q.No.52. Explain Report Controls in Database Controls in detail?

Major Report Controls are:

a) **Standing Data:** Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc.

i) Any changes or errors in these tables would have an adverse effect on the organizations basic functions.

ii) Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.

b) **Print-Run-to Run control Totals:** Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.

c) **Print Suspense Account Entries:** Similar to the update controls, the suspense account entries are to be periodically monitors with the respective error file and action taken on time.

d) **Existence/Recovery Controls:** The back-up and recovery strategies together encompass the controls required to restore failure in a database

Q.No.53. Explain different Output Controls in Detail?

1. **Output Controls** ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner.
2. Various Output Controls are as follows:

a) **Storage and Logging of sensitive/critical forms:** Pre-printed stationery like security forms should be stored securely to prevent unauthorized destruction or removal and usage.

b) **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data may be compromised.

c) **Spooling/Queuing:** "Spool" is an acronym for "**Simultaneous Peripherals Operations Online**". When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk.

i) This file is then "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification.

d) **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place.

e) **Report Distribution and Collection Controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data.

i) A log should be maintained for reports that were generated and to whom these were distributed.

ii) A log should be maintained about reports that were printed and collected. Uncollected reports should be stored securely.

f) Retention Controls: Retention controls consider the duration for which outputs should be retained before being destroyed.

Q.No.54. What are Asynchronous attacks? Explain the various forms of asynchronous attacks? (PM, N16 RTP, N14 RTP, M16 MTP2, M17 MTP)

Asynchronous Attacks

a) They occur in many environments where data can be moved asynchronously across telecommunication lines.

b) Data that are 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.

c) There are many forms of **asynchronous attacks.**

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

ii) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.

iii) **Piggybacking:**

- This is the act of electronically attaching to an authorized telecommunication link that intercepts and alters transmissions.
- A special terminal is tapped into the communication for this purpose.

iv) **Shut Down of the Computer/Denial of Service:**

- When overloading happens some systems have been proved to be vulnerable to shutting themselves.
- Hackers use this technique to shut down computer systems over the Internet.

3B.INFORMATION SYSTEMS AUDITING

Q.No.1. What is Information Systems Auditing and explain its objectives?

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:

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

b) **Data Integrity Objectives:** The importance to maintain integrity of data of an organization requires all the time.

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

d) **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.

Q.No.2. Explain the Need for Audit of Information Systems? (or) Explain about the impact of controls and audit influencing an organization?

a) **Organizational Costs of Data Loss:** *Data is a critical resource of an organisation for its present and future process.*

b) **Cost of Incorrect Decision Making:** *The high-level decisions require accurate data to make quality decision rules.*

c) **Costs of Computer Abuse:** *Unauthorized access to computer systems and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)*

d) **Value of Computer Hardware, Software and Personnel:** *These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.*

e) **High Costs of Computer Error:** A *data error during entry or process would cause great damage.*

f) **Maintenance of Privacy:** *Today, data collected in a business process contains private information about an individual too. there is a fear that privacy has eroded beyond acceptable levels.*

g) **Controlled evolution of computer Use:** *Use of Technology and reliability of complex computer systems cannot be guaranteed.*

Q.No.3. What is Concurrent or Continuous Audit? Explain different Types of Audit Tools?

Continuous auditing enables auditors to eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.

TYPES OF AUDIT TOOLS:

a) **Snapshots:**

i) The snapshot software is built into the system which takes images of the flow of any transaction as it moves through the application.

ii) These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

b) **Integrated Test Facility (ITF):**

i) 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.

ii) This test data would be included with the normal production data used as input to the application system.

c) **System Control Audit Review File (SCARF):** The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files.

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

e) **Audit Hooks:**

i) There are audit routines that flag suspicious transactions.

ii) *For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy.*

iii) They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud.

AUDIT TRAIL

Q.No.4. What is Audit Trail? Explain types and objectives of Audit Trail?

1. **Audit Trails** are logs that can be designed to record activity at the system, application, and user level.

Types of Audit Trail:

i) **The Accounting Audit Trail** shows the source and nature of data and processes that update the database.

ii) **The Operations Audit Trail** maintains a record of attempted or actual resource consumption within a system.

2. **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways:
   a) **Detecting Unauthorized Access:** *Detecting unauthorized access can occur in real time or after the fact.* The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls.
   b) **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors.
   c) **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

Q.No.5. What is the role of auditor in Auditing Environmental Controls? What are the factors that should focused by Auditing Environmental Controls?

1. **Audit of Environmental Controls:** Auditing environmental controls requires knowledge of building mechanical and electrical systems as well as fire codes. *The IS auditor needs to be able to determine if such controls are effective and if they are cost-effective.*
2. **Auditing environmental controls requires attention to these and other factors and activities, including:**
   a) **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, surge protectors, or motor generators, are used, inspected and maintained and if this is performed by qualified personnel.
   b) **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. He or she should examine how frequently these components are maintained and if this is done by qualified personnel.
   c) **Heating, Ventilation, and Air Conditioning (HVAC):** The IS auditor should determine if HVAC systems are providing adequate temperature and humidity levels, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.
   d) **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.
   e) **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if the organization has emergency evacuation plans and conducts fire drills.

f) **Cleanliness:** The IS auditor should examine data centers to see how clean they are.

Q.No.6. what is the role of Auditor in Auditing Physical Security Controls? What are the Physical Access Controls that should audit by Auditor?

1. **Audit of Physical Access Controls:** Auditing physical security controls requires knowledge of natural and man made hazards, physical security controls, and access control systems.
   a) **Siting and Marking:** Auditing building siting and marking requires attention to several key factors and features, including:
   b) **Proximity to hazards:** The IS auditor should estimate the building's distance to natural and man made hazards, such as Dams; Rivers; Natural gas and petroleum pipelines; Water mains and pipelines; Earthquake faults; Volcanoes;
   c) **Marking:** The IS auditor should inspect the building and surrounding area to see if building(s) containing information processing equipment identify the organization. Marking may be visible on the building itself, but also on signs or parking stickers on vehicles.
   d) **Physical barriers:** This includes fencing, walls, barbed/razor wire, bollards, and crash gates.

The IS auditor needs to determine their effectiveness.

e) **Surveillance:** The IS auditor needs to understand how video and human surveillance are used to control and monitor access. He or she needs to understand if it is effective in preventing or detecting incidents.

f) **Guards and dogs:** The IS auditor needs to understand the use and effectiveness of security guards and guard dogs.

g) **Key-Card systems:** The IS auditor needs to understand how key-card systems are used to control access to the facility. Whether the facility is divided into security zones and which persons are permitted to access which zones;

Q.No.7. What is the Role of IS Auditor in Auditing Logical Access Controls?

Role of IS Auditor in Auditing Logical Access Controls: Auditing Logical Access Controls requires attention to several key areas that include the following:

a) **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 the use of investigative and technical tools.

b) **Documentation:** The IS auditor should request network architecture and access documentation to compare what was discovered independently against existing documentation.

Q.No.8. Explain User Access Controls in Audit of Logical Access Controls?

USER ACCESS CONTROLS: User access controls are often the only barrier between unauthorized parties and sensitive or valuable information.

Auditing User Access Controls: Auditing user access controls requires attention to several factors, including:

a) **Authentication:** The auditor should examine network and system resources to determine if they require authentication.

b) **Access violations:** The auditor should determine if systems, networks, and authentication mechanisms can log access violations.

c) **User account lockout:** The auditor should determine if systems and networks can automatically lock user accounts that are the target of attacks.

d) **Intrusion detection and prevention:** The auditor should determine if there are any IDSs or IPSs that would detect authentication-bypass attempts.

e) **Dormant accounts:** The IS auditor should determine if any automated or manual process exists to identify and close dormant accounts.

f) **Shared accounts:** The IS auditor should determine if there are any shared user accounts; these are user accounts that are routinely (or even infrequently) used by more than one person.

g) **System accounts:** The IS auditor should identify all system-level accounts on networks. The IS auditor should determine who has the password for each system account, whether accesses by system accounts are logged, and who monitors those logs.

2. **Auditing Password Management:** Auditing password management requires attention to several key technologies and activities, including the following:

   Password standards: Some of the areas requiring examination are how many characters must a password have and whether there is a maximum length; how frequently must passwords be changed.

3. **Auditing User Access Provisioning:** Auditing the user access provisioning process requires attention to several key activities, including:

   a) **Access request processes:** The IS auditor should identify all user access request processes and determine if these processes are used consistently throughout the organization.

b) **Access approvals:** The IS auditor needs to determine how requests are approved and by what authority they are approved.

c) **New employee provisioning:** The IS auditor should examine the new employee provisioning process to see how a new employee's user accounts are initially set up.

d) **Segregation of Duties (SOD):** The IS auditor should determine if the organization makes any effort to identify segregation of duties. *This may include whether there are any SOD matrices in existence..*

e) **Access reviews:** The IS auditor should determine if there are any periodic access reviews and what aspects of user accounts are reviewed;

4. **Auditing Employee Terminations:** Auditing employee terminations requires attention to several key factors, including:

a) **Termination process:** The IS auditor should examine the employee termination process and determine its effectiveness. *This examination should include understanding on how terminations are performed.*

b) **Access reviews:** The IS auditor should determine if any internal reviews of terminated accounts are performed. *If such reviews are performed, the auditor should determine if any missed terminations are identified and if any process improvements are undertaken.*

c) **Contractor access and terminations:** The IS auditor needs to determine how contractor access and termination is managed and if such management is effective.

Q.No.9. Explain User Access Logs in Audit of Logical Access Controls?

The IS auditor needs to understand the capabilities of the system being audited and determine if the right events are being logged.

a) **Centralized access logs:** The IS auditor should determine if the organization's access logs are aggregated or if they are stored on individual systems.

b) **Access log protection:** The auditor needs to determine if access logs can be altered, destroyed, or attacked to cause the system to stop logging events.

c) **Access log review:** *The auditor should determine if access log reviews take place, who performs them, how issues requiring attention are identified, and what actions are taken when necessary.*

d) **Access log retention:** The IS auditor should determine how long access logs are retained by the organization and if they are back up.

Q.No.10. Explain Investigative Procedures in Audit of Logical Access Controls?

Auditing investigative procedures requires attention to several key activities, including:

a) **Investigation policies and procedures:** This would include who is responsible for performing investigations, where information about investigations is stored, and to whom the results of investigations are reported.

b) **Computer crime investigations:** The IS auditor should understand how internal investigations are transitioned to law enforcement.

c) **Computer forensics:** The auditor should also identify tools and techniques that are available to the organization for the acquisition and custody of forensic data.

Q.No.11. Explain Internet Points of Presence in Audit of Logical Access Controls?

The IS auditor needs to perform a "points of presence" audit to discover what technical information is available about the organization's Internet presence.

Some of the aspects of this intelligence gathering include:

a) **Search engines:** Google, Yahoo!, and other search engines should be consulted to see what information about the organization is available.

b) **Social networking sites:** Social networking sites such as Facebook, LinkedIn, Myspace, and Twitter should be searched to see what employees, former employees, and others are saying about the organization.

c) **Online sales sites:** Sites such as craigslist and eBay should be searched to see if anything related to the organization is sold online.

d) **Domain names:** The IS auditor should verify contact information for known domain names, as well as related domain names.

e) **Justification of Online Presence:** The IS auditor should examine business records to determine on what basis the organization established online capabilities such as e-mail, Internet-facing web sites, Internet e-commerce, Internet access for employees, and so on.

Q.No.12. What is the role of Auditor in Top Management and Information Systems Management Controls?

The major activities that senior management must perform are – **Planning, Organizing, Leading** and **Controlling**. The Role of auditor at each activity is discussed below:

a) **Planning:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.

b) **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources for three reasons:

   i) The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.

   ii) Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.

   iii) Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.

c) **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership - for example, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function.

d) **Controlling:** Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

Q.No.13. Explain the role of Auditor in System Development Management Controls?

Three different types of audits may be conducted during system development process as discussed in the Table

Different types of Audit during System Development Process

Concurrent Audit	Auditors assist the team in improving the quality of systems development for the specific system they are building and implementing.
Post - implementation Audit	Auditors *might be evaluating whether the system needs to be scrapped, continued, or modified in some way.*
General Audit	Auditors evaluate systems development controls overall.

Q.No.14. Explain the role of Auditor in Programming Management Controls?

Audit Trails under Programming Management Controls

Phase	Audit Trails
Planning	They should evaluate whether nature of and extent of planning are appropriate to different types of s/w that are developed or acquired.
Control	They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired.
Design	**i)** Auditors should find out whether programmers use some type of systematic approach to design.
Coding	Auditors should seek evidence - To determine whether programming management ensures that programmers follow structured programming conventions.
Testing	Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.
Operation and Maintenance	Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner.

Q.No.15. Explain the role of Auditor in Data Resource Management Controls?

a) Auditors should determine what controls are exercised to maintain data integrity.

b) They might also interview database users to determine their level of awareness of these controls.

c) Auditors might employ test data to evaluate whether access controls and update controls are working.

Q.No.16. Explain the role of Auditor in Quality Assurance Management Controls?

a) Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.

b) Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.

c) Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

Q.No.17. Explain the role of Auditor in Security Management Controls?

a) Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;

b) Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and

c) Auditors check whether the organizations have opted for an appropriate insurance plan or not.

Q.No.18. Explain the role of Auditor in Operations Management Controls?

a) Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

b) Auditors can use interviews, observations, and review of documentation to evaluate -

i) the activities of documentation librarians;

ii) how well operations management undertakes the capacity planning and performance monitoring function;

iii) the reliability of outsourcing vendor controls;

iv) whether operations management is monitoring compliance with the outsourcing contract; and

Q.No.19. Explain Boundary Controls and its Audit Trails?

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

a) Identity of the would-be user of the system;

b) Authentication information supplied;

c) Resources requested;

d) Action privileges requested;

e) Terminal Identifier;

f) Start and Finish Time;

Accounting Audit Trail: Action privileges allowed/denied.

Operations Audit Trail

a) Resource usage from log-on to log-out time.

b) Log of Resource consumption.

Q.No.20. Explain Input Controls and its Audit Trails?

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**

a) The identity of the person(organization) who was the source of the data;

b) The identity of the person(organization) who entered the data into the system;

c) The time and date when the data was captured;

d) The identifier of the physical device used to enter the data into the system;

e) The account or record to be updated by the transaction;

f) *The standing data to be updated by the transaction;*

2. **OPERATIONS AUDIT TRAIL**

a) Time to key in a source document or an instrument at a terminal;

b) Number of read errors made by an optical scanning device;

c) Number of keying errors identified during verification;

d) Frequency with which an instruction in a command language is used

Q.No.21. Explain Communication Controls and its Audit Trails?

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
   a) Unique identifier of the source/sink node;
   b) Time and date at which the message was received by the sink node;
   c) Time and date at which node in the network was traversed by the message; and
   d) Message sequence number; and the image of the message received at each node traversed in the network.
2. OPERATIONS AUDIT TRAIL
   a) Number of messages that have traversed each link and each node;
   b) Log of system restarts; and
   c) Message transit times between nodes and at nodes.

Q.No.22. Explain Processing Controls and its Audit Trails?

The audit trail maintains the chronology of events from the time data is received from the input to the time data is dispatched output subsystems.

1. ACCOUNTING AUDIT TRAIL
   a) To trace and replicate the processing performed on a data item.
   b) To follow triggered transactions from end to end by monitoring input data entry, intermediate results and output data values.
   c) 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.
   d) 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) A comprehensive log on hardware consumption - CPU time used, secondary storage space used, and communication facilities used.
   b) A comprehensive log on software consumption - compilers used, subroutine libraries used, file management facilities used, and communication software used.

Q.No.23. Explain Database Controls and its Audit Trails?

The audit trail maintains the chronology of events that occur to the database.

1. ACCOUNTING AUDIT TRAIL
   a) To confirm whether an application properly accepts, processes, and stores information.
   b) To attach a unique time stamp to all transactions.
   c) To attach before-images and after-images of the data item on which a transaction is applied to the audit trail.
   d) Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.
2. OPERATIONS AUDIT TRAIL: To maintain a chronology of resource consumption events that affects the database.

Q.No.24. Explain Output Controls and its Audit Trails?

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
   a) What output was presented to users;
   b) Who received the output;
   c) When the output was received;
   d) 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.

ORGANIZATION STRUCTURE AND RESPONSIBILITIES

Q.No.25. What is Job Title? How Job Title helps organizations in different ways?

A 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.

Job titles in IT are quite consistent across organizations. This consistency helps organizations in several ways:

a) **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.

b) **Compensation Baselining:** Because of the chronic shortage of talented IT workers, organizations are forced to be more competitive when trying to attract new workers. The use of standard job titles makes the task of comparing compensation far easier.

c) **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.

Q.No.26. Explain different job titles in Executive Management level?

Executive managers are the chief leaders and policymakers in an organization.

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

b) **CTO (Chief Technical Officer):** This position is usually responsible for an organization's overall technology strategy.

c) **CSO (Chief Security Officer):** This position is responsible for all aspects of security, including information security, physical security, and possibly executive protection.

d) **CISO (Chief Information Security Officer):** This position is responsible for all aspects of data-related security.

e) **CPO (Chief Privacy Officer):** This position is responsible for the protection and use of personal information.

Q.No.27. Explain different job titles in Software Development?

Positions in software development are involved in the design, development, and testing of software applications.

a) **Systems Architect:** This position is usually responsible for the overall information systems architecture in the organization.

b) **Systems Analyst:** This position may develop technical requirements, program design, and software test plans.

c) **Software Developer, Programmer:** This position develops application software.

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

Q.No.28. Explain different job titles in Data Management level?

Positions in data management are responsible for developing and implementing database designs and for maintaining databases.

a) **Database Architect:** This position develops logical and physical designs of data models for applications.

b) **Database Administrator (DBA):** This position builds and maintains databases designed by the database architect.

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

Q.No.29. Explain different job titles in Network Management level?

Positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks.

a) **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.

b) **Network Engineer:** This position builds and maintains network devices such as routers, switches, firewalls, and gateways.

c) **Network Administrator:** This position performs routine tasks in the network such as making minor configuration changes and monitoring event logs.

d) **Telecom Engineer:** Positions in this role work with telecommunications technologies such as data circuits, phone systems, and voice mail systems.

Q.No.30. Explain different job titles in Systems Management level?

Positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems.

a) **Systems Architect:** responsible for the overall architecture of systems.

b) **Systems Engineer:** responsible for designing, building, and maintaining servers and server operating systems.

c) **Storage Engineer:** responsible for designing, building, and maintaining storage subsystems.

d) **Systems Administrator:** responsible for performing maintenance and configuration operations on systems.

Q.No.31. Explain different job titles in General Operations

Positions in operations are responsible for day-to-day operational tasks that may include networks, servers, databases, and applications.

a) **Operations Manager:** responsible for overall operations that are carried out by others. Responsibilities will include establishing operations shift schedules.

b) **Operations Analyst:** responsible for the development of operational procedures; examining the health of networks, systems, and databases;

c) **Controls Analyst:** responsible for monitoring batch jobs, data entry work, and other tasks to make sure that they are operating correctly.

d) **Systems Operator:** responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.

e) **Data Entry:** responsible for keying batches of data from hard copy sources.

f) **Media Librarian:** responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

Q.No.32. Explain different job titles in Security Operations?

Positions in security operations are responsible for designing, building, and monitoring security systems.

a) **Security Architect:** This position is responsible for the design of security controls and systems
b) **Security Engineer:** This position is responsible for designing, building, and maintaining security services and systems that are designed by the security architect.
c) **Security Analyst:** This position is responsible for examining logs from firewalls, intrusion detection systems, and audit logs from systems and applications.
d) **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.
e) **Security Auditor:** This position is responsible for performing internal audits of IT controls to ensure that they are being operated properly.

Q.No.33. Explain different job titles in Service Desk?

a) Positions at the service desk are responsible for providing front line support services to IT and its customers.
b) **Help desk Analyst:** This position is responsible for providing front line user support services to personnel in the organization.
c) **Technical Support Analyst:** This position is responsible for providing technical support services to other IT personnel, and perhaps also to IT customers.

SEGREGATION OF DUTIES

Q.No.34. Explain about SEGREGATION OF DUTIES? Explain Some Examples of Segregation of Duties Controls?

Segregation of Duties (SOD), also known as separation of duties, ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation or exposure of sensitive data.

Some Examples of Segregation of Duties Controls

a) **Transaction Authorization:** Information systems can be programmed or configured to require two (or more) persons to approve certain transactions.
b) **Split custody of high-value assets:** Assets of high importance or value can be protected using various means of split custody. *For example, a password to an encryption key that protects a highly-valued asset can be split in two halves, one half assigned to two persons, and the other half assigned to two persons, so that no single individual knows the entire password.*
c) **Workflow:** Applications that are workflow-enabled can use a second (or third) level of approval before certain high-value or high-sensitivity activities can take place.
d) **Periodic reviews:** IT or internal audit personnel can periodically review user access rights to identify whether any segregation of duties issues exist.

Q.No.35. Explain the Application Areas of Computer Based Applications? (SELF STUDY)

Major areas of computer based applications are:

1. **Finance and Accounting:** The main goal of this subsystem is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget.

2. **Marketing and Sales:** The objective of this subsystem is to maximize the sales and ensure customer satisfaction.
3. **Production or Manufacturing:** The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service.
4. **Inventory /Stores Management:** The inventory management system is designed with a view to keeping the track of materials in the stores.
5. **Human Resource Management:** Effective and efficient utilization of manpower in a dispute-free environment in this key functional area ensures to facilitate disruption free and timely services in business.

