1. **Explain the factors influencing an organization towards control and audit of computers.**

a) Organisational Costs of Data Loss:

- Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in the environment.

b) Cost of Incorrect Decision Making:

- Management and operational controls taken by the managers involves detection, investigation and correction of the processes.
- These high level decisions require accurate data to make quality decision rules.

c) Costs of Computer Abuse:

- Unauthorised access to – computer systems
  - malwares
  - computer facilities
  - sensitive data

  can lead to destruction assets.

d) High Costs of Computer Error:

- In a computerised enterprise environment, a data error during entry or process would cause a great damage.

e) 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.

f) Maintenance of Privacy:

- Data collected in a business process through computers may contain private information.
- Which may creates a fear about privacy.

g) Controlled Evolution of Computers:

- Use of technology and reliability of complex computer systems cannot be guaranteed.
- The consequences of using unreliable system can be destructive.

2. Explain the impact of the Information System Audit function on organization.

- The IS Audit process is to evaluate the adequacy of internal controls about both * specific computer program and
  * the data processing environment.
- The IS Audit of an IS environment may include one or both:
  * Assessment of internal controls within the IS environment.
  * Assessment of the efficiency and effectiveness of the IS environment.
- Information System Audit is the process of attesting objectives that focuses on - Asset safeguarding
  - Data integrity
  - Effectiveness
  - Efficiency.
- This enables organizations to better achieve 4 objectives that are:

a) Asset Safeguarding Objectives:

- The information system assets must be protected by a system of
  internal controls from unauthorised access.

b) Data Integrity Objectives:

- It is fundamental attribute of IS Auditing.
- The importance to maintain integrity of data of an organisation requires all time.

c) System Effectiveness Objectives:

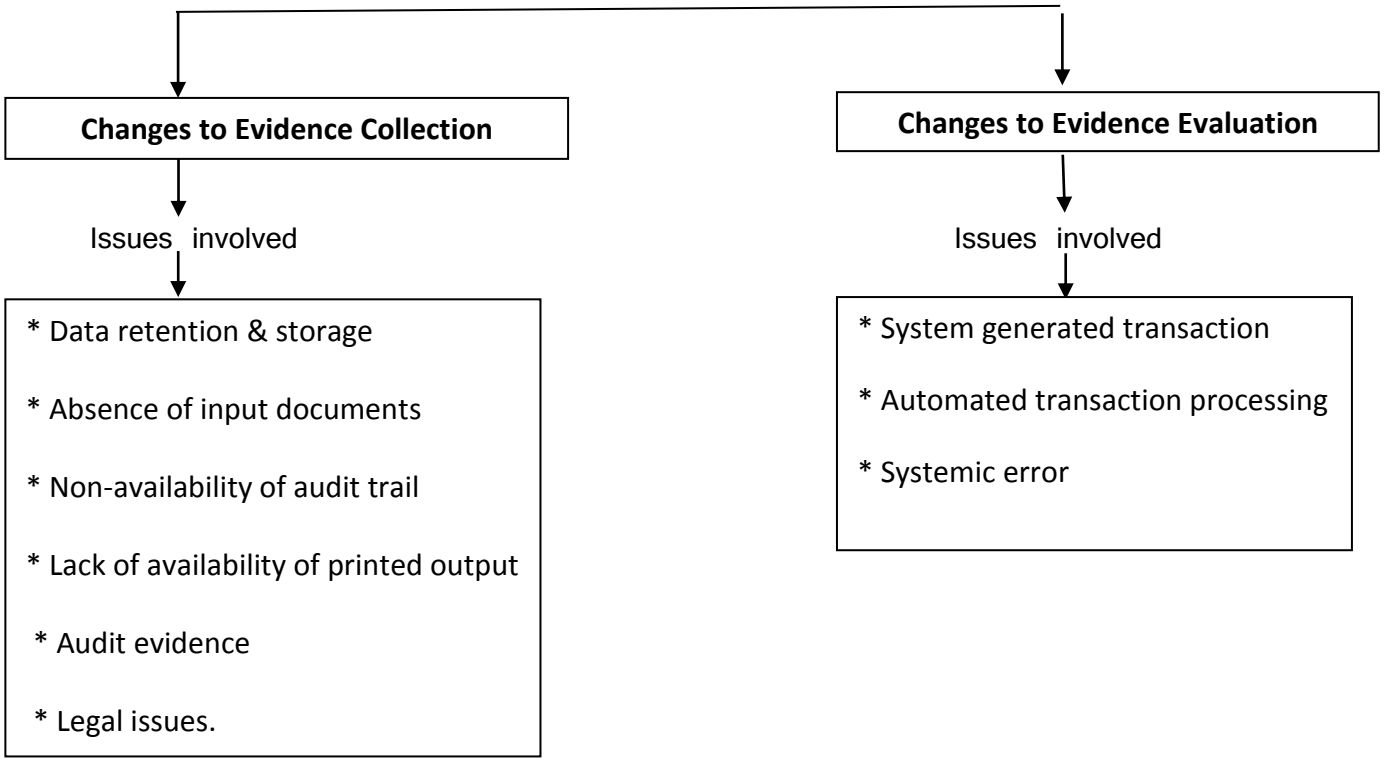
- Effectiveness of a system is evaluated by auditing the characteristics and objectives of the system.

d) System Efficiency Objectives:

- To optimise the use of various information system resources along
  with the impact on its computing environment.

3. **Write a note on effect of computers on audit.**

- – To cope up with the new technology usage in an enterprise, the auditor should be competent to provide independent evaluation as to
- – whether the business process activities are recorded and reported according to established standards or criteria.
- The two basic functions carried out to examine these changes are



4. **Explain the set of skills that is generally expected of the IS Auditor.**

- Sound knowledge of – business operations
  – practices
  – compliance requirements.
- Should possess the requisite professional technical qualification and certifications.
- A good understanding of information risks and controls.
- Ability to understand technical and