Q.No.36. How Telecommunication can create value to business?

a) **Time compression:** Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.
b) **Overcoming geographical dispersion:** Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit.
c) **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.

Q.No.37. What is ORGANIZATION STRUCTURE? What are the conditions which can change the ORGANIZATION STRUCTURE?

In most organizations, the organization chart is a living structure that changes frequently, based upon several conditions including the following:

a) **Market conditions:** Changes in market positions can cause an organization to realign its internal structure in order to strengthen itself.
b) **Regulation:** New regulations may induce an organization to change its organizational structure.
c) **Available talent:** When someone leaves the organization, a space opens in the org chart that often cannot be filled right away. Instead, senior management will temporarily change the structure of the organization by moving the leaderless department under the control of someone else.

4. E-COMMERCE, M-COMMERCE & EMERGING TECHNOLOGIES

INTRODUCTION TO E-COMMERCE

Q.No.1. What is E-commerce? Explain?

1. E - Commerce is the process of doing business electronically.
2. It refers to the use of Technology to in the form of Computers, Desktops, Mobile Applications, etc. enhance the processing of commercial transactions between a company, its customers and its business partners.

Q.No.2. Explain the steps involved in E-Commerce Transaction?

STEP 1: Go to website (like www.snapdeal.com, www.flipkart.com, www.amazon.in, etc) and create your user ids. Those who have social media ids, can directly link through those ids.

STEP 2: Select the type of product you wish to buy.

STEP 3: From the products listed, user needs to select the correct product s/he needs to buy.

STEP 4: User makes the final choice and goes for making payment online.

STEP 5: At the time of making payment, e-commerce vendor shows all details including the product being bought and the final price of the same for review of the customer and confirmation before final payment.

STEP 6: Once user goes for online payment, the e-commerce vendor displays the payment options. Payment options can be cash on delivery, Payment by Debit/Credit Cards, etc.

STEP 7: Once the user selects the payment option, he is directed to the payment gateway where he enters the OTP or the password and the payment is made by the Credit Card.

STEP 8: Based on the delivery terms, the product is delivered to the customer in specified time.

Q.No.3. Explain the Benefits of E-Business W.r.t Customer / Individual / User? (B)

BENEFITS TO CUSTOMER / INDIVIDUAL / USER:

a) **Convenience:** Every product at the tip of individual's fingertips on internet.

b) **Time saving:** No. of operations that can be performed both by potential buyers and sellers increase.

c) **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.

d) **Easy to find reviews:** There are often reviews about a particular site or product from the previous customers which provides valuable feedback.

e) **Coupon and Deals:** There are discount coupons and reward points available for customers to encourage online transaction.

f) **Anytime Access:** Even midnight access to the e commerce platforms is available which brings in customer suitability.

Q.No.4. Explain the Benefits of E-Business W.r.t Business / Sellers?

BENEFITS TO BUSINESS / SELLERS:

a) **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.

b) **Recurring payments made easy:** Each business has number of operations being homogeneous. Brings in uniformity of scaled operations.

c) **Instant Transaction:** The transactions of e commerce are based on real time processes. This has made possible to crack number of deals.

d) **Provides a dynamic market:** Since there are several players, providing a dynamic market which enhances quality and business.

e) **Reduction in costs:** To suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.

f) **Efficiency improvement due to:** Reduction in time to complete business transactions, particularly from delivery to payment.

g) **Creation of new markets:** This is done through the ability to easily and cheaply reach potential customers.

h) **Easier entry into new markets:** This is especially into geographically remote markets, for enterprises regardless of size and location.

i) **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.

j) **Elimination of Time Delays:** Faster time to market as business processes are linked, thus enabling seamless processing and eliminating time delays.

COMPONENTS OF E - COMMERCE

Q.No.5. What are the components of E-commerce?

E-COMMERCE COMPONENTS INCLUDE THE FOLLOWING:

a) **User:** This may be individual / organization or anybody using the e-commerce platforms.

b) **E-commerce Vendors:** This is the organization / entity providing the user, goods/ services asked for. For example: www.flipkart.com.

c) **Technology Infrastructure:** The computers, servers, database, mobile apps, digital libraries, data interchange enabling the e-commerce transactions.

d) **Internet / Network:** Internet connectivity is important for any e-commerce transactions to go through.

e) **Web portal:** This shall provide the interface through which an individual /organization shall perform e-commerce transactions.

f) **Payment Gateway:** The payment mode through which customers shall make payments. Ex: SBI BUDDY or PAYTM, Cash on Delivery (COD).

ARCHITECTURE OF NETWORKED SYSTEMS

Q.No.6. What is architecture of networked systems? Explain the types?

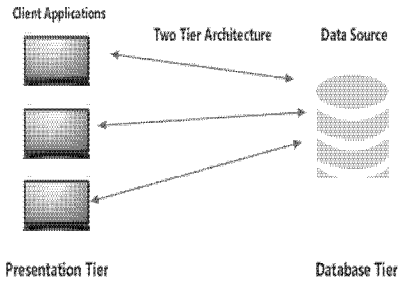
Architecture is a term to define the style of design and method of construction. In e-commerce, it denotes the way network architectures are build.

Networked systems can have two types of architecture namely: Two tier and Three tier.

a) **Two Tier Client Server:** In a Two tier network, client (user) sends request to Server and the Server responds to the request by fetching the data from it. The Two-tier architecture is divided into two tiers- Presentation Tier and Database Tier.

   i) **Presentation Tier (Client Application/Client Tier):** This is the interface that allows user to interact with the e-commerce / m-commerce vendor. User can login to an e-commerce vendor through this tier.

   ii) **Database Tier (Data Tier):** The product data / price data and other related data are kept here



   iii) ADVANTAGES:

   - The system performance is higher because business logic and database are physically close.
   - Since processing is shared between the client and server, more users could interact with system.
   - By having simple structure, it is easy to setup and maintain entire system smoothly.

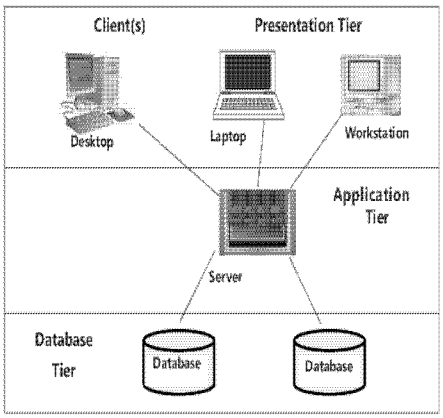
   iv) DISADVANTAGES:

   - Performance deteriorates if number of users' increases.
   - There is restricted flexibility and choice of DBMS, since data language used in server is proprietary to each vendor.

b) **Three Tier Client-Server:** Three-tier architecture is a client-server architecture in which the functional process logic, computer data storage and user interface are developed and maintained as independent modules on separate platforms. The three-tier architecture are as follows:

i) **Presentation Tier:** Occupies the top level and displays information related to services available on a website.

ii) **Application Tier:** Also, called the Middle Tier, Logic Tier, Business Logic or Logic Tier; It controls application functionality by performing detailed processing.



iii) **Database Tier:** This tier houses the database servers where information is stored and retrieved.

iv) **ADVANTAGES OF THREE-TIER SYSTEMS:**

- **Clear separation of user-interface-control and data presentation from application-logic:** Through this separation more clients can have access to a wide variety of server applications.
- **Dynamic load balancing:** If bottlenecks in terms of performance occur, the server process can be moved to other servers at runtime.
- **Change management:** It is easy and faster to exchange a component on the server than to furnish numerous PCs with new program versions.

v) **DISADVANTAGES OF THREE-TIER SYSTEM:**

- It creates an increased need for network traffic management, server load balancing, and fault tolerance.
- Current tools are relatively immature and are more complex.
- Maintenance tools are currently inadequate for maintaining server libraries.

Q.No.7. What is M-Commerce? What are the three layers in M-Commerce?

M-Commerce (Mobile Commerce): M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs).

The three layers are

S. No.	Layer	Includes	Purpose
1	Client / User Interface	Mobile Web Browser and Internet.	This layer helps the e-commerce customer connect to e-commerce merchant.
2	Application Layer	Application Server and back end server.	This layer allows customer to check the products available on merchant's website.
3	Database Layer	The information store house, where all data relating to products, price it kept.	This layer is accessible to user through application layer.

RISKS & CONTROLS

Q.No.8. What are the Risks associated with e-commerce?

Risk: **Risk** is possibility of loss. Risks associated with e-commerce transactions are high compared to general internet activities. These include the following:

a) **Privacy and Security:** Comes in the point of hacking. There are often issues of security and privacy due to lack of personalized digital access and knowledge.

b) **Quality issues:** There are quality issues raised by customers as the original product differs from the one that was ordered.

c) **Delay in goods and Hidden Costs:** When goods are ordered from another country, there are hidden costs enforced by Companies.

d) **Security and credit card issues:** There is possibility of credit cards and debit cards duplication which poses a security threat.

e) **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.

f) **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.

g) **Lack of authenticity of transactions:** The electronic documents that are produced during an e-Commerce transaction may not be authentic and reliable.

h) **Data Loss or theft or duplication:** The data transmitted over the Internet may be lost, duplicated, tampered with or replayed.

i) **Attack from hackers:** Web servers used for e-Commerce maybe vulnerable to hackers.

Q.No.9. What is Internal Control? Who require controls in the chain of e-business environment?

Internal control: Internal control is a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies.

In an e-business environment, controls are necessary for all persons in the chain, including-

a) **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.

b) **Sellers / Buyers / Merchants:** Many e-commerce businesses have lost huge amount of money as they did not have proper controls put in place.

c) **Government:** Governments have few critical concerns namely:

   i) Tax accounting of all products / services sold.

   ii) All products / services sold are legal. There have been instances where narcotics drugs have found to be sold and bought through electronic means.

d) **Network Service Providers:** They need to ensure availability and security of network. Any downtime of network can be disastrous for business.

e) **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.

f) **Logistics Service Providers:** Logistics service providers are the ones who are finally responsible for timely product deliveries.

g) **Payment Gateways:** E-commerce vendors' business shall run only when their payment gateways are efficient, effective and foolproof.

Q.No.10. What controls are needed for various participants in an e-commerce environment?

Each participant needs to put in place policies, practices and procedures to protect from e-commerce / m-commerce related risks. These will include the following:

1. **Educating the Participant about the Nature of Risks:** Every participant needs to be educated / sensitized towards risk associated with such transactions. Organizations need to put in place infrastructure / policy guidelines for the same.
2. **Communication of Organizational Policies to its Customers:** To avoid customer dissatisfaction and disputes, it is necessary to make the following information clear throughout your website:
   a) **Privacy Policies:** These should be available through links on any website.
   b) **Information security:** Create a page that educates customers about any security practices and controls.

c) **Shipping and billing policies:** These should be clear, comprehensive and available through a link on the home page during online purchase.

d) **Refund policies:** Establish and display a clear, concise statement of a customer's refund and credit policy.

3. **Ensure Compliance With Industry Body Standards:** All e-Commerce organizations are required to be complying with and adhere to the rules outlined by the law of land. In India Reserve Bank of India, has been releasing these standards from time to time.

4. **Protect your e-commerce business from intrusion:**

a) **Viruses:** Check your website daily for viruses, the presence of which can result in the loss of valuable data.

b) **Hackers:** Use software packages to carry out regular assessments of how vulnerable your website is to hackers.

c) **Passwords:** Ensure employees change these regularly and that passwords set by former employees of your organization are defunct.

d) **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.

e) **Sensitive data:** Consider encrypting financial information and other confidential data (using encryption software).

Q.No.11. What are the control objectives in e-business/ e-commerce? Explain?

The control objectives in E-Business are:

a) **Prevent organizational costs of data Loss:** Data is a critical resource of an organization for its present and future process.

b) **Prevent loss from incorrect decision making:** The high-level decisions require accurate data to make quality decision rules.

c) **Prevent loss of Computer Hardware, Software and Personnel:** These are critical resources of an organization which has a credible impact on its infrastructure and business competitiveness.

d) **Prevent from high costs of computer Error**: A data error during entry or process would cause great damage.

e) **Safeguard assets from unauthorized access:** The information system assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorized access.

f) **Ensure data integrity:** The extent of access to the information and the value of data to the business from the perspective of the decision maker, competition and the market environment.

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

h) **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.

Q.No.12. Write about several IT Risks as per SA (Standard on Auditing) 315?

SA 315 recognizes that IT poses specific risks to an entity's internal control in the form of the following:

a) Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.

b) Unauthorized access to data that may result in destruction of data or improper changes to data.

c) The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.

d) Unauthorized changes to data in master files.

e) Unauthorized changes to systems or programs.

f) Failure to make necessary *changes to systems or programs.*

Q.No.13. What type of controls are being used for addressing key cyber security risks?

The controls addressing key cyber security risks are as under:

a) A Network Diagram detailing servers, databases, hubs, routers, internal and external network, etc.

b) List of the Digital Assets used by the Company and the IT Managers responsible for the protection for those digital assets along with the physical location of those assets.

c) Any incidents of cyber security breach which occurred and the actions taken and controls built in to avoid them from occurring again.

d) Are the IT managers responsible for the safeguarding of the assets from cyber- attacks, adequately skilled and trained to perform the functions.

e) 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.

f) Adequate approvals exist before the access is granted to any IT resources.

GUIDELINES AND LAWS GOVERNING E-COMMERCE

Q.No.14. What are the policy Guidelines for E-Commerce?

E-commerce / m-commerce policy guidelines for business are:

1. **Billing:** The issues are :
   a) Format of bill
   b) The details to be shared in bills
   c) Applicable GST.
2. **Product guarantee / warranty:** Proper display of product guarantee / warranty online as well as documents sent along with the products.
3. **Shipping:** The shipping time, frequency of shipping, the packing at time of shipping, all these needs to be put in policy documents.
4. **Delivery:** Policy needs to be defined for:
   a) Which mode of delivery to be chosen?
   b) When deliveries to be made?
   c) Where deliveries to be made?
5. **Return:** Policy for return of goods needs to be put in place defining:
   a) Which goods to be accepted in return?
   b) The number of days within which returns can be accepted.
   c) The process of verifying the authenticity of products received back.
6. **Payment:** Policy guidelines need to be created for the following payment related issues:
   a) Mode of payment.
   b) For which products, specific payment mode shall be there. Organisation restricts cash on delivery for few consumable products.

Q.No.15. What are the commercial laws applicable to e-commerce and m-commerce transactions?

Following commercial laws are applicable are.

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 of 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 Custom Act, 1962:** The act that defines import / export of goods / services from India and provides for levy of appropriate customs duty. India being a signatory to General Agreement on Trade and Tariff (GATT) under World Trade Organisation, cannot levy any custom duty that GATT non-compliant.

f) **The Goods and Services Tax Act, 2017 (GST):** This Act 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.

g) **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.

h) **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.

i) **Foreign Exchange Management Act (FEMA 1999):** The law to regulate foreign direct investments, flow of foreign exchange in India. The law has important implications for e-commerce / m-commerce business. With a view to promote foreign investment, as per regulations framed under Foreign Exchange Management Act, (FEMA) 1999.

j) **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.

Q.No.16. What are the Special Laws for governing E-Commerce?

E-commerce are covered under few other laws as these transactions are done electronically.

1. **Information Technology Act, 2000**: The law is applicable to all online transactions in India, and provides for penalties, prosecution for non-compliances. The important issues dealt in by the law includes:
   - **a)** Legality of products / services being offered online.
   - **b)** Data Protection
   - **c)** Protecting Your Customer's Privacy Online
   - **d)** Online Advertising Compliance
   - **e)** Compliance with Information Technology Act, provisions.

2. **Reserve Bank of India, 1932:** Reserve Bank of India (RBI), from time to time frames guidelines to be followed by e-commerce / m-commerce merchants allowing online payments through various modes. The merchant needs to comply with these guidelines. For example:
   - **a)** The conversion of all Credit / Debit cards to be made CHIP based.
   - **b)** An OTP / PIN for all transactions done on point of sale machines through debit / credit cards.

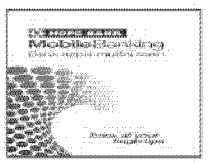
DIGITAL PAYMENT

Q.No.17. What is Digital Payment? What are New Methods of Digital Payment?

It is also called electronic payment. No hard cash is involved in the digital payments. All the transactions in digital payments are completed online.

NEW METHODS OF DIGITAL PAYMENT

a) **UPI Apps:** Unified Payment Interface 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. User must register for mobile banking to use UPI apps. Currently, this service is only available for android phone users. There are too many good UPI apps available such as BHIM, SBI UPI app, HDFC UPI app.



b) **Immediate Payment Service (IMPS):** It is an instant interbank electronic fund transfer service through mobile phones. It is also being extended through other channels such as ATM, Internet Banking, etc.

c) **Mobile Apps: BHIM (Bharat Interface for Money)** is a Mobile App developed by National Payments Corporation of India (NPCI) based on UPI (Unified Payment Interface). It is built on the Immediate Payment Service infrastructure and allows the user to instantly transfer money between the bank 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

d) **Mobile Wallets:** It is defined as virtual wallets that stores payment card information on a mobile device. Mobile Wallets provide a convenient way for a user to make-in-store payments .There are mobile wallets like PayTm, Freecharge, SBI Buddy, MobiKwick etc.

e) **Aadhar Enabled Payment Service (AEPS):** Customer needs only his or her Aadhaar number to pay to any merchant. AEPS allows bank to bank transactions. Customers will need to link their AADHAR numbers to their bank accounts.

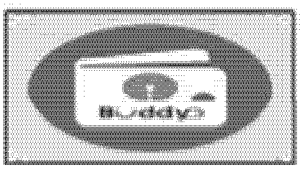
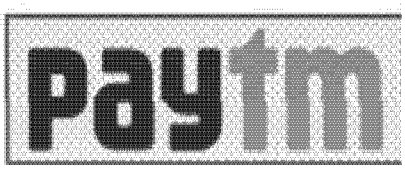
f) **Unstructure Supplementary Service Data (USSD):** USSD banking or *99# Banking is a mobile banking based digital payment mode. User does not need to have a smartphone or internet connection to use USSD banking. S/he can easily use it with any normal feature phone. S/he can use this service for checking balance, sending money, changing Mobile Banking Personal Identification number (MPIN).etc.

Q.No.18. What are the Traditional Methods of Digital Payment?

TRADITIONAL METHODS OF DIGITAL PAYMENT

a) **E-Wallet:** E-wallet or mobile wallet is the digital version of physical wallet with more functionality. User can keep his / her money in an E-wallet and use it when needed. Use the E-wallets to recharge phone, pay at various places and send money to friends.

   EX: State bank buddy, ICICI Pockets, Freecharge, Paytm etc.

b) **Cards:** Cards are provided by banks to their account holders. These have been the most used digital payment modes till now. Various types of cards are as follows:

   i) **Credit Cards:** A small plastic card issued by a bank, or issuer etc., allowing the holder to purchase goods or services on credit. User of the card makes payment to card issuer at end of billing cycle which is generally a monthly cycle. Credit Card issuer charge customers per transactions / 5% of transaction as transaction fees.

   ii) **Debits Cards:** A small plastic card issued by a bank. Allowing the holder to purchase goods or services on credit. In this mode of payment, the buyer's cash flow is immediately affected that as soon as payment is authorized buyers account is debited.

c) **Net Banking:** In this mode, the customers log to his / her bank account and makes payments. All public sectors, large private sector banks allow net banking facilities to their customers.

Q.No.19. List out the Advantages and Drawbacks of Digital Payments?

ADVANTAGES OF DIGITAL PAYMENTS:

a) **Easy and convenient:** Digital payments are easy and convenient. Person do not need to take loads of cash with themselves.

b) **Pay or send money from anywhere:** With digital payment modes, one can pay from anywhere anytime.

c) **Discounts from taxes:** Government has announced many discounts to encourage digital payments. User get 0.75% discounts on fuels.

d) **Written record:** These are automatically recorded in passbook or inside E-Wallet app. This helps to maintain record, track spending and budget planning.

e) **Less Risk:** 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.

DRAWBACKS OF DIGITAL PAYMENTS:

a) **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.

b) **The risk of data theft:** Hackers can hack the servers of the bank or the E-Wallet a customer is using and easily get his/her personal information.

c) **Overspending:** Digital payment modes are used, one has an access to all his/her money that can result in overspending.

COMPUTING TECHNOLOGIES

Q.No.20. What is Virtualization? What are different Application Areas of Virtualization?

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.

Application Areas of Virtualization

a) **Server Consolidation:** Virtual machines are used to consolidate many physical servers into fewer servers, which in turn host virtual machines. This is also known as "Physical-to-Virtual" or 'P2V' transformation.

b) **Disaster Recovery:** Virtual machines can be used as "hot standby" environments for physical production servers. This changes the classical "backup-and- restore" philosophy, by providing backup images that can "boot" into live virtual machines, capable of taking over workload for a production server experiencing an outage.

c) **Testing and Training:** Virtualization can give root access to a virtual machine. This can be very useful such as in kernel development and operating systems.

d) **Portable Applications:** Portable applications are needed when running an application from a removable drive, without installing it on the system's main disk drive.

e) **Portable Workspaces:** Recent technologies have used virtualization to create portable workspaces on devices like iPods and USB memory sticks.

Q.No.21. Explain the Common Types of Virtualization?

Hardware Virtualization:

a) 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.

b) The software that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Manager.

Network Virtualization: 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.

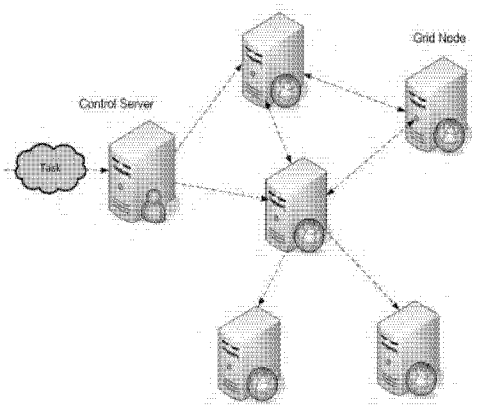
Storage Virtualization:

a) 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.

b) The servers connected to the storage system aren't aware of where the data really is.

Q.No.22. What is Grid Computing? Explain different Application Areas of Grid Computing?

1. Grid Computing is a computer network in which each computer's resources are shared with every other computer in a communication system.
2. Processing power, memory and data storage are allocated to authorized users then resources are accessed by users to perform specific tasks.
3. In the ideal grid computing system, every resource is shared, turning a computer network into a powerful supercomputer performance.



Application Areas of Grid Computing

a) Civil engineers collaborate to design, execute, & analyze shake table experiments.

b) An insurance company mines data from partner hospitals for fraud detection.

c) An enterprise configures internal & external resources to support e-Business workload.

d) Large-scale science and engineering computing resources which are geographically and organizationally dispersed could use Grid.

Q.No.23. Explain different Benefits of Grid Computing?

a) **Making use of Underutilized Resources:** Grid computing provides a framework for exploiting these underutilized resources and thus has the possibility of substantially increasing the efficiency of resource usage.

b) **Resource Balancing:** An unexpected peak can be routed to relatively idle machines in the grid;

c) **Parallel CPU Capacity:** A CPU-intensive grid application can be thought of as many smaller sub-jobs, each executing on a different machine in the grid.

d) **Virtual resources and virtual organizations for collaboration:** The users of the grid can be organized dynamically into a number of virtual organizations, each with different policy requirements. These virtual organizations can share their resources, collectively as a larger grid.

e) **Access to additional resources:** In addition to CPU and storage resources, a grid can provide access to other resources such as bandwidth to perform a complex task.

f) **Reliability:** The machines also use duplicate processors in such a way that when they fail, one can be replaced without turning the other off.

Q.No.24. What type of resources used by all users of the grid? Explain?

Resources may be used by all users of the grid are:

a) **Computation:** The most common resource is Computing Cycles provided by the processors of the machines on the grid .

b) **Storage:** Storage can be memory attached to the processor or it can be other permanent storage media.

c) **Communications:** The bandwidth available for communications can often be a critical resource that can limit utilization of the grid.

d) **Software and Licenses:** Some software licensing arrangements permit the software to be installed on all of the machines of a grid but may limit the number of installations that can be simultaneously used at any given instant.

e) **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.

Q.No.25. What are the constraints to be taken to develop secured grid?

Following constraints are taken from the characteristics of grid environment and application.

a) **Single Sign-on:** A user should authenticate once and they should be able to acquire resources.

b) **Protection of Credentials:** User passwords, private keys, etc. should be protected.

c) **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.

d) **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.

e) **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.

f) **Support for multiple implementations:** There should be a security policy which should provide security to multiple sources based on public and private key cryptography.

Q.No.26. What is cloud computing? What are the Characteristics of Cloud Computing?

1. A cloud is a collection of servers, applications, databases, documents, agreements, spread sheets, storage capacity etc. which allows organizations to share these resources from anywhere.
2. Cloud Computing is the use of various services, such as software development platforms, servers, storage, and software, over the Internet, often referred to as the "cloud."
3. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.
4. CHARACTERISTICS:
   a) **Elasticity and Scalability:** Cloud computing gives us the ability to expand and reduce resources according to the specific service requirement.
   b) **Pay-per-Use:** We pay for cloud services only when we use them, either for the short term or for a longer duration.
   c) **On-demand:** Because we invoke cloud services only when we need them, they are not permanent parts of the IT infrastructure.
   d) **Resiliency:** The resiliency of a cloud service offering can completely isolate the failure of server and storage resources from cloud users.
   e) **Multi Tenancy:** Public cloud service providers often can host the cloud services for multiple users within the same infrastructure.
   f) **Workload Movement:** This characteristic is related to resiliency and cost considerations. Here, cloud-computing providers can migrate workloads across servers both inside the data center and across data centers (even in a different geographic area).

Q.No.27. What are the Advantages and disadvantages of Cloud Computing?

ADVANTAGES OF CLOUD COMPUTING

a) **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.
b) **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.
c) **Globalize the workforce:** People worldwide can access the cloud with Internet connection.
d) **Streamline business processes:** Getting more work done in less time with less resources are possible.
e) **Reduce capital costs:** Not required to spend huge money on hardware, software, or licensing fees.
f) **Pervasive accessibility:** Data and applications can be accesses anytime, anywhere, using any smart computing device, making our life so much easier.
g) **Monitor projects more effectively:** It is feasible to confine within budgetary allocations and can be ahead of completion cycle times.
h) **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.
i) **Minimize maintenance and licensing software:** As there is no too much of non-premise computing resources, maintenance becomes simple and updates and renewals of software systems rely on the cloud vendor or provider.
j) **Improved flexibility:** It is possible to make fast changes in our work environment without serious issues at stake.

DRAWBACKS OF CLOUD COMPUTING

a) If Internet connection is lost, the link to the cloud and thereby to the data and applications is lost.

b) Security is a major concern as entire working with data and applications depend on other cloud vendors or providers.

c) cloud does not permit the control on resources as these are not owned by the user or customer.

d) Depending on the cloud vendor or provide, customers may have to face restrictions on the availability of applications, operating systems and infrastructure options.

TYPES OF CLOUDS

Q.No.28. What is Private Cloud? Explain different Characteristics of Private Cloud? Discuss several advantages and disadvantages?

1. **PRIVATE CLOUD:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits.
2. **CHARACTERISTICS OF PRIVATE CLOUD:**
   a) **Secure:** The private cloud is secure as it is deployed and managed by the organization itself, and hence there is least chance of data being leaked out of the cloud.
   b) **Central Control:** As usually the private cloud is managed by the organization itself, there is no need for the organization to rely on anybody and it is controlled by the organization itself.
   c) **Weak Service Level Agreements (SLAs):** SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider in private cloud.
3. **ADVANTAGES OF PRIVATE CLOUD:**
   a) It improves average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies.
   b) It provides a high level of security and privacy to the user.
   c) It is small and controlled and maintained by the organization.
4. **Limitation of Private Cloud** is that IT teams in the organization may have to invest in buying, building and managing the clouds independently. Budget is a constraint in private clouds.

Q.No.29. What is public cloud? Explain Characteristics of Public Cloud? Discuss several advantages and disadvantages of public cloud?

1. **PUBLIC CLOUD:** The public cloud is the cloud infrastructure that is provisioned for open use by the general public and the services are offered on pay-per-use basis.
2. **CHARACTERISTICS OF PUBLIC CLOUD:**
   a) **Highly Scalable:** The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are considered to be scalable.
   b) **Affordable:** The cloud is offered to the public on a pay-as-you-go basis;
   c) **Less Secure:** Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.
   d) **Highly Available:** It is highly available because anybody from any part of the world can access the public cloud with proper permission.
   e) **Stringent SLAs:** As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.

3. ADVANTAGES OF PUBLIC CLOUD:
   a) It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
   b) There is no need for establishing infrastructure for setting up and maintaining the cloud.
   c) Strict SLAs are followed.
   d) There is no limit for the number of users.
4. **Limitation of Public cloud** is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen

Q.No.30. What is hybrid cloud? Explain Characteristics of Cloud? Discuss several advantages and disadvantages of Hybrid cloud?

1. HYBRID CLOUD: This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments.
2. CHARACTERISTICS OF HYBRID CLOUD:
   a) **Scalable:** As the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable.
   b) **Partially Secure:** The hybrid cloud thus cannot be fully termed as secure but as partially secure.
   c) **Stringent SLAs:** Overall the SLAs are more stringent than the private cloud and might be as per the public cloud service providers.
   d) **Complex Cloud Management:** Cloud management is complex as it involves more than one type of deployment models and also the number of users is high.
3. Advantages of Hybrid Cloud
   a) It is highly scalable and gives the power of both private and public clouds.
   b) It provides better security than the public cloud.
4. **Limitation of Hybrid Cloud** is that the security features are not as good as the private cloud and complex to manage.

Q.No.31. What is community cloud? What are the Characteristics of Community Cloud? Discuss several advantages and disadvantages of community cloud?

1. COMMUNITY CLOUD: 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.
2. CHARACTERISTICS OF COMMUNITY CLOUD:
   a) **Collaborative and Distributive Maintenance:** In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
   b) **Partially Secure:** This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.
   c) **Cost Effective:** As the complete cloud if being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.
3. ADVANTAGES OF COMMUNITY CLOUD:
   a) It allows establishing a low-cost private cloud.
   b) It allows collaborative work on the cloud.
   c) It allows sharing of responsibilities among the organizations.

d) It has better security than the public cloud.

4. **Limitation of the Community Cloud** is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud.

CLOUD COMPUTING SERVICE MODELS

Q.No.32. What is Infrastructure as a Service (IaaS) model? Explain Characteristics of IaaS?

Infrastructure as a Service, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand.

CHARACTERISTICS OF LAAS:

a) **Web access to the resources:** The IaaS model enables the IT users to access infrastructure resources over the Internet.

b) **Centralized Management:** The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.

c) **Elasticity and Dynamic Scaling:** The usage of resources can be increased or decreased according to the requirements.

d) **Shared infrastructure:** IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.

e) **Metered Services:** The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

Q.No.33. Explain about Platform as a Service (PaaS) model?

1. **Platform as a Service** model provides the users the ability to develop and deploy an application on the development platform provided by the service provider.
2. 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.
3. For example- Google AppEngine, Windows Azure Compute etc.

Q.No.34. Explain about Software as a Service (SaaS) model?

1. **Software as a Service (SaaS)** provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.
2. Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure.
3. For example, one can make his/her own word document in Google docs online.

Q.No.35. What is Mobile Computing? Explain different components of 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

The key components of Mobile Computing are:

a) **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.

b) **Mobile Hardware:** Mobile Hardware includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones.

c) **Mobile Software:** It is the operating system of that appliance and is the essential component that makes the mobile device operates.

Q.No.36. Write about the Benefits of Mobile Computing?

a) 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.

b) It facilitates access to corporate services and information at any time, from anywhere.

c) It provides remote access to the corporate Knowledge base at the job location.

d) It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Q.No.37. Write about the Limitations of Mobile Computing?

a) **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections

b) **Security Standards:** One can easily attack the VPN through a huge number of networks interconnected through the line.

c) **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power.

d) **Transmission interferences:** Signal receiving in tunnels, some buildings, and rural areas is often poor.

e) **Potential health hazards:** Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.

f) **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use.

Q.No.38. What is Green Computing or Green IT? What are the Best Practices of Green Computing?

It is the study and practice of establishing/ using computers and IT resources in a more efficient and environmentally friendly and responsible way.

Green Computing Best Practices

1. **Develop a sustainable Green Computing plan**
   - ***a)*** Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment.
   - ***b)*** *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**
   - **a)** Dispose e-waste according to central, state and local regulations.
   - **b)** Manufacturers must offer safe end-of-life management and recycling options when products become unusable.
3. **Make environmentally sound purchase decisions**
   - **a)** Purchase of desktop computers, notebooks and monitors based on environmental attributes.
   - ***b)*** *Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.*

4. **Reduce Paper Consumption**
   a) Reduce paper consumption by use of e-mail and electronic archiving.
   b) Use online marketing rather than paper based marketing.
   c) *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**
   a) Use notebook computers rather than desktop computers whenever possible;
   b) Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
   c) *Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.*

Q.No.39. What is BYOD (Bring Your Own Device)? Write down the advantages associated with BYOD?

1. **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.
2. ADVANTAGES OF BYOD:
   a) **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry;
   b) **Lower IT budgets:** Could involve financial savings to the organization since employees would be using the devices they already possess.
   c) **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
   d) **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.
   e) **Increased employee efficiency:** The efficiency of employees is more when the employee works on his/her own device.

Q.No.40. Write down the Threats (or) risks associated with BYOD?

Emerging BYOD Threats:

i) **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. the IT practice team is unaware about the number of devices being connected to the network. this lack of visibility can be hazardous.

ii) **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.

iii) **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.

iv) **Implementation Risks:** The absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse.

Q.No.41. What is Internet of Things (IoT) and Explain its applications?

1. **Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, 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.
2. ***For example:*** *Washing machines with Wi-Fi networking capabilities can connect themselves to home Wi-Fi. Once these machines are so connected they can be controlled through machine manufacturer mobile APP from anywhere in the world.*

APPLICATIONS:

1. **All home appliances to be connected and that shall create a virtual home.**
   a) Home owners can keep track of all activities in house through their hand held devices.
   b) Home security CCTV is also monitored through hand held devices.
2. **Office machines shall be connected through net.**
   a) Human resource managers shall be able to see how many people have had a cup of acoffee from vending machine and how many are present.
   b) How many printouts are being generated through office printer?
3. **Governments can keep track of resource utilizations:** Under SWACHH mission government can tag all dustbins with IOT sensors.

Q.No.42. What are the risks associated with Internet of Things (IoT)?

Risks:

A. **Risk to Product manufacturer**

The manufacturers will to ensure the huge data generated from IoT devices is kept secured. Hacking / Loosing this data may be distractors for entity as well as the individual to whom it relates to.

B. **Risk to user of these products**

   a) **Security:** As home devices / office equipment's are connected to network they shall be hit by all network related risks, including hacking, virus attacks, stealing confidential data etc.
   b) **Privacy, autonomy and control:** There is a huge risk that individuals may lose control over their personal life. Their personal life can be hacked and made public.
   c) **Intentional obsolescence of devices:** This may happen due to -
      - Companies which want to bring a new product may force users to dump the old products. This they can do by disabling the operating software of old product.

C. **Technology Risk:** Platform fragmentation and lack of technical standards are situations where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications tough.

D. **Environmental Risk due to Technology:** These studies are being done to see the impact on house air quality, due to use of heavy earth metals in devices.

Q.No.43.What is Artificial Intelligence? What are the applications of Artificial Intelligence?

1. "The ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgment to solve problems and adapt to new situations". The ability described above when exhibited by machines is called as Artificial intelligence (AI). It is intelligence exhibited by machines.
2. *Expert systems, Pattern recognition, Natural language processing, and many others are some of the various purposes on which AI may be applied.*

SOME COMMERCIAL APPLICATIONS:

a) Autonomous vehicles (such as drones and self-driving cars).
b) Medical diagnosis, in cancer research. Predicting the chances of an individual getting ill by a disease.
c) Proving mathematical theorems.
d) Playing games (such as Chess).
e) Search engines (such as Google search).
f) Online assistants (Apple online assistant such as SIRI).

Q.No.44. what are the risks and controls of **Artificial Intelligence?**

Risks of Artificial Intelligence:

1. AI relies heavily of data it gets. Incorrect data can lead to incorrect conclusions.
2. AI (robots) carries a security threats. Countries are discussing to have a KILL button in all AI capable machines. This is important otherwise someday machine may start controlling humans.
3. AI in long term may kill human skills of thinking the unthinkable.
4. **Controls of Artificial Intelligence:** The set of controls in AI will be extremely complex because of the nature of processing of information and must be dealt with based on the nature of the AI tool and the purpose, etc.

Q.No.45. What is Machine Learning? What are the applications and risks associated with Machine Learning?

Machine Learning is a type of Artificial Intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can change when exposed to new data.

Note: *Machine learning being an application of AI, the nature of risks and controls remain similar to those posed by AI systems.*

Q.No.46. What is Web 3.0? Write about Components of Web 3.0?

a) 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.
b) Web 3.0 technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats.
c) An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence. These systems can answer the questions posed by the users, because the application can think on its own and find the most probable answer, to the query submitted by the user.

Components of Web 3.0:

a) **Semantic Web:** This allows the data and information to be readily intercepted by machines, so that the machines are able to take contextual decisions on their own.
b) **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet.

Q.No.47. Difference between Traditional Commerce and E-Commerce?

Traditional Commerce Vs. E-Commerce

BASE FOR COMPARISON	TRADITIONAL COMMERCE	E-COMMERCE
Definition	goods / services which are manual and non-electronic.	transactions or exchange of information, electronically on the internet.
Transaction Processing	Manual	Electronically
Availability for commercial transactions	For limited time.	24 x 7 x 365
Nature of purchase	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
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.
Resource focus	Supply side	Demand side
Marketing	One way marketing	One-to-one marketing
Payment	Cash, cheque, credit card, etc.	Credit card, fund transfer, Cash in Delivery, Payment Wallets,
Delivery of goods	Instantly	Takes time.

Q.No.48. Explain the WORK FLOW DIAGRAM of E-COMMERCE?

Description of E-Commerce Work Flow Diagram

S. No.	Step	Activities
1	Customers login	Few e-commerce merchants may allow same transactions to be done through phone, but the basic information flow is e-mode.
2	Product / Service Selection	Customer selects products / services from available options.
3	Customer Places Order	Order placed for selected product / service by customer. This step leads to next important activity PAYMENT GATEWAY.
4	Payment Gateway	Here customer makes a selection of the payment method. In case payment methods is other than cash on delivery (COD).
5	Dispatch and Shipping Process	This process may be executed at two different ends. First if product / service inventory is managed by e-commerce vendor than dispatch shall be initiated at merchant warehouse. Second, many e-commerce merchants allow third party vendors to sale through merchant websites. For example: FLIPKART
6	Delivery Tracking	Another key element denoting success of e-commerce business is timely delivery. Merchants keep a track of where the product / service delivery to customers are immediately updated.
7	COD tracking	In case products are sold on COD payment mode, merchants need to have additional check on matching delivery with payments.

5. CORE BANKING SYSTEMS

Q.No.1. Discuss the major products & services provided and rendered by commercial banks?

1. **Acceptance of Deposits:** Deposits involve deposits by customers in various schemes for pre-defined periods.
2. **Granting of Advances:** Advances constitute a major source of lending by commercial banks.
3. **Remittances:**
   a) **Remittances** involve transfer of funds from one place to another.
   b) Electronic Funds Transfer is the mode of remittance which facilitates almost instantaneous transfer of funds between two centers electronically.
4. **Collections:**
   a) **Collections** involve collecting proceeds on behalf of the customer.
   b) Customers can lodge various instruments such as cheques, drafts, pay orders, travelers cheques, dividend and interest warrants.
5. **Clearing:**
   a) **Clearing** involves collecting instruments on behalf of customers of bank.
   b) The instruments mentioned above may be payable locally or at an outside center.
   c) Clearing house settles the inter-Bank transactions among the local participating member banks.
6. **Letters of Credit and Guarantees:** A Letter of Credit (LC) is an undertaking by a bank to the payee (the supplier of goods) to pay to him, on behalf of the applicant (the buyer) any amount up to the limit specified in the LC.
7. **Credit Cards:**
   a) The processing of applications for issuance of credit cards is usually entrusted to a separate division at the central office of a bank.
   b) Most credit cards issued by banks are linked to one of the international credit card networks like VISA, Master, Amex or RuPay.
8. **Debit Cards:**
   a) Debit cards are generally issued to account holder by the central office of the bank.
   b) When a debit card is used for a transaction, the amount is immediately deducted from the customer's account balance.

Q.No.2. Explain the Challenges of IT in banking services?

Challenges of IT in banking services:

a) **Frequent changes or obsolescence of technology**: Technology changing constantly and becomes outdated very quickly.

b) **Multiplicity and complexity of systems:** The Technology architecture used for services is quite complex. Hence, this requires the bank personnel to have requisite technology skills or outsource relevant skill set.

c) **Different types of controls for different types of technologies/ systems:** Deployment of Technology gives rise to new types of risks and need to be mitigated by relevant controls.

d) **Proper alignment with business objectives and legal/ regulatory requirements:** Banks must ensure that the CBS implemented, cater to all the business objectives and needs of the bank, in addition to the legal/regulatory requirements envisaged(predict).

e) **Dependence on vendors due to outsourcing of IT services**: In a CBS environment, the bank requires staff with specialized domain skills to manage IT. Hence, these services could be outsourced to vendors and gives rise to vendor risks .

f) **Vendor related concentration risk:** There may not one but multiple vendors providing different services. these situations result in higher risks due to heavy dependence on vendors.

g) **Segregation of Duties (SoD):** The segregation of duties as per organization structure should be clearly mapped in the CBS used by the bank. This is a high-risk area since any SoD conflicts can be a potential vulnerability for fraudulent activities.

RISKS AND CONTROLS

Q.No.3. Define the term Risk Analysis? Explain how these Risks are mitigated?

Risk Analysis is defined as the process of identifying security risks/threats and determining their magnitude and impact on an organization.

The gap is caused by:

a) Widespread use of technology and Interconnectivity of systems;

b) Elimination of distance, time and space as constraints;

c) Devolution of management and control;

d) Attractiveness of conducting unconventional digital attacks; and

e) External factors such as legislative, legal and regulatory requirements or IT developments.

Risks are mitigated by implementing risk assessment. This involves:

a) Identification of threats and vulnerabilities in the system;

b) The identification and analysis of security controls for information systems.

Q.No.4. Define the term RISK? Explain several examples of risks evolved in banking sectors?

DEFINITION:

a) As per ISO: **Risk** is uncertainty in achieving objectives. Risk can be positive or negative.

b) In simple terms, **Risk** can be defined as: "the potential harm caused if a threat exploits a particular vulnerability to cause damage to an asset".

Some examples are as follows:

1. **Risks to Data**
   - **a)** Unauthorized data changes affecting integrity of data;
   - **b)** Absence of logs and audit trail/ logs;
   - **c)** Unauthorized transactions;
   - **d)** Unauthorized entry/ corrections/ deletions;
   - **e)** Transactions without vouchers;
   - **f)** Changing data using other's password;
2. **Some sample risks relating to Banking are as follows:**
   - **a)** Loss of confidential data;
   - **b)** Unauthorized access to customer information;
   - **c)** Inaccuracy of data leading to incorrect decision-making;
   - **d)** Loss due to errors;
   - **e)** Loss of money/reputation/business due to Frauds;

Q.No.5. Discuss various IT risks which could have a significant impact on critical business/ banking sector? (or) Explain the Impact of IT Risks in banking segment?

There are new IT risks which could have a significant impact on critical business operations, such as:

a) External dangers from hackers, leading to denial of service (DoS) and virus attacks, extortion and leakage of corporate information.

b) Phishing attacks through Internet Banking. Phishing is the attempt to obtain sensitive information such as usernames, passwords, by disguising as a trustworthy entity in an electronic communication.

Other IT Risks:

i) Unauthorized or incorrect Interest rate changes;

ii) Incorrect Interest computation;

iii) Incorrect computation of charges;

iv) Unauthorized increased in credit limits;

v) Payments of stolen drafts;

vi) Payment of stopped cheques;

Q.No.6. Discuss the concept of IT Risk Management?

Based on the type of risk, project and its significance to the business, Board and Senior Management may choose to take up any of the following risk management strategy in isolation or combination as required:

a) **Avoid:** Eliminate the risk by not taking up or avoiding the specific business process which involves risk.

b) **Mitigate:** Implement controls (e.g. acquire and deploy security technology to protect the IT infrastructure).

c) **Transfer:** Share risk with partners or transfer to insurance coverage.

d) **Accept:** Formally acknowledge that the risk exists and monitor it.

Q.No.7. What are the indicators of higher IT risk?

Some of the risk indicators are:

a) IT security is not given required priority;

b) Attitude of "Computer will take care of everything - no checking is required";

c) Lack of transparency of IT operations and responsibility assigned;

d) Lack of Input control;

e) Lack of output verification;

f) Lack of evidence;

g) Lack of access control;

h) Lack of audit trails;

Q.No.8. Discuss the Internal Control System in Banks?

Internal Control System: The objective of internal control system is adherence to management policies, safeguarding assets through prevention and detection of fraud and error, ensuring accuracy and completeness of the accounting record and timely preparation of the reliable financial information.

Some examples of internal controls in bank branch are:

a) Work of one staff member is invariably supervised/ checked by another staff member, irrespective of the nature of work (Maker-Checker process).

b) A system of job rotation among staff exists.

c) Financial and administrative powers of each official/ position is fixed and communicated to all persons concerned.

d) Branch managers must send periodic confirmation to their controlling authority on compliance of the laid down systems and procedures.

e) All books are to be balanced periodically. Balancing is to be confirmed by an authorized official.

f) Details of lost security forms are immediately advised to controlling so that they can exercise caution.

Q.No.9. Discuss the IT Controls in Banks?

IT risks need to be mitigated by implementing the right type and level of controls in the automated environment. This is done by integrating controls into IT.

Sample list of IT related controls are:

a) The system maintains a record of all log-ins and log-outs.

b) 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.

c) The system checks whether the amount to be withdrawn is within the drawing power.

d) The system flashes a message if the balance in a lien account would fall below the lien amount after the processing of the transaction.

e) Access to the system is available only between stipulated hours and specified days only.

f) 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.*

Q.No.10. Discuss several General Controls applied in Banking Systems?

General Controls are apply to all systems components, processes, and data for a given enterprise or systems environment.

General controls include:

a) Information Security Policy: The security policy is approved by the senior management and encompasses all areas of operations of bank.

b) Administration, Access, and Authentication: IT should be administered with appropriate policies and procedures clearly defining the levels of access to information and authentication of users.

c) Separation of key IT functions: Secure deployment of IT requires the bank to have structure separate IT organisation with key demarcation/ isolation of duties for different personnel within IT department.

d) Management of Systems Acquisition and Implementation: The process of acquisition and implementation of CBS systems should be properly controlled.

e) Change Management: All key changes including hardware, software and business processes must be properly approved by the management, before implementation.

f) Backup, Recovery and Business Continuity: Banking operations should be ensured by having appropriate business continuity including backup, recovery and off-site data centre.

g) Proper Development and Implementation of Application Software: Application software in case developed and implemented must be properly controlled by using standard software development process.

ARCHITECTURE OF CBS

Q.No.11. Discuss the term CBS? Explain several examples of CBS?

1. **Core Banking Solution (CBS)** refers to a common IT solution wherein a central shared database supports the entire banking application.
2. Business processes in all the branches of a bank update a common database in a central server located at a Data Center, which gives a consolidated view of the bank's operations.
3. Branches function as delivery channels providing services to its customers.
4. Core Banking Solution brings significant benefits such as a customer is a customer of the bank and not only of the branch.

Some examples of CBS software are.

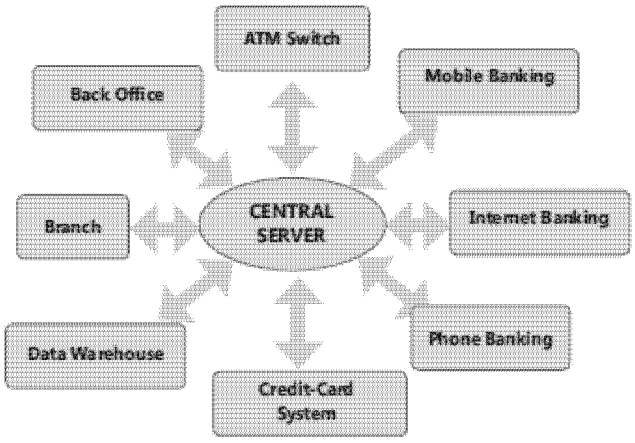
a) **Finacle:** Core banking software suite developed by Infosys that provides universal banking functionality covering all modules for banks covering all banking services.

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 enables communication through any touch point to provide full access to provide complete range of banking services with anytime, anywhere paradigm.



Q.No.12. Explain about CBS Architecture? Discuss the key aspects of CBS?

CBS Architecture

1. CBS for a bank functions not only as a heart (circulatory system) but also as a nervous system. All transactions flow through these core systems, which, at an absolute minimum, must remain running and responsive during business hours.
2. The platform where communication technology and information technology are merged to suit core needs of banking is known as core banking solutions.
3. Here, computer software is used to perform core operations of banking like recording of transactions, passbook maintenance, and interest calculations on loans & deposits, customer records, balance of payments and withdrawal.
4. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

Some key aspects in-built into architecture of a CBS are:

a) **Information flow**: Facilitates information flow within the bank and Improves the speed and accuracy of decision-making.

b) **Customer centric**: Through a holistic core banking architecture, enables banks to target customers with the right offers at the right time with the right channel to increase profitability.

c) **Regulatory compliance**: CBS has built-in and regularly updated regulatory platform which will ensure compliance.

d) **Resource optimization**: Optimizes utilization of information and resources of banks and lowers costs through improved asset reusability, faster turnaround times, faster processing.

Q.No.13. Discuss the Core features of CBS?

Core features of CBS are as follows:

a) On-line, real-time processing.

b) Transactions are posted immediately.

c) All databases updated simultaneously.

d) Centralized Operations (All transactions are stored in one common server).

e) Separate hierarchy for business and operations.

f) Business & Services are productized.

g) Remote interaction with customers.

h) Reliance on transaction balancing.

Q.No.14. Discuss the Major components/ features of the CBS solution?

A CBS is built with these inherent features such as:

a) Opening new accounts and customer on-boarding.

b) Managing deposits and withdrawals.

c) Transactions management from initiation to reporting.

d) Interest calculation and management.

e) Processing cash deposits and withdrawals.

f) Processing payments and cheques.

g) Processing and servicing loans.

Q.No.15. Discuss about Technology and work-flow of CBS?

1. **Core Banking Solution (CBS)** refers to a common IT solution wherein a central shared database supports the entire banking application.
2. CBS is a Technology environment based on client-server architecture, having a Remote Server (called Data Centre) and Client (called Service Outlets which are connected through channel servers) branches.
3. CBS has brought significant changes so far as workflow and housekeeping activities/ accounting processes at branches are concerned.
   a) User-actions and controls are elaborately menu-driven.
   b) User is prompted by software to initiate an action and to apply a control.
   c) Various periodical runs/ mass activities like Application of Interest & Service Charges,

d) Updating of parameters globally, balancing/ reconciliation of ledgers and TDS etc. are carried out centrally at the Data Centre.

Q.No.16. Discuss the stages of deployment and implementation of CBS?

The deployment and implementation of CBS should be controlled at various stages:

a) Planning: Planning for implementing the CBS should be done as per strategic and business objectives of bank.

b) Approval: The decision to implement CBS requires high investment and recurring costs and will impact how banking services. Hence, the decision must be approved by the board of directors.

c) Selection: Although there are multiple vendors of CBS, bank should select the right solution considering various parameters as defined by the bank to meet their specific requirements and business objectives.

d) Design and develop or procured: There should be appropriate controls covering the design or development or procurement of CBS for the bank.

e) Testing: Extensive testing must be done before the CBS is live.

f) Implementation: CBS must be implemented as per pre-defined and agreed plan with specific project milestones to ensure successful implementation.

g) Maintenance: CBS must be maintained as required. E.g. program bugs fixed, version changes implemented, etc.

h) Support: CBS must be supported to ensure that it is working effectively.

i) Updation: CBS modules must be updated based on requirements of business processes, technology updates and regulatory requirements.;

j) Audit: Audit of CBS must be done internally and externally as required to ensure that controls are working as envisaged.

Q.No.17. Discuss the key components of CBS? (or) Discuss various Technology Components of CBS?

1. The CBS facilities providing banking services for branches of a bank which are networked and connected to common data center.
2. This facilitates staff to process transactions of customers of any branch.
3. Hence, all the customers of all the branches are customers of the bank.

The key technology components of CBS are as follows:

a) Database Environment
b) Application Environment
c) Web Environment
d) Security solution
e) Connectivity to the Corporate Network and the Internet
f) Data Centre and Disaster Recovery Centre
g) Network Solution architecture to provide total connectivity
h) Enterprise Security architecture
i) Branch and Delivery channel environment
j) Online Transaction monitoring for fraud risk management

Q.No.18. What is a Server? Discuss various types of servers being used in CBS?

SERVER: The **Server** is a sophisticated computer that accepts service requests from different machines called clients. The requests are processed by the server and sent back to the clients. There are different types of servers used in deploying CBS.

Some of these are:

1. **Application Server:** The **Application Server** performs necessary operations and this updates the account of the customer. The results are updated in the database server at the centralized data center.
2. **Database Server:** The **Database Server** contains the entire data of the Bank. The data would consist of various accounts of the customers and master data. The data contained in the database must be high secure.
3. **Automated Teller Machines (ATM) Channel Server:** This server contains the details of ATM account holders. When the Central Database is busy with central end-of- day activities or for any other reason, the file containing the account balance of the customer is sent to the ATM switch. Such a file is called Positive Balance File (PBF).
4. **Internet Banking Channel Server (IBCS): IBCS (Internet Banking Channel Server)** software stores the user name and password of the entire internet banking customers. IBCS server also contains the details about the branch to which the customer belongs.
5. **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. Authentication process is the method by which the details provided by the customer are compared with the data already stored in the data server to make sure that the customer is genuine and has been provided with internet banking facilities.
6. **Web Server:** The **Web Server** is used to host all web services and internet related software. All the online requests and websites are hosted and serviced through the web server.
7. **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. The proxy provides the resource either by connecting to the specified server or by serving it from a cache.
8. **Anti-Virus Software Server:** The **Anti-Virus** Server is used to host anti-virus software which is deployed for ensuring all the software deployed are first scanned to ensure that appropriate virus/ malware scans are performed.

CORE BUSINESS PROCESS FLOW AND RELEVANT RISKS & CONTROLS

Q.No.19. Explain Business process flow of Current & Savings Accounts (CASA)? Write about the Risk & Controls around the CASA Process?

Process flow of Current & Savings Accounts (CASA):

a) Either the customer approaches the relationship manager to apply for a CASA facility or will apply the same through internet banking, the charges/ rates for the facility are provided by the relationship manager basis the request 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. KYC(Know Your Customer) is a process by which banks obtain information about the identity and address of the customers. KYC documents can be Passport, Driving License, etc.

c) The documents received from the customers are handed over to the Credit team / Risk team for sanctioning of the facilities/limits of the customers.

d) Credit team verifies the document's, assess the financial and credit worthiness of the borrowers and updates facilities in the customer account.

e) Current / Account savings account along with the facilities requested are provided to the customer for daily functioning.

f) Customers can avail facilities such as cheque deposits / withdrawal, Cash deposit / withdrawal, Real Time Gross Settlement (RTGS), National Electronics Funds Transfer System (NEFT), Electronic Clearing Service (ECS), Overdraft Fund Transfer services provided by the bank.

Risk & Controls around the CASA Process

S. No.	Risk	Key Controls
1.	Credit Line setup is unauthorized and not in line with the banks policy.	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk Policy and that the Client can be given the Credit Line.
2.	Credit Line setup in CBS is unauthorized and not in line with the banks policy.	Access rights to authorize the credit limit in case of account setup system should be restricted to authorized personnel.
3.	Customer Master defined in CBS is not in accordance with the Pre-Disbursement Certificate.	Access rights to authorize the customer master in CBS should be restricted to authorized personnel.
4.	Inaccurate interest / charge being calculated in CBS.	Interest on fund based facilities are automatically calculated in the CBS as per the defined rules.

Q.No.20. What are the steps involved in credit card transaction? Discuss several Risks and Controls around the Credit Card Process?

steps involved in credit card transaction:

Step 1: Authorization: This is the first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the card issuing bank, where it is authorized or denied, and the merchant is allowed to process the sale.

Step 2: Batching: This is the second step in processing a credit card. At the end of the day, the merchant reviews all the day's sales to ensure that all of them were authorized and signed by the cardholder. It then transmits all the sales at once, called a batch, to the acquirer to receive payment.

Step 3: Clearing: This is the third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network (such as VISA, MASTER CARD, AMEX, RUPAY), where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts its interchange fees, which are shared with the card network and transfers the remaining amount through the network, back to the acquirer.

Step 4: Funding: This is the fourth and final step in processing a credit card. After receiving payment from the issuer, minus interchange fees, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.

Risks and Controls around the Credit Card Process

S. No.	Risks	Key Controls
1.	Credit Line setup is unauthorized and not in line with the banks policy.	Access rights to authorize the credit limit in the credit card system should be restricted to authorized personnel.
2.	Credit Line setup can be breached.	Transaction cannot be made if the aggregate limit of out-standing amount exceeds the credit limit assigned to customer.
3.	Inaccurate interest / charge being 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 de- fined masters.
4.	Inaccurate reconciliations performed.	Daily reconciliation for the balances received from credit card network with the transactions updated in the credit card system on card network level.

Q.No.21. Discuss the process of Internet Banking? (or) Discuss the Processes involved in Online Banking?

Internet Banking: The customer applies to the bank for such a facility. The user is provided with a User ID and Password. As is the best practice the password is expected to be changed soon after the first log on.

a) For accessing the website, naturally a browser like Internet Explorer, Firefox or Chrome is used.

b) On access, user is directed to secure web server. The internet banking website is hosted on the web server. The web server is in the central data centre of the bank. Access to the web server is permitted only to authorized users.

c) To protect the web server from unauthorized use and abuse, the traffic is necessarily to go past a firewall.

d) An individual who accesses the website of bank through the browser will be able to access the web server and there will be a display of the bank's web page on the screen of the client's computer.

e) The web page will have a specified area wherein a mention of user ID and password will be made.

f) The password will not be displayed in plain text but will only be in an encrypted form.

g) The web server forwards the customer details to the internet banking applications server which in turn accesses the IDBS. The server has already the database of all the customers who have been provided with internet banking facility.

h) The information received from the web server is verified with the data of the customer held in the internet banking (IBAS).

i) Based on the authentication check, the Internet Banking Application Server (IBAS) sends an acknowledgement to the web server. The web server displays the message. Once the authentication process is completed correctly, the customer is provided internet banking facility, which would include:

- **i)** Password change
- **ii)** Balance inquiry
- **iii)** Fund transfer
- **iv)** Request for cheque book
- **v)** Stop payment
- **vi)** Copy of statement of account; and
- **vii)** ATM/ Credit Card related queries

j) The customer then chooses one of the services from the list. The service requested is directed by the web server to the IBAS for processing.

k) The Internet Banking Channel Server (IBCS) will retrieve 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 middleware is expected to convert the data to suit the requirements of IBCS.

l) Internet banking database server then forwards the customer data to the IBAS which processes the transaction. The IBCS then sends the data to the IBAS. The IBAS then sends the same to the web browser.

m) The web server generates a dynamic web page for the service requested

n) The customer would be able to get the service required e.g., viewing of the statement of account or a screen made available for him to request for a cheque book, the user may choose to log out.

Q.No.22. Discuss the process flow of e-Commerce Transaction?

a) Most of the e-Commerce transactions involve advance payment either through a credit or debit card issued by a bank.

b) Here, the user logs in on the e-commerce web site, places an order and selects option of payment - Cards, or Internet Banking.

c) If it is Internet Banking, the merchant site is directed to bank's Merchant-Internet banking server.

d) User must log in and authorize payment. This requires customer enter OTP (Online Transaction Password) received on mobile, to complete the transaction. After this, the customer is redirected to merchant site.

Q.No.23. What are the Risks associated with CBS?

Risks associated with CBS

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?

c) **Authentication procedures:** 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 interface and application software.

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.

Q.No.24. Discuss several IT related Risks and mitigating Controls w.r.t Data Centre and Network Operations?

1. Auditors are expected to be control experts.
2. Hence auditors need to understand how CBS works, the inherent risks, implemented controls and evaluate the residual risks and consequent exposures.
3. From a business perspective, the risks that can be classified as:
   a) **Efficiency:** Response is delayed resulting in dissatisfied stakeholder.
   b) **Effectiveness:** Process is ineffective and multiple runs consume time.
   c) **Reliability:** Users lose confidence in information system.
   d) **Confidentiality:** Due to loss of critical data.
   e) **Integrity:** Incomplete or inaccurate data due to errors in input or processing.
   f) **Availability:** Information system is not available when required.
   g) **Compliance:** The information system does not comply with legal, regulatory, contractual or internal compliance requirements.

Sample Listing of Risks and Controls w.r.t Data Centre and Network Operations

Risks	Key IT Controls
Invalid items may be recorded or valid items may be inaccurately or incompletely recorded.	Access to automated job scheduling tools, and executable programs are defined to restrict to appropriate individuals as per job requirement.
Timely and adequate technical support may not be available and issues may not be resolved.	Entity has written agreement(s) with outside contractors and/ or software vendors to provide for technical support, as needed.

User queries may not be timely and adequately resolved.	Help desk function exists to provide support on user queries regarding systems.
Timely execution and complete processing and availability of data may not be ensured.	Performance and capacity utilization of the computer systems are measured, reported, and reviewed by management

Q.No.25. What type of sub-processes should be applied in banks for Information Security, as per ISO 27001? (or) "RBI has suggested using ISO 27001:2013 to implement information security" Explain the sub-processes to be implemented to mitigate risks?

1. Information security is critical to mitigate the risks of Information technology.
2. Security refers to ensure Confidentiality, Integrity and Availability of information.
3. RBI has suggested use of ISO 27001:2013 implement information security.
4. Information security is comprised of the following sub-processes:
   a) **Information Security Policies, Procedures, and practices:** Refers to the processes relating to approval and implementation of information security.
   b) **User Security Administration:** Refers to security for various users of information systems.
   c) **Application Security:** Refers to how security is implemented at various aspects of application right from configuration, setting of parameters and security for transactions through various application controls.
   d) **Database Security:** Refers to various aspects of implementing security for the database software.
   e) **Operating System Security:** Refers to security for operating system software which is installed in the servers and systems which are connected to the servers.
   f) **Network Security:** Refers to how security is provided at various layers of network and connectivity to the servers.
   g) **Physical Security:** Refers to security implemented through physical access controls.

Sample Listing of Risks and Controls w.r.t Information Security

Risks	Key IT Controls
Significant information resources may be modified inappropriately, disclosed without authorization	Super user access or administrator passwords are changed on system installation and are available with administrator only.
Lack of management direction and commitment to protect information assets.	Security policies are established and management monitors compliance with policies.
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.
User accountability is not established.	All users are required to have a unique user id.

APPLICABLE REGULATORY AND COMPLIANCE REQUIREMENTS

Q.No.26. Discuss the key functions of RBI?

1. The **Reserve Bank of India (RBI)** was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934.
2. Some of the key functions of RBI are given here.

a) **Monetary Authority**: Formulates implements and monitors the monetary policy with the objective of maintaining price stability and ensuring adequate flow of credit to productive sectors.

b) **Regulator and supervisor of the financial system**: Prescribes broad parameters of banking operations within which the country's banking and financial system functions with the objective of maintaining public confidence in the system, protect depositors' interest and provide cost-effective banking services to the public.

c) **Issuer of currency**: Issues and exchanges or destroys currency and coins not fit for circulation with the objective to give the public adequate quantity of supplies of currency notes and coins and in good quality.

Q.No.27. What is Money Laundering? What are the key provisions of Prevention of Money Laundering Act (PMLA)?

- **Money Laundering: Money Laundering** is the process by which the proceeds of the crime and the true ownership of those proceeds are concealed or made opaque (not transparent) so that the proceeds appear to come from a legitimate source.
- Money laundering is commonly used by criminals to make "dirty" money appear "clean" or the profits of criminal activities are made to appear legitimate.

1. **Prevention of Money Laundering Act (PMLA)**

a) Under Section 12 of PMLA, every banking company, financial institution and intermediary is required to maintain a record of transactions as may be prescribed by rules and furnish information to the Director within such time as may be prescribed.

b) Under rule 6 of PMLR, such records are to be maintained for a period of ten years from the date of transaction.

c) The key aspects of PMLA are as follows:

i) Maintenance of record of all cash transactions above 10 lakhs

ii) All series of cash transactions of value less than10 lakhs integrally connected if they have taken place within a month (aggregate value above 10 lakhs)

iii) All cash transactions here forged or counterfeit notes have been used.

iv) All suspicious transactions made in cash or otherwise.

2. **Anti-Money laundering (AML) using Technology**

a) Negative publicity, damage to reputation and loss of goodwill, legal and regulatory sanctions and adverse effect on the bottom line are all possible consequences of a bank's failure to manage the risk of money laundering.

b) The challenge is even greater for banks using CBS as all transactions are integrated.

c) Banks are using special fraud and risk management software to prevent and detect fraud and integrate this as part of their internal process and daily processing and reporting.

3. **Financing of Terrorism**

a) Money to fund terrorist activities moves through the global financial system via wire transfers and in and out of personal and business accounts.

b) Although terrorist financing is a form of money laundering, the money frequently starts out clean i.e. as a 'charitable donation' before moving to terrorist accounts. It is highly time sensitive requiring quick response.

c) As per compliance requirements of PMLA, CBS software should include various types of reports which are to be generated periodically for filing with regulatory agencies.

Q.No.28. Briefly explain all the stages of Money Laundering and how banks are used in laundering money?

Three stages of Money Laundering

a) **Placement:** The first stage involves the **Placement** of proceeds derived from illegal activities - the movement of proceeds, frequently currency, from the scene of the crime to a place, or into a form, less suspicious and more convenient for the criminal.

b) **Layering:** Layering involves the separation of proceeds from illegal source using complex transactions designed to not discovered in the audit trail and hide the proceeds. The criminals frequently use shell corporations, offshore banks or countries with loose regulation and secrecy laws for this purpose.

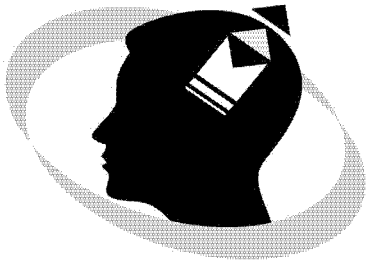
c) **Integration:** Integration involves conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations. Integration creates the illusion of a legitimate source for criminally derived funds and involves techniques as numerous and creative as those used by legitimate businesses

THE END

CA - INTER
COURSE MATERIAL

Quality Education
beyond your imagination...

PART B – DEFINITIONS



MASTER MINDS

CA • CMA • CS • MEC • CEC

GUNTUR | RAJAHMUNDRY | KURNOOL | VIZAG | NELLORE

HYDERABAD | VIJAYAWADA | TIRUPATHI

Cell: 98851 25025 / 26

Visit us @ www.mastermindsindia.com | Mail: mastermindsinfo@ymail.com

Facebook Page: Masterminds For CA | Youtube Channel: Masterminds For CA

1. AUTOMATED BUSINESS PROCESSES

'A' CATEGORY	
1. Business Process	**2. OPERATIONAL PROCESSES (OR PRIMARY PROCESSES)**
A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal.	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. Examples: Generating revenue - Order to Cash cycle, Procurement - Purchase to Pay cycle.
3. Supporting Processes (OR Secondary Processes)	**4. Business Process Automation (BPA)**
Supporting Processes back core processes and functions within an organization. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. Examples: Accounting, Human Resource (HR) Management .	**a)** It can be defined as removing the human element from existing business processes by automating the repetitive or standardized process components. **b)** BPA is the technology-enabled automation of company activities, including sales, management, operations, supply chain, human resources, information technology, etc.
5. Confidentiality	**6. Integrity**
To ensure that data is only available to persons who have right to see the same;	To ensure that no un-authorized amendments can be made in the data;
7. Availability	**8. Timeliness**
To ensure that data is available when asked for, and	To ensure that data is made available in at the right time.
9. Enterprise Risk Management (ERM)	**10. RISK**
It may be defined as a process, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.	As per International Organization for Standardization (ISO): **Risk** is uncertainty in achieving objectives. Risk can be positive or negative. **Risk** may be defined as the possibility that an event will occur and adversely affect the achievement of objectives.
11. Strategic Risk	**12. Financial Risk**
Risk that would prevent an organization from accomplishing its objectives (meeting its goals).	Risk that could result in a negative financial impact to the organization (waste or loss of assets).
13. Regulatory Risk(Compliance)	**14. Reputational Risk**
Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.	Risk that could expose the organization to negative publicity.
15. Operational Risk	**16. Control:**
Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations.	It 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.

17. Internal Controls	18. Segregation of Duties (SOD)
Internal Controls are a system consisting of specific policies and procedures designed to provide management with reasonable assurance that the goals and objectives it believes important to the entity will be met.	**Segregation of Duties (SOD)** is the process of assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. Segregation of duties is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud.
19. Application Controls	**20. Flowchart**
Application Controls are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing.	A Flowchart is a diagram prepared by the programmer of the sequence of steps involved in solving a problem. **a)** It is an essential tool for programming and illustrates the strategy and thread of logic followed in the program. **b)** A flowchart helps the programmer avoid fuzzy thinking and accidental omissions of intermediate steps.
21. Document Flowchart	**22. System Flowchart**
This flowchart traces the physical flow of documents through an organization – that is, the flow of documents from the departments, groups, or individuals who first created them to their final destinations.	This typically depicts the electronic flow of data and processing steps in an Information System. While Document Flowcharts focus on tangible documents, system flowchart concentrates on the computerized data flows of Information systems.
23. Program Flowchart	**24. Data Flow Diagrams (DFDs)**
It is most detailed and is concerned with the logical/arithmetic operations on data within the CPU and the flow of data between the CPU on the one hand and the input/output peripherals on the other.	DFD basically provides an overview of: **a)** What data a system processes; **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.
25. Procure to Pay (Purchase to Pay or P2P)	**26. Order to Cash (OTC or O2C)**
a) **Procure to Pay (Purchase to Pay or P2P)** is the process of obtaining and managing the raw materials needed for manufacturing a product or providing a service. **b)** It involves the transactional flow of data that is sent to a supplier as well as the data that surrounds the fulfillment of the actual order and payment for the product or service.	**Order to Cash (OTC or O2C) is a set of business processes that involve receiving and** fulfilling customer requests for goods or services. **a)** It is a set of business processes that involve receiving and fulfilling customer requests for goods or services. An order to cash cycle consists of multiple sub-processes including:
27. Human Resources life cycle	**28. Web Defacement:**
The **Human Resources** 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.	The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.

29. Cyber Terrorism	30. Phishing
Many terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.	Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity (e.g. Passwords, credit card information).
31. Cybercrimes	
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.	
'B' CATEGORY	
32. Management Processes	**33. Internal Control System**
Management processes measure, monitor and control activities related to business procedures and systems. 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. Examples: internal communications, governance, strategic planning, budgeting.	**Internal Control System**" means all the policies and procedures adopted by the management of an entity to assist in achieving management's objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.
34. Risk Assessment	**35. Communication**
a) Every entity faces a variety of risks from external and internal resources. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. b) Thus, risk assessment forms the basis for determining how risks will be managed.	**Communication** is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the enterprise, flowing up, down, and across the entity. External communication provides information to external parties in response to requirements and expectations.
36. Masters	**37. Inventory Cycle**
Masters refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory, Finance etc. The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed. (B) Ex: a) **Vendor Master:** Credit period, vendor bank account details, etc. b) **Customer Master:** Credit limit, Bill to address, Ship to address, etc.	The **Inventory Cycle** is a process of accurately tracking the on-hand inventory levels for an enterprise. An inventory system should maintain accurate record of all stock movements to calculate the correct balance of inventory.
'C' CATEGORY	
38. Risk Avoidance:	**39. Risk Reduction**
Risk Avoidance: exiting the activities giving rise to risk.	Taking action to reduce the likelihood or impact related to the risk.

40. Risk Alternative Actions	41. Risk Share or Insure
Deciding and considering other feasible steps to minimize risks.	Transferring or sharing a portion of the risk, to finance it.
42. Risk Accept	**43. Control Environment**
No action is taken, due to a cost/benefit decision.	**a)** The Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. **b)** The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance responsibilities; and the rigor around performance measures, incentives, and rewards to drive accountability for performance.
44. Control Activities	**45. General Controls**
Control Activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity and may be preventive or detective in nature.	**General Controls** include controls over information technology management, information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems - from mainframe to client/server to desktop computing environments.
46. Configuration	**47. Transactions**
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. Configuration will define how software will function and what menu options are displayed. Ex: Control on parameters: Creation of Customer Type, Vendor Type, year-end process	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. For example: **i)** sales transactions **ii)** purchase transactions **iii)** stock transfer transactions
48. Email Account Hacking	**49. Credit Card Fraud**
If victim's email account is hacked and obscene emails are sent to people in victim's address book.	Unsuspecting victims would use infected computers to make online transactions.
50. "Access"	**51. "Computer"**
"**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;	"**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;

52. "Computer Network"	53. "Data"
"Computer Network" means the interconnection of one or more Computers or Computer **systems** or Communication device through-The use of satellite, microwave, terrestrial line, wire, wireless or other communication media;	"**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;
54. "Information"	**55. Sensitive Personal Data Information (SPDI)**
"**Information**" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;	Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under section 43A of the Information Technology Act 2000 define a data protection framework for the processing of digital data by Body Corporate.
56. Personal Information	
"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." Example for personal information : **a)** Passwords **b)** Financial information **c)** Physical/physiological/mental health condition **d)** Sexual orientation **e)** Medical records and history; and **f)** Biometric information	

2. FINANCIAL AND ACCOUNTING SYSTEMS

'A' CATEGORY	
1. System	**2. Integrated System**
1. The word "system" can be explained as, "a set of detailed methods, procedures and routines created to carry out a specific activity, perform a duty, or solve a problem". **2.** It is an organized, purposeful structure that consists of interrelated and interdependent elements (components, entities, factors, members, parts etc.)	An **Integrated System** that has combined different functions together in order to work as one entity and maintaining data in a centralized manner. Central database is the main characteristics of an integrated ERP system.
3. Non-Integrated System	**4. MASTER DATA**
A **Non-Integrated System** is a system of maintaining data in a decentralized way. Each department shall maintain its own data separately and not in an integrated way. In case of non-integrated systems, separate database is maintained by each department separately.	**1.** Relatively permanent data not expected to change frequently. **2.** Master data is generally not typed by the user, it is selected from the available list. **3.** Master data entry is usually done less frequently say once a year or when there is a need to update. **Eg.:** Accounting Master Data, Inventory Master Data, Payroll Master Data, Statutory Master Data

5. NON-MASTER DATA

a) Non-permanent data and expected to change frequently. It is also called Transaction Data
b) Non-master data is typed by the user and not selected from available list as it is a non-permanent and it keeps on changing again and again.

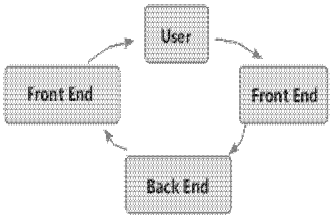
E.g.: Date recorded in each transaction is expected to change again and again and will not be constant in all the transactions.

6. FRONT END

Front End - It is part of the overall software which actually interacts with the user who is using the software.

7. Back End

It is a part of the overall software which does not directly interact with the user, but interact with Front End only.



8. Installed Applications

Installed Applications are programs installed on the hard disc of the user's computer.

9. Web Applications

Web Applications are not installed on the hard disc of the user's computer, it is installed on a web server and it is accessed using a browser and internet connection.

10. ERP System

1. ERP is an enterprise-wide information system designed to coordinate all the resources, information, and activities needed to complete business processes such as order fulfillment or billing.
2. An ERP system is based on a common database and a modular software design.
3. Some of the well-known ERPs in the market today include SAP, Oracle, MFG Pro, MS Axapta etc.

11. Ideal ERP System

1. An **Ideal ERP System** is that system which caters all types of needs of an organization and provides right data and right point of time to right users for their purpose.
2. Generally, an ideal ERP system is that system where a single database is utilized and contains all data for various software modules.

12. Customer Relationship Management

1. CRM is a term applied to processes implemented by a company to handle its contact with its customers.
2. CRM software is used to support these processes, storing information on current and prospective customers.
3. The rationale behind this approach is to improve services provided directly to customers and to use the information in the system for targeted marketing.

13. Role Based Access Control (RBAC)

a) It is a policy neutral access control mechanism defined around roles and privileges.
b) The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.
c) RBAC can be used to facilitate administration of security in large organizations with hundreds to thousands of users and thousands of permissions.

14. Rules-based Access Control (RAC)

a) RAC takes into account the data affected, the identity attempting to perform a task, and other triggers governed by business rules.
b) RAC uses specific rules that indicate what can and cannot happen between a subject/ user and an object. A manager, for example, has the ability to approve his/her employees' hours worked.
c) RAC can be used to facilitate administration of security in small to medium sized organizations with hundreds of users and limited permissions.

15. Human Resource Module	16. SUPPLY CHAIN MODULE
a) This module enhances the work process and data management within HR department of enterprises. b) 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. c) The task of managing the details and task flow of the most important resource i.e. human resource is managed using this module.	a) This module provides extensive functionality for logistics, manufacturing, planning, and analytics. b) Enterprises can optimize their supply chain for months in advance; streamline processes such as supply network, demand, and material requirement planning; create detailed scheduling; refine production integration, and maximize transportation scheduling.
17. Data mining,	**18. E-commerce**
Data mining, involves sorting through large data sets to identify trends, patterns and relationships; predictive analytics, which seeks to predict customer behavior, equipment failures and other future events;	**E-commerce** companies and marketing services providers do click stream analysis to identify **website visitors who are more likely to buy a product or service based on navigation and page**-viewing patterns.
19. Business Intelligence (BI)	**20. Extensible Business Reporting Language (XBRL)**
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.	**Extensible Business Reporting Language (XBRL)** - an international standards-based business reporting language developed by accountants for financial reporting; c) **XBRL** is a freely available and global standard for exchanging business information. d) **XBRL** lets reporting information move between organizations rapidly, accurately and digitally. e) **XBRL** is a standards-based way to communicate and exchange business information between business systems.
21. XBRL Tagging	
XBRL Tagging is the process by which any financial data is tagged with the most appropriate element in an accounting taxonomy (a dictionary of accounting terms) that best represents the data in addition to tags that facilitate identification/classification (such as enterprise, reporting period, reporting currency, unit of measurement etc.).	
'B' CATEGORY	
22. Process	**23. Business Process**
In the systems engineering arena, a **Process** is defined as a sequence of events that uses inputs to produce outputs. From a business perspective, a **Process** is a coordinated and standardized flow of activities performed by people or machines, which can traverse functional or departmental boundaries to achieve a business objective and creates value for internal or external customers.	a) A Business Process consists of a set of activities that are performed in coordination in an organizational and technical environment. b) These activities jointly realize a business goal.

24. Data Analytics	25. Basel III
a) **Data Analytics** is the process of examining data sets to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software. b) **Data Analytics** initiatives can help businesses increase revenues, improve operational efficiency, optimize marketing campaigns and customer service efforts, respond more quickly to emerging market trends and gain a competitive edge over rivals -- all with the ultimate goal of boosting business performance.	**Basel III** is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector. These measures aim to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source and to improve risk management and governance.
26. Book keeping life cycle	**27. FINANCIAL ACCOUNTING MODULE**
Accounting or Book keeping cycle covers the business processes involved in recording and processing accounting events of a company. It begins when a transaction or financial event occurs and ends with its inclusion in the financial statements.	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.
28. CONTROLLING MODULE	**29. SALES & DISTRIBUTION MODULE**
This module helps in analyzing the actual figures with the planned data and in planning business strategies. Two kinds of elements are managed in Controlling -**Cost Elements** and **Revenue Elements**. These elements are stored in the Financial Accounting module.	It is used by organizations to support sales and distribution activities of products and services, starting from enquiry to order and then ending with delivery.
30. Material Management (MM) Module	**31. QUALITY MANAGEMENT MODULE**
Material Management (MM) Module as the term suggests manages materials required, processed and produced in enterprises.	1. This quality management module helps an organization to accelerate their business by adopting a structured and functional way of managing quality in different processes. 2. Quality Management module collaborates in procurement and sales, production, planning, inspection, notification, control, audit management and so on.
32. Data Warehouse	
a) Data warehouse is a repository of an organization's electronically stored data. b) This is a module that can be accessed by an organizations customers, suppliers and employees. c) This classic definition of the data warehouse is to retrieve and analyze data, to extract, transform and load data, and to manage the data dictionary are also considered essential components	
'C' CATEGORY	
33. Report	**34. Text mining**
A **Report** simply means presentation of information in proper and meaningful way. The basic purpose of any Financial and Accounting system is to give right information at right point of time to right people for right decision making.	**Text mining** provides a means of analyzing documents, emails and other text-based content.

35. Regulatory Compliance	36. PLANT MAINTENANCE MODULE
Regulatory Compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations. Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business.	**a)** This is a functional module which handles the maintaining of equipment and enables efficient planning of production and generation schedules. **b)** It supports cost-efficient maintenance methods, such as risk-based maintenance or preventive maintenance, and provides comprehensive outage planning and powerful work order management.
37. Project Systems Module	
a) This is an integrated project management tool used for planning and managing projects. **b)** It has several tools that enable project management process such as cost and planning budget, scheduling, requisitioning of materials and services.	

3. INFORMATION SYSTEMS AND ITS COMPONENTS

'A' CATEGORY

1. Information	2. System
Data is a raw fact and can take the form of a numbers or statement such as a date or a measurement which has some meaning. The processed data is called information.	**a)** The system can be defined as "a group of mutually related, cooperating elements with a defined boundary; working on reaching a common goal by taking inputs and producing outputs in organized transformation process." **b)** A system contains several subsystems with sub goals, all contributing to meeting the overall system goal.
3. Information systems	**4. Central Processing Unit (CPU)**
Information System (IS) is a combination of people, hardware, software, communication devices, network and data resources that processes data and provide information for a specific purpose.	**a)** The Central Processing Unit (CPU or microprocessor) is the actual hardware that interprets and executes the program (software) instructions and coordinates how all the other hardware devices work together. **b)** The CPU is built on a small flake of silicon and can contain the equivalent of several million transistors. **c)** The processor or CPU is like the brain of the computer. **d)** The main function of CPU is to execute programs stored in memory.
5. Operating Systems (OS)	**6. Database Management Systems (DBMS)**
An **Operating System (OS)** is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs. Some Operating systems used nowadays are Windows 7, Windows 8, Linux, UNIX, etc.	DBMS is a software system that helps in organizing, controlling and using the data needed by the application program. It is basically just a computerized record keeping.

7. Database Model	8. Relational Database
It determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated.	**a)** It allows the definition of data and their structures, storage and retrieval operations and integrity constraints that can be organized in a table structure. **b)** A table is a collection of records and each record in a table contains the same fields, which define the nature of the data stored in the table. **c)** Keys are commonly used to join or combine data from two or more tables.
9. Object-Oriented Database	**10. Big data**
a) An object- oriented database (also referred to as object-oriented database management system or OODBMS) is a set of objects. **b)** It provides a mechanism to store complex data such as images, audio and video, etc. **c)** An object-oriented database management system is a relational database designed to manage all these independent programs, using the data produced to quickly respond to requests for information by a larger application. **d)** Object-oriented programming is based on a series of working objects. Each object is an independently functioning application or program, assigned with a specific task or role to perform.	**a)** A new buzzword that has been capturing the attention of businesses lately is big data. **b)** The term refers to such massively large data sets that conventional database tools do not have the processing power to analyze them. **c)** For example, WalMart must process over one million customer transactions every hour.
11. Data Mining	**12. Packet**
a) Data Mining is the process of analyzing data to find previously unknown trends, patterns, and associations to make decisions. **b)** Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse. **c)** EX: A baseball team may find that collegiate baseball players with specific statistics in hitting, pitching, and fielding make for more successful major league players.	The fundamental unit of data transmitted over the Internet. When a device intends to send a message to another device, it breaks the message down into smaller pieces, called packets. Each packet has the sender's address, the destination address, a sequence number.
13. Hub	**14. Bridge**
a) A simple network device that connects other devices to the network and sends packets to all the devices connected to it. **b)** A hub is basically a multiport repeater that connects multiple wires coming from different branches. ***c)*** *Hubs cannot filter data, so data packets are sent to all connected devices.*	**a)** Bridge is a communications processor that connects two Local Area Networks (LANs) working on the same protocol. **b)** A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.

15. Router	16. Network Topology
A device that receives and analyses packets and then routes them towards their destination. In some cases, a router will send a packet to another router; in other cases, it will send it directly to its destination.	**a)** The term 'Topology' defines the physical or logical arrangement of links in a network. It is the geometric representation of the relationship of all the links and linking devices (usually called Nodes) to each other. **b)** Common topologies are **Star Network, Bus Network, Ring Network and Mesh Network.**
17. Protocol	**18. IP Address**
Protocol: In computer networking, a protocol is the set of rules that allow two (or more) devices to exchange information back and forth across the network.	**a)** Every device that communicates on the Internet, whether it be a personal computer, a tablet, a smartphone, or anything else, is assigned a unique identifying number called an IP (Internet Protocol) address. **b)** Presently we are using IPv4 (version 4), IPv6 standards Ex: domain wikipedia.org has the IP address of 107.23.196.166.
19. Domain Name	**20. Wi-Fi**
a) A Domain Name is a human-friendly name for a device on the Internet. **b)** These names generally consist of a descriptive text followed by the top-level domain (TLD). For example, Wikipedia's domain name is wikipedia.org;	**a)** Wi-Fi stands for wireless fidelity. Wi-Fi is a technology that takes an Internet signal and converts it into radio waves. **b)** These radio waves can be picked up within a radius of approximately 65 feet by devices with a wireless adapter. **c)** Each new specification improved the speed and range of Wi- Fi, allowing for more uses. One of the primary places where Wi-Fi is being used is in the home. **d)** However, with increase in smart phone sales, Wi-Fi hotspot services are being provided at various public places to provide better customer service.
21. Voice over Internet Protocol (VoIP)	**22. Control**
a) A growing class of data being transferred over the Internet is Voice Data. **b)** A protocol called VoIP enables sounds to be converted to a digital format for transmission over the Internet and then recreated at the other end. **c)** By using many existing technologies and software, voice communication over the Internet is now available to anyone with a browser (think Skype, Google Hangouts, Whatsapp calls).	Controls are defined as policies, procedures, practices, and organization structure ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected. An information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.
23. Preventive Controls	**24. Detective Controls**
Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. These controls prevent errors, omissions, or security incidents from occurring. Any control can be implemented in both manual and computerized environment for preventive purpose.	**a)** **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.

Some of the examples of Preventive Controls are: **a)** Employment of qualified personnel **b)** Segregation of duties **c)** Access control **d)** Anti-virus software (sometimes this acts like a corrective control also), etc **e)** User instruction manuals. **f)** Firewalls, Passwords.	**b)** For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities.
25. Corrective Controls	**26. Logical Access Controls**
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.	These are the controls relating to logical access to information resources such as data and programs is restricted to authorized users to safeguard information against unauthorized use, disclosure or modification, damage or loss. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.
27. Data Diddling	**28. Cryptography**
This involves the change of data before or after they entered the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.	**a)** 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. **b)** 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).
29. Information Systems Auditing	**30. Snapshots**
It is defined as the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both.	**a)** Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. **b)** 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. **c)** These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.
31. System Control Audit Review File (SCARF)	**32. Audit Trails**
The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file called the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up.	Audit Trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained.

33. Segregation of Duties (SOD)	
It is also known as separation of duties, ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation or exposure of sensitive data.	

'B' CATEGORY

34. Registers	35. Random Access Memory (RAM)
These are high speed memory units within CPU for storing small amount of data (mostly 32 or 64 bits).	**a)** This is Read Write memory whose main purpose is to hold program and data while they are in use. Information can be read as well as modified. **b)** It is responsible for storing the instructions and data that the computer is using at that present moment. **c)** Volatile in nature means Information is lost as soon as power is turned off.
36. Read Only Memory (ROM)	**37. Cache Memory**
a) This is non-volatile in nature (contents remain even in absence of power). **b)** Usually, these are used to store small amount of information for quick reference by CPU. **c)** Information can be read not modified. **d)** Generally used by manufacturers to store data and programs like translators that is used repeatedly.	**a)** Cache is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations. **b)** These copies can be accesses by Processor/Registers more rapidly than main memory. **c)** Cache memory can be used in order to bridge the speed differences between Registers and Primary memory. **d)** The cache acts as temporary memory and boosts processing power. **e)** It is the property of locality of reference that improves effective memory access time in a computer.
38. Virtual Memory	**39. Software**
a) Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems in conjunction with the hardware. **b)** If a computer lacks the Random-Access Memory (RAM) needed to run a program or operation, OS uses virtual memory to compensate. **c)** Virtual memory combines computer's RAM with temporary space on the hard disk. **d)** When RAM runs low, virtual memory moves data from RAM to a space called a paging file. Moving data to and from the paging file frees up RAM to complete its work. **e)** Thus, Virtual memory is an allocation of hard disk space to help RAM.	**Software** is defined as a set of instructions that tell the hardware what to do. Software is created through the process of programming. Without software, the hardware would not be functional.
40. Application Software	**41. Data**
It is a collection of programs which address a real-life problem of its end users which may be business or scientific or any other problem. EX.MS-OFFICE, TALLY etc.	Data are the raw bits and pieces of information with no context. Data can be quantitative or qualitative. Quantitative data is numeric, Qualitative data is descriptive.

42. Database	43. Hierarchical Database Model
A database is an organized collection of related information.	**a)** In Hierarchical Database Model, records are logically organized into a hierarchy of relationships. **b)** A hierarchically structured database is arranged logically in an inverted tree pattern. **c)** All records in hierarchy are called Nodes. Each node is related to the others in a parent child relationship. **d)** Each parent record may have one or more child records, but no child record may have more than one parent record.
44. Network Model	**45. Computer Network**
a) A network database structure views all records in sets. Each set is composed of an owner record and one or more member records. **b)** However, unlike the hierarchical mode, the network model also permits a record to be a member of more than one set at one time. **c)** This feature allows the network model to implement the many-to-one and the many-to-many relationship types.	**a)** Computer network is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. **b)** Each component, namely the computer in a computer network is called a 'Node'.
46. Routing	**47. Bandwidth**
It refers to the process of deciding on how to communicate the data from source to destination in a network.	It refers to the amount of data which can be sent across a network in given time.
48. Resilience	**49. Contention**
It refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.	It refers to the situation that arises when there is a conflict for some common resource in a network. *For example, network contention could arise when two or more computer systems try to communicate at the same time.*
50. Repeater	**51. MAC Address**
a) A repeater regenerates the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. **b)** They do not amplify the signal, when the signal becomes weak, they copy the signal bit by bit and generate it at the original strength.	**MAC Address:** These are most often assigned by the manufacturer of a Network Interface Controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism.
52. Switch	**53. Domain Name System (DNS**
A network device that connects multiple devices together and filters packets based on their destination within the connected devices.	DNS which acts as the directory on the Internet. When a request to access a device with a domain name is given, a DNS server is queried. It returns the IP address of the device requested, allowing for proper routing.

54. Transmission Mode	55. Packet Switching
a) It is used to define the direction of signal flow between two linked devices. There are three types of transmission modes characterized as per the direction of the exchanges: **b)** **Simplex** (wherein the data flows in only one direction- unidirectional), **c)** **Half-Duplex** (where in the data flows in one direction or the other, but not both at the same time) and **d)** **Full Duplex** (in which the data flows in both directions simultaneously).	**a)** When a packet is sent from one device out over the Internet, it does not follow a straight path to its destination. **b)** Instead, it is passed from one router to another across the Internet until it is reaches its destination. **c)** In fact, sometimes two packets from the same message will take different routes. Sometimes, packets will arrive at their destination out of order. When this happens, the receiving device restores them to their proper order.
56. Environmental Controls	**57. Bomb**
These are the controls relating to IT environment such as power, air-conditioning, Uninterrupted Power Supply (UPS), smoke detection, fire extinguishers, dehumidifiers etc.	Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately.
58. Worm	**59. Salami Techniques**
A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are standalone programs, and they can be detected easily in comparison to Trojans and computer viruses.	This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted.
60. Spoofing	**61. Personal Identification Number (PIN)**
A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable.	PIN is similar to a password assigned to a user by an institution, It is a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
62. Job Title	
a) A 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. **b)** Job titles in IT have matured and are quite consistent across organizations. This consistency helps organizations in several ways.	

'C' CATEGORY

63. Input	64. Process
Data is collected from an organization or from external environments and converted into suitable format required for processing.	A process is a series of steps undertaken to achieve desired outcome or goal.

65. Output	66. Hardware
Then information is stored for future use or communicated to user after application of respective procedure on it.	**a)** It is the tangible portion of our computer systems, something we can touch and see. **b)** It consists of devices that perform the functions of input, processing, data storage and output activities of the computer.
67. Input Devices	**68. Processing Devices**
Input devices are devices through which we interact with the systems. Some examples of input devices includes Keyboard, Mouse, Scanners, Bar Code, MICR readers, Webcams, Microphone and Stylus/ Touch Screen.	The Central Processing Unit (CPU or microprocessor) is the actual hardware that interprets and executes the program (software) instructions and coordinates how all the other hardware devices work together.
69. Data Storage Devices	**70. Output Devices**
They refer to the memory where data and programs are stored.	Computers systems provide output to decision makers at all levels in an enterprise to solve business problems, the desired output may be in visual, audio or digital forms. Most common examples of output devices are Speakers, Headphones, Screen (Monitor), Printer, Plotter etc.
71. Secondary Memory	**72. Connection Oriented Networks**
The secondary memory devices are non-volatile (contents are permanent in nature), greater capacity (they are available in large size), greater economy (the cost of these is lesser compared to register and RAMs). Ex: USB Pen Drives, Floppy drive, Hard Drive, CD, DVD and Smart cards.	In this method connection is first established and then data is exchanged like it happens in case of telephone networks.
73. Connectionless Networks	**74. Christmas Card**
In this method no prior connection is made before data exchanges. Data which is being exchanged in fact has a complete contact information of recipient and at each intermediate destination it is decided how to proceed further.	It is a well-known example of Trojan and was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half finished work.
75. Rounding Down	**76. Trap Doors**
This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.	Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

4. E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

1. E-commerce	2. Payment Gateway
a) E-commerce is the process of doing business electronically. b) It refers to the use of Technology to enhance the processing of commercial transactions between a company, its customers and its business partners.	The payment mode through which customers shall make payments. Payment gateway represents the way e-commerce / m-commerce vendors collects their payments. Presently numerous methods of payments by buyers to sellers are being used, including Credit / Debit Card Payments, Online bank payments, Third Party Payment wallets, like SBI BUDDY or PAYTM, Cash on Delivery (COD).
3. Digital Library	**4. Two Tier architecture**
A **digital library** is a special library with a focused collection of digital objects that can include text, visual material, audio material, video material, stored as electronic media formats (as opposed to print, microform, or other media), along with means for organizing, storing, and retrieving the files and media contained in the library collection.	In a **Two-tier network**, client (user) sends request to Server and the Server responds to the request by fetching the data from it. The Two-tier architecture is divided into two tiers- **Presentation Tier and Database Tier.**
5. Presentation Tier (Client Application/Client Tier)	**6. Database Tier (Data Tier)**
This is the interface that allows user to interact with the e-commerce / m-commerce vendor. User can login to an e-commerce vendor through this tier. This application also connects to database tier and displays the various products / prices to customers.	The product data / price data and other related data are kept here. User has not access to data / information at this level but he/she can display all data / information stored here through application tier.
7. Application Tier	**8. M-commerce**
It is also called as Middle Tier, Logic Tier, Business Logic or Logic Tier; this tier is pulled from the presentation tier. It controls application functionality by performing detailed processing.	M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). M-commerce enables users to access the Internet without needing to find a place to plug in.
9. Digital Payment	**10. UPI Apps**
It is a way of payment which is made through digital modes. In digital payments, payer and payee both use digital modes to send and receive money. It is also called electronic payment. No hard cash is involved in the digital payments. All the transactions in digital payments are completed online. It is an instant and convenient way to make payments.	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. User can transfer funds between two accounts using UPI apps. User must register for mobile banking to use UPI apps. Currently, this service is only available for android phone users. There are too many good UPI apps available such as BHIM, SBI UPI app, HDFC UPI app.

11. Virtualization	12. Grid Computing
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.	It 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. In the ideal grid computing system, every resource is shared, turning a computer network into a powerful supercomputer.
13. Cloud Computing	**14. Infrastructure as a Service (IaaS)**
a) **"The Cloud"** refers to applications, services, and data storage on the Internet. **b)** Cloud computing is the use of these services by individuals and organizations. You probably already using cloud computing in some forms. **c)** The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.	It is 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.
15. Software as a Service (SaaS)	**16. Security as a Service (SECaaS)**
SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.	**a)** 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. **b)** 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.
17. Identity as a Service (IDaaS)	**18. Mobile Computing**
a) 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. **b)** Generally, IDaaS includes directory authentication services, risk and event monitoring, single sign-on services.	It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world.
19. Green Computing or Green IT	**20. BYOD (Bring Your Own Device)**
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.	**a)** It refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. **b)** It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. **c)** The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours.

21. Web 3.0	22. Internet Of Things (IOT)
a) 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. b) An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence.	a) The **Internet of Things (IOT)** is a system of interrelated computing devices, mechanical and digital machines, objects, 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. b) For example: Washing machines with Wi-Fi networking capabilities can connect themselves to home Wi-Fi. Once these machines are so connected they can be controlled through machine manufacturer mobile APP from anywhere in the world.
23. Artificial Intelligence	**24. Machine Learning**
"The ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgment to solve problems and adapt to new situations". The ability described above when exhibited by machines is called as Artificial intelligence (AI). It is intelligence exhibited by machines.	Machine Learning is a type of Artificial Intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can change when exposed to new data.
'B' CATEGORY	
25. Web portal	**26. Data Interchange**
This shall provide the interface through which an individual /organization shall perform e-commerce transactions. These web portals can be accessed through desktops / laptops / PDA / hand- held computing devices / mobiles and now through smart TVs also.	It is an electronic communication of data. For ensuring the correctness of data interchange between multiple players in e-commerce, business specific protocols are being used.
27. Three Tier Architecture	**28. Immediate Payment Service (IMPS)**
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.	It is an instant interbank electronic fund transfer service through mobile phones. It is also being extended through other channels such as ATM, Internet Banking, etc.
29. Mobile Wallets	**30. Aadhaar Enabled Payment Service (AEPS)**
It is defined as virtual wallets that stores payment card information on a mobile device. Mobile Wallets provide a convenient way for a user to make-in-store payments and can be used that merchants listed with the mobile wallet service providers. There are mobile wallets like PayTm, Freecharge, Buddy, MobiKwick etc.	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.
31. Unstructured Supplementary Service Data (USSD)	**32. E-Wallet**
USSD banking or *99# Banking is a mobile banking based digital payment mode. User does not need to have a smartphone or internet connection to use USSD banking. S/he can easily use it with any normal feature phone. USSD banking is as easy as checking of mobile balance. S/he can use this service for many financial and non-financial operations such as checking balance, sending money, changing Mobile Banking Personal Identification number (MPIN) etc.	E-wallet or mobile wallet is the digital version of physical wallet with more functionality. User can keep his / her money in an E-wallet and use it when needed. Use the E-wallets to recharge phone, pay at various places and send money to friends. If user's have a smartphone and a stable internet connection, they can use E-wallets to make payments.

33. Credit Cards	34. Debit Cards
A small plastic card issued by a bank, or issuer etc., allowing the holder to purchase goods or services on credit. In this mode of payment, the buyer's cash flow is not immediately impacted. User of the card makes payment to card issuer at end of billing cycle which is generally a monthly cycle. Credit Card issuer charge customers per transactions / 5% of transaction as transaction fees.	A small plastic card issued by a bank. Allowing the holder to purchase goods or services on credit. In this mode of payment, the buyer's cash flow is immediately affected that as soon as payment is authorized buyers account is debited.
35. Hardware Virtualization	**36. Network 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.	**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.
37. Storage Virtualization	**38. Private Cloud**
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.	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 managed by the single organization **(On- Premise Private Cloud)** or can be managed by third party **(Outsourced Private Cloud)**.
39. Public Cloud	**40. Hybrid Cloud**
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.	This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments.
41. Community Cloud	**42. Network as a Service (NaaS)**
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.	**a)** It 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. **b)** 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.
43. Storage as a Service (STaaS)	**44. Database as a Service (DBaaS)**
It Provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term.	**a)** It Provides users with seamless mechanisms to create, store, and access databases at a host site on demand. **b)** 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.

45. Platform as a Service (PaaS)	46. Testing as a Service (TaaS)
PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider.	It 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.
47. Communication as a Service (CaaS)	**48. Data as a Service (DaaS)**
a) 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. **b)** Examples are: Voice over IP (VoIP), Instant Messaging (IM).	It 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.
49. Semantic Web	**50. Web Services**
This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines are able to take contextual decisions on their own.	It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.

'C' CATEGORY

51. Traditional Commerce	52. E-commerce Vendors
Traditional commerce includes all those activities which encourage exchange, goods / services which are manual and non-electronic.	This is the organization / entity providing the user, goods/ services asked for. For example: www.flipkart.com.
53. Architecture	**54. Net Banking**
It is a term to define the style of design and method of construction, used generally for buildings and other physical structures. In e-commerce, it denotes the way network architectures are build.	In this mode, the customers log to his / her bank account and makes payments. All public sectors, large private sector banks allow net banking facilities to their customers.
55. Backend as a Service (BaaS)	**56. Desktop as a Service (DTaaS)**
It Provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.	It Provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. It is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades.
57. API as a Service (APIaaS)	**58. Email as a Service (EaaS)**
It Allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.	It 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.

5. CORE BANKING SYSTEMS

'A' CATEGORY

1. Application Controls

a) Application Controls are controls which are implemented in an application to prevent or detect and correct errors.
b) These controls are in-built in the application software to ensure accurate and reliable processing.
c) Application controls ensure that all transactions are authorized, complete and accurate. Application Controls pertain to the scope of individual business processes or application systems.

2. General Controls

General Controls, also known as Infrastructure Controls pervade across different layers of IT environment and information systems.
General Controls are pervasive controls and apply to all systems components, processes, and data for a given enterprise or systems environment.

3. Core Banking Solution (CBS)

a) **Core Banking Solution (CBS)** refers to a common IT solution wherein a central shared database supports the entire banking application.
b) CBS is centralized Banking Application software that has several components which have been designed to meet the demands of the banking industry.
c) Further, the CBS is modular in structure and is capable of being implemented in stages as per requirements of the bank.

4. Customer Identification File (CIF)

Customer Identification File (CIF) is a digital or virtual file where the customer identity details with a valid photo ID and address details are stored and given a unique number which is called CIF number. A customer may have many accounts of different nature, like current account, savings account, loans etc., but all these accounts will be mapped to one CIF only.

5. 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 provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes.

6. Web Server

The **Web Server** is used to host all web services and internet related software. All the online requests and websites are hosted and serviced through the web server. A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.

7. Money Laundering

a) **Money Laundering** is the process by which the proceeds of the crime and the true ownership of those proceeds are concealed or made opaque so that the proceeds appear to come from a legitimate source.
b) The objective in money laundering is to conceal the existence, illegal source, or illegal application of income to make it appear legitimate.
c) Money laundering is commonly used by criminals to make "dirty" money appear "clean" or the profits of criminal activities are made to appear legitimate.

8. Cyber Crimes

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 a target. cyber-crimes are 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."

'B' CATEGORY

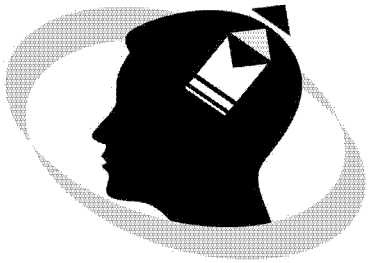
9. ECS Credit	10. ECS Debit
In the case of **ECS credit**, there is a single receiver of funds from a large number of customers. The beneficiary (i.e., the receiver of funds) obtains mandate from its customers to withdraw funds from their specified Bank accounts on a specific date.	In the case of **ECS debit**, there is a single account to be debited against which many accounts with a number of banks in the same clearing house area are credited. This system is useful for distribution of dividend interest, payment of salaries by large units, etc.
11. Automated Teller Machines (ATM) Channel Server	**12. Internet Banking Channel Server (IBCS)**
This server contains the details of ATM account holders. Soon after the facility of using the ATM is created by the Bank, the details of such customers are loaded on to the ATM server. When the Central Database is busy with central end-of- day activities or for any other reason, the file containing the account balance of the customer is sent to the ATM switch. Such a file is called Positive Balance File (PBF).	**IBCS (Internet Banking Channel Server)** software stores the user name and password of the entire internet banking customers. Please note that the ATM server does not hold the PIN numbers of the ATM account holders. IBCS server also contains the details about the branch to which the customer belongs. The Internet Banking customer would first have to log into the bank's website with the user name and password.
13. Internet Banking Application Server	**14. Basel III**
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. Authentication process is the method by which the details provided by the customer are compared with the data already stored in the data server to make sure that the customer is genuine and has been provided with internet banking facilities.	Basel III is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector. These measures aim to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source to improve risk management and governance. One of the dimensions of Basel III is determining capital adequacy based on risk assessment.
15. Server	
a) The **Server** is a sophisticated computer that accepts service requests from **b)** Different machines called clients. The requests are processed by the server and **c)** Sent back to the clients. This server is a powerful and robust system as performs the entire core banking operations. There are different types of servers used in deploying CBS they are **d)** **(i)** Application Server **(ii)** Database Server **(iii)** Automated Teller Machine channel Server, **(iv)** Internet Banking Channel Server,**(v)** Internet Banking Application Server **(vi)** Web Server, **(vii)** Proxy Server, **(viii)** Anti-Virus Software Server, etc.	

THE END

CA - INTER
COURSE MATERIAL

Quality Education
beyond your imagination...

PART C - DIFFERENCES



MASTER MINDS

CA • CMA • CS • MEC • CEC

GUNTUR | RAJAHMUNDRY | KURNOOL | VIZAG | NELLORE

HYDERABAD | VIJAYAWADA | TIRUPATHI

Cell: 98851 25025 / 26

Visit us @ www.mastermindsindia.com | Mail: mastermindsinfo@ymail.com

Facebook Page: Masterminds For CA | Youtube Channel: Masterminds For CA

1. AUTOMATED BUSINESS PROCESS

1. OPERATIONAL PROCESSES vs SUPPORTING PROCESSES

No.	OPERATIONAL PROCESSES (OR PRIMARY PROCESSES)	SUPPORTING PROCESSES (OR SECONDARY PROCESSES)
1.	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.	Supporting Processes back core processes and functions within an organization. One key differentiator between operational and support processes is that support processes do not provide value to customers directly.
2.	Examples: Generating revenue - Order to Cash cycle, Procurement - Purchase to Pay cycle.	Examples: Accounting, Human Resource (HR) Management .

2. SUPPORTING PROCESSES vs MANAGEMENT PROCESSES

No.	SUPPORTING PROCESSES (OR SECONDARY PROCESSES)	MANAGEMENT PROCESSES
1.	Supporting Processes back core processes and functions within an organization. One key differentiator between operational and support processes is that support processes do not provide value to customers directly.	Management processes measure, monitor and control activities related to business procedures and systems. 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.
2.	Examples: Accounting, Human Resource (HR) Management	Examples: internal communications, governance, strategic planning, budgeting.

3. Business Process vs Business Process Automation (BPA)

No.	Business Process	Business Process Automation (BPA)
1.	A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal.	It can be defined as removing the human element from existing business processes by automating the repetitive or standardized process components.
2.		BPA is the technology-enabled automation of company activities, including sales, management, operations, supply chain, human resources, information technology, etc.
3.		In other words, BPA is the tactic, that helps the business to automate processes to operate efficiently and effectively.

4. RISK vs Control

No.	RISK	Control
1.	As per International Organization for Standardization (ISO): **Risk** is uncertainty in achieving objectives. Risk can be positive or negative. **Risk** may be defined as the possibility that an event will occur and adversely affect the achievement of objectives.	It 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.

5. Internal Controls vs "Internal Control System"

No.	Internal Controls	"Internal Control System"
1.	**Internal Controls** are a system consisting of specific policies and procedures designed to provide management with reasonable assurance that the goals and objectives it believes important to the entity will be met.	"**Internal Control System**" means all the policies and procedures adopted by the management of an entity to assist in achieving management's objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.

6. Flowcharts vs Data Flow Diagram

No.	Flowcharts	Data Flow Diagram
1.	A Flowchart is a diagram prepared by the programmer of the sequence of steps involved in solving a problem.	What data a system processes;
2.	It is an essential tool for programming and illustrates the strategy and thread of logic followed in the program.	What transformations are performed;
3.	A flowchart helps the programmer avoid fuzzy thinking and accidental omissions of intermediate steps.	What data are stored;
4.		What results are produced and where they flow.

7. Document Flowchart vs System Flowchart

Types of Flowchart	Explanation
Document Flowchart	This flowchart traces the physical flow of documents through an organization – that is, the flow of documents from the departments, groups, or individuals who first created them to their final destinations.
System Flowchart	This typically depicts the electronic flow of data and processing steps in an Information System. While Document Flowcharts focus on tangible documents, system flowchart concentrates on the computerized data flows of Information systems.

8. DATA vs INFORMATION

No.	DATA	INFORMATION
1.	"**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;	"**Information**" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

2. FINANCIAL AND ACCOUNTING SYSTEMS

1. Integrated System vs Non-Integrated System

No.	Integrated System	Non-Integrated System
1.	An **Integrated System** that has combined different functions together in order to work as one entity and maintaining data in a centralized manner. Central database is the main characteristics of an integrated ERP system.	A **Non-Integrated System** is a system of maintaining data in a decentralized way. Each department shall maintain its own data separately and not in an integrated way. In case of non-integrated systems, separate database is maintained by each department separately.

2. MASTER DATA vs NON-MASTER DATA

No.	MASTER DATA	NON-MASTER DATA
1.	Relatively permanent data not expected to change frequently.	Non-permanent data and expected to change frequently. It is also called Transaction Data
2.	Master data is generally not typed by the user, it is selected from the available list.	Non-master data is typed by the user and not selected from available list as it is a non-permanent and it keeps on changing again and again.
3.	Master data entry is usually done less frequently say once a year or when there is a need to update.	Sometimes transactional data could also be selected from a drop down list of inputs available to the user.
4.	Master data is selected from the available list of masters (e.g. Ledgers) to maintain standardization.	E.g.: Date recorded in each transaction is expected to change again and again and will not be constant in all the transactions.
5.	Eg.: **Accounting Master Data, Inventory Master Data, Payroll Master Data, Statutory Master Data**	

3. FRONT END vs BACK END

No.	FRONT END	BACK END
1.	**Front End** - It is part of the overall software which actually interacts with the user who is using the software.	**Back End** - It is a part of the overall software which does not directly interact with the user, but interact with Front End only.

4. Installed Application vs Web Application

Particulars	Installed Application	Web Application
Installation & Maintenance	As software is installed on hard disc of the computer used by user, it needs to be installed on every computer one by one. Maintenance and updating of software may take lot time and efforts.	As software is installed on only one computer, i.e. on web server, it need not be installed on each computer. Maintenance and updating of software becomes extremely easy.
Accessibility	As software is installed on the hard disc of the user's computer, It cannot be used from any computer.	As software is not installed on the hard disc of user's computer and it is used through browser and internet, it can be used from any computer in the world 24 x 7.

Mobile Application	Using the software through mobile application is difficult in this case.	Using mobile application becomes very easy as data is available 24 x 7.
Data Storage	Data is physically stored in the premises of the user, i.e. on the hard disc of the user's server. Hence user will have full control over the data.	Data is not stored in the user's server. It is stored on a web server. Hence user will not have any control over the data.
Data Security	As the data is in physical control of the user, user shall have the full physical control over the data and he/she can ensure that it is not accessed without proper access.	Data security is a big challenge in case of web application as the data is not in control owner of data. It is maintained on a web server.
Performance	A well written installed application shall always be faster than web application, reason being data is picked from local server without internet.	As data is picked from web server using internet, speed of operation may be slower.
Flexibility	Installed applications shall have more flexibility and controls as compared to web application. It is very easy to write desktop applications that take advantage of the user's hardware.	Web applications do not even compare to the flexibility of desktop applications. If you want to write a web application that basically interacts with the user's hardware, you are doing it wrong!

5. ERP vs Ideal ERP

No.	ERP	Ideal ERP
1.	ERP is an enterprise-wide information system designed to coordinate all the resources, information, and activities needed to complete business processes such as order fulfillment or billing.	An **Ideal ERP System** is that system which caters all types of needs of an organization and provides right data and right point of time to right users for their purpose.
2.	An ERP system supports most of the business system that maintains in a single database the data needed for a variety of business functions such as Manufacturing, Supply Chain Management, Financials, Projects, Human Resources and Customer Relationship Management and Financial & Accounting Systems.	Generally, an ideal ERP system is that system where a single database is utilized and contains all data for various software modules.

6. RBAC vs RAC

No.	Role Based Access Control (RBAC)	Rules-based Access Control (RAC)
1.	RBAC is sometimes referred to as Role-Based Security.	RAC takes into account the data affected, the identity attempting to perform a task, and other triggers governed by business rules.
2.	It is a policy neutral access control mechanism defined around roles and privileges.	RAC uses specific rules that indicate what can and cannot happen between a subject/ user and an object. A manager, for example, has the ability to approve his/her employees' hours worked.
3.	The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.	RAC can be used to facilitate administration of security in small to medium sized organizations with hundreds of users and limited permissions.
4.	RBAC can be used to facilitate administration of security in large organizations with hundreds to thousands of users and thousands of permissions.	

7. Accounting & Tax Compliance Software vs Only Tax Compliance Software

S. 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 system, reconciliation with accounting data is needed, possibility of mismatch of data is always there.
5	Cost	More - if tax compliance feature is not available in accounting system, getting it customized may require some amount of cost which may be higher than buying separate software.	Less - as this is specific purpose software, there shall be less complications and the cost also shall be less.

3. INFORMATION SYSTEMS AND ITS COMPONENTS

1. Cache Memory Vs. Virtual Memory

1. **Cache Memory:**
   - **a)** There is a huge speed difference between Registers and Primary Memory.
   - **b)** Cache memory can be used in order to bridge the speed differences between Registers and Primary memory.
   - **c)** Cache is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations.
   - **d)** These copies can be accesses by Processor/Registers more rapidly than main memory.
   - **e)** The cache acts as temporary memory and boosts processing power.
   - **f)** It is the property of locality of reference that improves effective memory access time in a computer.
2. **Virtual Memory:**
   - **a)** Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems in conjunction with the hardware.
   - **b)** If a computer lacks the Random-Access Memory (RAM) needed to run a program or operation, OS uses virtual memory to compensate.
   - **c)** Virtual memory combines computer's RAM with temporary space on the hard disk.
   - **d)** When RAM runs low, virtual memory moves data from RAM to a space called a paging file.
   - **e)** Moving data to and from the paging file frees up RAM to complete its work.
   - **f)** Thus, Virtual memory is an allocation of hard disk space to help RAM.

2. Data warehouse Vs. Data Mining

1. **Data warehouse:**
   a) The concept of the data warehouse is extract data from one or more of the organization's databases and load it into the data warehouse (which is itself another database) for storage and analysis.
   b) It uses non-operational data.
   c) This means that the data warehouse is using a copy of data from the active databases that the company uses in its day- to-day operations, so the data warehouse must pull data from the existing databases on a regular, scheduled basis.
2. **Data Mining:**
   a) Data Mining is the process of analyzing data to find previously unknown trends, patterns, and associations to make decisions.
   b) Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse. EX: A baseball team may find that collegiate baseball players with specific statistics in hitting, pitching, and fielding make for more successful major league players.

3. Big data Vs. Data Mining

1. **Big data:**
   a) A new buzzword that has been capturing the attention of businesses lately is big data.
   b) The term refers to such massively large data sets that conventional database tools do not have the processing power to analyze them.
   c) For example, WalMart must process over one million customer transactions every hour.
2. **Data Mining:**
   a) Data Mining is the process of analyzing data to find previously unknown trends, patterns, and associations to make decisions.
   b) Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse.
   c) EX: A baseball team may find that collegiate baseball players with specific statistics in hitting, pitching, and fielding make for more successful major league players.

4. Preventive Vs. Detective Vs. Corrective Controls

1. **Preventive Controls:**
   a) Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring.
   b) These controls prevent errors, omissions, or security incidents from occurring.
   c) Any control can be implemented in both manual and computerized environment.
2. **Detective Controls:**
   a) These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence.
   b) In other words, Detective Controls detect errors or incidents that elude preventive controls.
   c) *For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities.*
3. **Corrective Controls:**
   a) It is desirable to correct errors, omissions, or incidents once they have been detected.
   b) 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.

5. Rounding Down Vs. Salami Techniques

1. **Rounding Down:** This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.
2. **Salami Techniques:**
   a) This involves slicing of small amounts of money from a computerized transaction or account.
   b) A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted.

6. Passwords Vs. Personal Identification Number (PIN)

1. **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.
2. **Personal Identification Number (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.

7. Transcription Errors Vs. Transposition Errors

1. **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. These fall into three classes:
   a) **Addition errors** occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
   b) **Truncation errors** occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
   c) **Substitution errors** are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.
2. **Transposition Errors:** It is a simple error of data entry that occurs when two digits that are either individual or part of larger sequence of numbers are reversed (Transpose) when posting a transaction. There are two types of transposition errors.
   a) **Single transposition** errors occur when two adjacent digits are recorded as 21345 instead of 12345.
   b) **Multiple transposition** errors occur when non-adjacent digits are transposed. For example, 12345 are recorded as 32154.

8. System Control Audit Review File (SCARF) Vs. Continuous and Intermittent Simulation (CIS).

1. **System Control Audit Review File (SCARF):**
   a) The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions.
   b) The information collected is written onto a special audit file the SCARF master files.
2. **Continuous and Intermittent Simulation (CIS):**
   a) This is a variation of the SCARF continuous audit technique.
   b) This technique can be used to trap exceptions whenever the application system uses a database management system.

9. Concurrent Audit Vs. General Audit.

1. **Concurrent Audit:**
   a) Auditors are members of the system development team.
   b) They assist the team in improving the quality of systems development for the specific system they are building and implementing through concurrent audit.
2. **General Audit:**
   a) Auditors evaluate systems development controls overall.
   b) They seek 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.

4. E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

1. Traditional Commerce Vs. E-Commerce

No.	Basis for Comparison	Traditional Commerce	E-Commerce
1.	**Definition**	Traditional Commerce includes all those activities which encourage exchange of goods / services which are manual or Non-electronic	E-commerce means carrying out commercial transactions or exchange of information, electronically on the internet
2.	**Transaction Processing**	Manual	Electronically
3.	**Availability for commercial Transactions**	For limited time, special stores which may run 24 hours, but in general available for limited time.	24×7365
4.	**Nature of Purchase**	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
5.	**Customer Interaction**	Face-to-Face	Screen-to-Face
6.	**Business Scope**	Limited to particular area	Worldwide reach
7.	**Information Exchange**	No uniform platform for exchange of information.	Provides a uniform platform for information exchange.
8.	**Resource Focus**	Supply side	Demand side
9.	**Marketing**	One way marketing	One-to-one marketing
10.	**Payment**	Cash, Cheque, Credit card etc.	Credit card, cash in delivery, fund transfer, payment wallets, UPCI application etc.
11.	**Delivery of goods**	Instantly	Takes time, but now e-commerce websites have created options of same day delivery, or delivery within 4 hours

2. Two tier architecture Vs. Three tier architecture

Two Tier Client Server: In a **Two-tier network,** client (user) sends request to server and the server responds to the request by fetching the data from it. The Two-tier architecture is divided into two tiers- **Presentation Tier and Database Tier.**

1. **Presentation Tier (Client Application/Client Tier):** This is the interface that allows user to interact with the e-commerce / m-commerce vendor. User can login to an e-commerce vendor through this tier. This application also connects to database tier and displays the various products / prices to customers.

2. **Database Tier (Data Tier):** The product data / price data and other related data are kept here. User has not access to data / information at this level but he/she can display all data / information stored here through application tier.

Three Tier Client Server: 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 are as follows:

1. **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.
2. **Application Tier:** Also, called the Middle Tier, Logic Tier, Business Logic or Logic Tier; this tier is pulled from the presentation tier. It controls application functionality by performing detailed processing.
3. **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.

3. Grid Computing Vs. Cloud Computing

Grid Computing:

a) **Grid Computing** is a computer network in which each computer's resources are shared with every other computer in the system.

b) It is a distributed architecture of large numbers of computers connected to solve a complex problem.

c) In the ideal grid computing system, every resource is shared, turning a computer network into a powerful supercomputer.

Cloud Computing:

a) **"The Cloud"** refers to applications, services, and data storage on the Internet.

b) Cloud computing is the use of these services by individuals and organizations. You probably already using cloud computing in some forms.

c) The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

4. Public Cloud Vs. Private Cloud

Private cloud:

a) This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits.

b) These are also called **Internal Clouds** or Corporate Clouds.

c) Private Clouds can either managed by the single organization **(On- Premise Private Cloud)** or can be managed by third party **(Outsourced Private Cloud)**.

Public cloud:

a) The public cloud is the cloud infrastructure that is provisioned for open use by the general public.

b) It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them.

c) Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis.

5. SAAS Vs. PAAS

Software as a Service (SaaS):

a) **SaaS** provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.

b) Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure.

c) SaaS changes the way the software is delivered to the customers.

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

e) For example, one can make his/her own word document in Google docs online.

Platform as a Service (PaaS):

a) **PaaS** provides the users the ability to develop and deploy an application on the development platform provided by the service provider.

b) In traditional application development, the application will be developed locally and will be hosted in the central location.

c) 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.

d) For example- Google AppEngine, Windows Azure Compute etc.

6. Artificial Intelligence Vs. Machine Learning.

Artificial intelligence:

a) "The ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgment to solve problems and adapt to new situations".

b) The ability described above when exhibited by machines is called as Artificial intelligence (AI). It is intelligence exhibited by machines.

Machine Learning:

a) Machine Learning is a type of Artificial Intelligence (AI) that provides computers with the ability to learn without being explicitly programmed.

b) Machine learning focuses on the development of computer programs that can change when exposed to new data.

7. M-Commerce Vs. E-Commerce.

M-Commerce (Mobile Commerce):

a) M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs).

b) M-commerce enables users to access the Internet without needing to find a place to plug in.

E-Commerce (Electronic Commerce):

a) **E**-commerce is the process of doing business electronically.

b) It refers to the use of Technology to enhance the processing of commercial transactions between a company, its customers and its business partners.

c) It involves the automation of a variety of Business-To-Business (B2B) and Business-To-Consumer (B2C) transactions through reliable and secure connections.

d) This could include the use of technology in the form of Computers, Desktops, Mobile Applications, etc.

5. CORE BANKING SYSTEMS

1. ECS Credit vs. ECS Debit.

1. **ECS Credit:**
   a) In the case of ECS credit, there is a single receiver of funds from a large number of customers.
   b) The beneficiary (i.e., the receiver of funds) obtains mandate from its customers to withdraw funds from their specified Bank accounts on a specific date.
2. **ECS Debit:**
   a) In the case of ECS debit, there is a single account to be debited against which many accounts with a number of banks in the same clearing house area are credited.
   b) This system is useful for distribution of dividend interest, payment of salaries by large units, etc.

2. Application Controls Vs. General Controls

1. **Application Controls:**
   a) Application Controls are controls which are implemented in an application to prevent or detect and correct errors.
   b) These controls are in-built in the application software to ensure accurate and reliable processing.
   c) Application controls ensure that all transactions are authorized, complete and accurate. Application Controls pertain to the scope of individual business processes or application systems.
2. **General Controls:**
   a) General Controls, also known as Infrastructure Controls pervade across different layers of IT environment and information systems.
   b) General Controls are pervasive controls and apply to all systems components, processes, and data for a given enterprise or systems environment.

3. Web Server Vs. Proxy Server

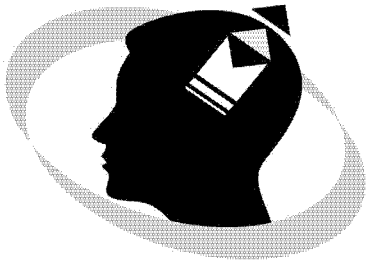
1. **Web Server:**
   a) The **Web Server** is used to host all web services and internet related software.
   b) All the online requests and websites are hosted and serviced through the web server.
   c) A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.
   d) Dedicated computers and appliances may be referred to as Web servers as well.
2. **Proxy Server:**
   a) A Proxy Server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services.
   b) A client connects to the proxy server, and then requests a connection, file, or other resource available on a different server.
   c) The proxy provides the resource either by connecting to the specified server or by serving it from a cache.
   d) In some cases, the proxy may alter the client's request or the server's response for various purposes.

THE END

CA - INTER
COURSE MATERIAL

Quality Education
beyond your imagination...

PART D – TRUE/FALSE QUESTIONS



MASTER MINDS

CA • CMA • CS • MEC • CEC

GUNTUR | RAJAHMUNDRY | KURNOOL | VIZAG | NELLORE

HYDERABAD | VIJAYAWADA | TIRUPATHI

Cell: 98851 25025 / 26

Visit us @ www.mastermindsindia.com | Mail: mastermindsinfo@ymail.com

Facebook Page: Masterminds For CA | Youtube Channel: Masterminds For CA

1. AUTOMATED BUSINESS PROCESSES

1.	Set of activities that will accomplish a specific organizational goal is called Business Process	T
2.	The processes deliver value to the customer by helping to produce a product (or) service are called Supporting Process	F
3.	Removing human element from existing business process is called Automation	T
4.	No un-authorized amendments can be made in data is called confidentiality	F
5.	The data is available when asked for is called Availability	T
6.	Automation reduces the time it takes to achieve a task	T
7.	Automation cannot reduces the number of tasks employees would otherwise need to do manually	F
8.	IT security and controls are sub-set of the overall enterprise risk management strategy	T
9.	Enterprise Risk management is not a process	F
10.	Non-profit organizations cannot provide value to its stake holders by using Enterprise Risk Management	F
11.	Rationalize capital is one of the benefit of Enterprise Risk Management (ERM)	T
12.	Seize opportunities is one of the component of ERM	F
13.	Reduction Risk Response is taking action to Reduce the likelihood (or) Impact related to the risk	T
14.	Transferring (or) sharing a portion of the risk is called Accept Risk Response	F
15.	Existing the activities giving rise to risk is called Avoidance risk response	T
16.	Deciding and considering other feasible steps to minimize risks is called Alternative Actions Risk response	T
17.	Risk is uncertainty in achieving objectives	T
18.	Infrastructure is not a risk of Business Process Automation	F
19.	Strategic Risk that would prevent an organization from accomplishing its objectives	T
20.	The Risk that could Expose the organization to negative publicity is called operational risk	F
21.	Risk that could result in a negative financial impact to the organization is called financial risk	T
22.	Control is a policy (or) Procedure designed to achieve business objectives	T
23.	Internal controls and internal control system two are same procedures	F
24.	The control environment sets the fame of organization	T
25.	Monitoring of controls is not a component of internal controls	F
26.	Segregation of Duties (SOD) is the process of assigning different people the responsibilities of authorizing transactions	T
27.	Communication is the continual process of providing and obtaining necessary information	T
28.	The cost of an internal control does not exceed the Expected benefits to be derived – It is the limitation of Internal control	T
29.	Accidental omissions cannot avoid by flowcharts	F

30.	Flow chart is an essential tool for programming	T
31.	Flow charts are not useful for Designing and documenting programs	F
32.	The diagrammatic representation of sequence of steps to solve a problem is called flow chart	T
33.	Document flow charts focus on the computerized Data flow	F
34.	System flowcharts focus on the tangible documents	F
35.	Program flowcharts represents the flow of data between the CPU and Input/Output peripherals	T
36.	Documentation is one of the advantage of flowcharts	T
37.	Detecting, locating and removing mistakes in programs is called program debugging	T
38.	Effective analysis is one of the limitations of flowcharts	F
39.	If modifications to a flowchart are required, it may require complete re-drawing	T
40.	In reproduction of flowcharts the symbols can be typed	F
41.	The full form of DFD is Data Flow Diagram	T
42.	Data store is not a component of Data Flow Diagram	F
43.	In DFD, An entity is the Source (or) Destination of Data	T
44.	In DFD, the symbol of process is Rectangle	F
45.	DFD represents the flow of Data in an organization	T
46.	The symbol of Data store in DFD is circle	F
47.	In DFD, data flow is represented by an arrow	T
48.	Procure to pay is the process of obtaining and managing the raw materials for manufacturing	T
49.	Order to cash is a process that involve receiving and fulfilling customer request for goods	T
50.	Inventory cycle is a process of accurately tracking the on-hand inventory levels of an enterprise	T
51.	Human resources cycle cannot covers all the stages of an employee's time with in a specific enterprise	F
52.	On boarding is the process of getting the successful applicant setup in the system as a new employee	T
53.	Career development is one of the stage in Human resource cycle	T
54.	Transition is the process by which the employee becomes a member of the company's work force	F
55.	Employees who have left the company continue to have system access is a risk of human resource cycle	T
56.	New employees are not added to the payroll is not a risk of human resource cycle	F
57.	Digital signatures have been given legal validity in the IT Act 2000	T
58.	Email account hacking is one of the cyber-crime under the IT Act 2000	T
59.	The home page of a website is replaced with a pornographic page is called cyber terrorism	F
60.	Back doors are the Malicious programs	T
61.	Fraudulently acquiring sensitive information through masquerading a site as a trusted entity is called phishing	T

62.	Unauthorized reproduction of computer software is under cyber crime	**T**
63.	Inter connecting of one (or) more computers is called communication	**F**
64.	Information contains message, text, images, sound, voice, codes	**T**
65.	Password is not a sensitive information	**F**
66.	Medical records and history is a sensitive information	**T**
67.	Consent is an agreement from the provider of sensitive personal data	**T**

2. FINANCIAL AND ACCOUNTING SYSTEMS

1.	A set of detailed methods created to solve a problem is called system	**T**
2.	Non-Integrated system maintains Data in a centralized manner	**F**
3.	Integrated system maintains Data in a decentralized manner	**F**
4.	Master data is a permanent data not expected to change frequently	**T**
5.	Master data typed by the user	**F**
6.	Non-Master data expected to change frequently	**T**
7.	Non-Master data is not typed by the user	**F**
8.	Front end is the software which actually interacts with the user	**T**
9.	Back end is the software which does not directly interact with the user	**T**
10.	Back end software is meant for handling request from users	**F**
11.	Front end software is meant for storing the data	**F**
12.	Front end software is meant for presenting information in proper format	**T**
13.	Front end software handles raw data	**F**
14.	Back end speaks in technical language not understood by layman	**T**
15.	Web applications are installed on the hard disc of the user's computer	**F**
16.	Installed applications are installed on the webserver	**F**
17.	Installed application needs to be installed on every computer one by one	**T**
18.	Web application installed on only one computer, i.e. on web server	**T**
19.	Installed application can be used from any computer in the world	**F**
20.	Data security is poor in web server	**T**
21.	Installed application is faster than web application	**T**
22.	Web applications have more flexibility than installed applications	**F**
23.	The full form of ERP is Enterprise Resource Planning	**T**
24.	An ERP is based on a common database	**T**
25.	MS Axapta is not an ERP software	**F**
26.	Oracle is an ERP software	**T**
27.	ERP process huge volumes of data within short time	**T**
28.	An Ideal ERP system provides right data and right point of time to right users for their purpose	**T**
29.	In ERP system, all Data can be stored in single data base, it may not be a Risk	**F**
30.	Role Based Access Control (RBAC) and Rules-based Access Control two are same methods	**F**

31.	Process is defined as a sequence of events	**T**
32.	Human Resource Module maintains total employee data base	**T**
33.	CRM is an acronym for customer relationship management	**T**
34.	CRM cannot improve customer revenues	**F**
35.	CRM helps to optimize marketing	**T**
36.	Report means presentation of information in proper and meaning full way	**T**
37.	An MIS report is not for evaluate business process	**F**
38.	Structured is one of the character of MIS reports	**T**
39.	The quantitative data involves non-numerical data	**F**
40.	The qualitative data involves numerical data	**F**
41.	Data mining is used to identify new trends	**T**
42.	Doing business electronically is called E-commerce	**T**
43.	XBRL is an Acronym for Extensible Best Reporting Language	**F**
44.	XBRL developed by Accountants for financial reporting	**T**
45.	XBRL not designed for reporting information move between organizations	**F**
46.	XBRL analyse the reports accurately	**T**
47.	Government doesn't use XBRL	**F**
48.	XBRL supports many languages	**T**
49.	Basel iii is developed by the Basel committee	**T**
50.	Basel iii is designed for supervision and risk management of the banking sector	**T**
51.	Compliance means conforming to a rule	**T**
52.	Regulatory compliance means comply with laws and regulations	**T**

3. INFORMATION SYSTEMS AND ITS COMPONENTS

1.	Data and information are same	**F**
2.	Generally a system contains several subsystems	**T**
3.	A feedback mechanism is required to monitor the performance of the system	**T**
4.	Information system refers to the interaction between processes and technology	**T**
5.	An information system does not require people	**F**
6.	A process is a series of steps undertaken to achieve desired outcome or goal	**T**
7.	A system has several interrelated and interdependent subsystems or components	**T**
8.	A subsystem can function in isolation	**F**
9.	The way a subsystem works with another subsystem is called integration	**F**
10.	Software is called tangible	**F**
11.	The main function of CPU is to execute programs stored in hard disk	**F**
12.	Registers are high speed memory units with in CPU for storing large amount of data	**F**
13.	There is a huge speed difference between registers and primary memory	**T**
14.	RAM is a volatile memory	**T**
15.	Secondary storage differs from primary storage in that it is not difficult accessible by the CPU	**T**

16.	Secondary storage devices are volatile	F
17.	Virtual memory is a separate device of storage	F
18.	Virtual memory moves data from RAM to a space called paging file	T
19.	Tactile output are helpful for blind people	T
20.	The hardware could function without software	F
21.	Operating system creates the interface between the user and the hardware	T
22.	API system stands for application program interface	T
23.	Task management feature of OS helps in allocating resources to make optimum utilisation of services	T
24.	Operating systems provide logical security	T
25.	Development of application software is inexpensive	F
26.	Benefit administrative is an important module of HRMS	T
27.	Data is now helping companies to create strategy for future	T
28.	By itself, data is useful	F
29.	Data which is put in to context aggregated analysed will be helpful for organisation decision making	T
30.	The goal of many information systems is to transform data in to information	T
31.	A database is an organised collection of related information	T
32.	Databases are always digital	F
33.	Microsoft access and open office base are examples of personal database management systems	T
34.	A database model determines the physical structure of a database	F
35.	A data base is a collection of data records	F
36.	A hierarchically structured database is arranged logically in an inverted tree pattern	T
37.	All records in hierarchy is called nodes	T
38.	The network model can represent redundancy in data more efficiently than in hierarchical model	T
39.	A network database structure views all records in nodes	F
40.	A record is one instance of a set of fields in a table	T
41.	A relation is a table with columns and rows	T
42.	In a relational database, all the tables are related by one or more fields	T
43.	Keys are used to access the files	F
44.	An object – oriented database provides a mechanism to store complex data	T
45.	An object – oriented database is basically a relational data base	T
46.	DBMS maximises data redundancy	F
47.	Data integrity is maintained by having accurate consistent and up – to – date data	T
48.	DBMS delays faster application development	F
49.	Even with safeguards in place it may possible for some unauthorised users to access the database	T
50.	Big Data term refers to such massively large data sets that conventional database	T

	tools do not have the processing power to analyse them	
51.	Data marts are very large databases	F
52.	The concept of data warehouse is ETL	T
53.	A data warehouse provides a decentralized view of all data in an enterprise	T
54.	Data mining is a collection of databases	T
55.	Data mining is the process of analysing data to find previously unknown trends , patterns and associations	T
56.	A network is a group of devices connected to each other	T
57.	Computer networks are helpful only to share the data but not resources	F
58.	Connection oriented networks operate like telephone networks	T
59.	Resilence refers to the ability of a network to recover from any kind of error	T
60.	Contention and polling methods are same	F
61.	Resource sharing implies sharing of peripherals	T
62.	The message in the network can be broken down in to smaller pieces called packets	T
63.	Repeater directly amplifies the signal	F
64.	Hubs can filter the data	F
65.	A hub is a multiport repeater	T
66.	A Bridge connects LAN's of different protocols	F
67.	MAC address and IP address are same	F
68.	MAC address is the manufacturer registered identification number	T
69.	A switch filters packets based on their destination	T
70.	A router routs packets to their destination	T
71.	Topology only refers to physical arrangement of links	F
72.	Signal flow can be in many ways between two linked devices	T
73.	A protocol is a set of rules that allow to or more devices to exchange information in a network	T
74.	An IP address is a unique identification number assigned to a device on internet	T
75.	Currently IPV6 is in use	T
76.	In Wikipedia.org the top level domain will be Wikipedia	F
77.	DNS is a directory on internet	T
78.	Wi – fi uses micro waves	F
79.	The Wi – fi specification starts with 802.11	T
80.	A skype or Whatsapp call is made using VOIP	T
81.	A well designed information system, systems should have proper controls in place	T
82.	Control process includes safeguarding assests to maintain data accurately	T
83.	Controls will help in achieving business objectives and avoid undesired events	T
84.	We can easily find competent and trust worthy IT personnel	F
85.	Segregation of duties will reduce likelihood of errors and wrongful acts in an IS	T
86.	As per the time of action controls are three in numbers	T

87.	Same control can be implemented in both manual and computerized environment for the same purpose	**T**
88.	Detective controls detect errors incidents that elude (or) escape preventive controls	**T**
89.	Corrective controls comes into picture before detective controls	**F**
90.	Environmental controls protect the physical security of an IS	**T**
91.	Physical access controls and environmental controls are same	**F**
92.	Physical access controls relates to physical security of the intangible IS resources and also intangibles resources stored on tangible media	**T**
93.	Operating system controls comes under logical Access controls	**T**
94.	Logical Access controls provide confidentially and authenticity to the data in IS	**T**
95.	An enormous technical knowledge is required for performing data diddling	**F**
96.	Logical bombs infect other programs	**F**
97.	A worm copies itself to another machine on network	**T**
98.	SALAMI technique and rounding down technique are same	**F**
99.	Access priviliges should always be minimal w.r.t the job functions	**T**
100.	Segregation of networks enforces network access control	**T**
101.	A fire wall is a system that enforces access control between two networks	**T**
102.	Converting cipher text into cleartext is called encryption	**F**
103.	Using a call back device we maintain continuous connection	**F**
104.	A log in procedure is a first line of defense against un authorised access	**T**
105.	An access taken is used to approve all actions attempted by the user during the session	**T**
106.	Access control list uses access taken	**T**
107.	Event logging is tough and unviable method to maintain logs	**F**
108.	The log files are never reviewed	**F**
109.	Clock synchronization is mandatory for event logging	**T**
110.	Theft of data carried on the disk drives of portable computers is high risk factors	**T**
111.	Managerial controls provide a stable infrastructure of IS	**T**
112.	Top management is not responsible for preparing a master plan for information systems functions	**F**
113.	Operational plan covers three to five years of operations	**F**
114.	The steering committee should assume the overall responsibility for the activities of the IS	**T**
115.	All systems must be properly and formally authorized to ensure economic justification and feasibility	**T**
116.	All programs includes must be thoroughly tested before they are implemented	**T**
117.	Concurrency controls are important to maintain the integrity of data	**T**
118.	There should be adequate insurance to replace IS assets and to cover the extra cost associated with restoring normal operations	**T**
119.	There is no relation between IT continuity plan Business Continuity plan	**F**
120.	Data may be lost or corrupted through component failure	**T**

121.	File library is just collection of files	**F**
122.	Any function or activity that works to ensure the processing accuracy of the application control	**T**
123.	PIN is not similar to a password	**F**
124.	Biometric devices also comes under Boundary controls	**T**
125.	Human intervention does not cause any errors or frauds in IS	**F**
126.	There is no relation between input controls and source document control	**F**
127.	Hash totals and sub totals are one and the same	**F**
128.	Input validation controls are intended to detect errors in the transaction data before the data are processed	**T**
129.	Limit check is applied only to output data	**F**
130.	Picture check is related to graphics	**F**
131.	A check digit is used to check the integrity of the code for further processing	**T**
132.	Transmission errors are controlled using parity check	**T**
133.	Multiplexers are used effectively use the communication line	**T**
134.	Flow controls are required to neutralize the speed differences between two nodes	**T**
135.	In contention method there is competition between the nodes to gain access to the channel	**T**
136.	Virtual memory controls are helpful to control real memory	**T**
137.	Master files and transactions files need not be synchronizes	**F**
138.	Output controls are only required in batch environment	**F**
139.	Recovery controls involve roll – forward and roll – back methods	**F**
140.	Once generated output can be destroyed as and when required	**F**
141.	Data integrity is a fundamental attribute of IS auditing	**T**
142.	System effectiveness and system efficiency are same	**F**
143.	Real time recording needs real time auditing	**T**
144.	Snapshot is helpful for tracing a transaction in a computerized environment	**T**
145.	Integrated test facility (ITF) method works with the real entity instead of dummy entity	**F**
146.	SCARF involves embedding of audit software module with the host application system	**T**
147.	Continuous and intermittent simulation (CIS) and SCARF are same	**F**
148.	Audit hooks are used to flag suspicious transactions	**T**
149.	Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained	**T**
150.	Audit trails are logs that can be designed to record activity at all three levels in an IS	**T**
151.	Personal accountability can be ensured using audit trails	**T**
152.	Audit of environment controls is not a mandatory component of IS audit plan	**F**
153.	Dormant accounts poses a risk to the IS environment	**T**
154.	Segregation of duties is different from separation of duties	**F**

155.	Preventive and detective controls should be put in place to manage segregation of duties matters	T

4. E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

1.	www.flipkart.com is an E-commerce vendor	T
2.	Many E-commerce companies are investing huge amounts of money in automating the whole ware houses	T
3.	Fast delivery is not an unique selling proposition (USP) for E-commerce vendors	F
4.	Loyalty programs establish a long term relationship with customer	T
5.	E-commerce companies do not open outlets	F
6.	Cash on delivery is most preferred method	T
7.	E-commerce vendors uses SSL (Secure Socket Layer) for enforcing security	T
8.	Small and mid-sized E-commerce organisations don't use shared infrastructure	F
9.	A mobile app can run on laptops	F
10.	Android is an open source operating system	T
11.	IOS is an open source operating system	F
12.	A digital library is a special library with focussed collections of digital objects	T
13.	An electronic library is a type of information retrieval system	T
14.	Data interchange is a manual communication of data	F
15.	Internet (or) Network is the key to success of E-commerce transactions	T
16.	Web portal provides an interface to perform E-commerce transactions	T
17.	Payment gateway represents the way E-commerce/M-commerce vendors collect their payments	T
18.	Application tier is a part of two tier architecture	F
19.	Presentation tier and client tier are different	F
20.	Two-tier architecture is simple to install	T
21.	Application tier, middle tier, logic tier represents same tier	T
22.	Dynamic load balancing is possible through three-tier architecture	T
23.	E-commerce and M-commerce are same	F
24.	M-commerce can be done using laptops	F
25.	Risk is possibility of loss	T
26.	Problem of anonymity occurs in E-commerce	T
27.	Lack of audit trails is not a big issue in E-commerce	F
28.	System effectiveness and system efficiency are same	F
29.	IT Act, 2000 Law Governs All Internet Activities In India	T
30.	UPI and IMPS comes under digital payment methods	T
31.	UPI is a system that powers multiple bank accounts and several banking services in a single mobile app	T
32.	BHIM is not an UPI app	F
33.	Mobile wallet is a virtual wallet	T
34.	Unstructured Supplementary Service Data (USSD) requires smart phone and internet	F
35.	The core concept of virtualization lies in partioning the single physical layer into multiple logical layers	T
36.	Hardware virtualization and platform virtualization are different	F

37.	Grid computing is a special kind of distributed computing	T
38.	Making use of underutilised services is the biggest use of Grid computing	T
39.	"The cloud" refers to applications, services and data storage on internet	T
40.	Google drive is an example of cloud computing service	T
41.	The internet is commonly visualized as cloud	T
42.	Security is a major concern in cloud computing	T
43.	Private cloud and internal cloud are same	T
44.	Service level agreements (SLA's) play very important role in any cloud service	T
45.	Public cloud is highly scalable	T
46.	There will be weak SLA's in public cloud	F
47.	Community cloud and hybrid cloud are same	F
48.	Infrastructure as a service (IAAS) is a hardware level service	T
49.	Elasticity and dynamic scaling services are possible in IAAS	T
50.	Windows Azrue is an example of platform as a services (PAAS)	T
51.	Mobile internet access is generally faster than direct cable connections	F
52.	Green computing involves using computers in an Environmental friendly way	T
53.	The basic aim of Green IT is to increase customer's energy savings	T
54.	The BYOD policy will render work spaces flexible	T
55.	Happy employees and lower IT budgets are possible through BYOD	T
56.	Early adoption of new technologies becomes tough with BYOD	F
57.	Web 3.0 also known as semantic Web	T
58.	Web services supports computer to computer interaction over internet	T
59.	Washing machines with Wi-Fi networking capabilities comes under IOT	T
60.	Hacking becomes a big threat to IOT	T
61.	Online assistant SIRI uses artificial intelligence	T
62.	AI does not rely on data it gets	F
63.	Data mining and machine learning are dissimilar	F
64.	Google car uses machine learning	T
65.	AI and machine learning are different	F

5. CORE BANKING SYSTEMS

1.	MICR technology allows machines to read and process cheques	T
2.	ECS is widely used in banks for clearing	T
3.	Banks do not provide any special services to HNI (High Net worth Individuals)	F
4.	IT risks are very threatful to banks	T
5.	IT risks in banks are only related to operations	F
6.	In internet banking we will have phishing attacks	T
7.	General controls are micro in nature	F
8.	Business continuity planning includes backup, recovery and off-site data centre planning	T
9.	Core Banking Solutions (CBS) supports entire Banking operations	T
10.	CBS is modular in structure	T
11.	CBS is a combination of application software and network devices	T
12.	Datacentre and Disaster Recovery centre are critical to CBS	T

13.	A CBS is an ERD for Bank	**T**
14.	Internal audit of CBS is not required	**F**
15.	The core of the CBS is the bank	**F**
16.	CIF is a digital file of customer data	**T**
17.	Database server is only accessed by application server	**F**
18.	A Proxy server allows clients to make indirect network connections	**T**
19.	To protect the webserver from unauthorised use and abuse a firewall is used	**T**
20.	In the context of CBS software, configuration refers to the way a software system is setup for use	**T**
21.	Data from CBS database is transferred to a data warehouse	**T**
22.	Money laundering is generally used to make "Clean" money appear "Dirty"	**F**
23.	Transaction logging is an application Control	**F**
24.	Completeness check is a general control	**T**
25.	On-line real time processing is a core feature of CBS	**T**
26.	Violation of privacy is a computer related offence as per IT Act, 2000	**T**
27.	The primary objective of SPDI is securing personal data of customers	**T**

THE END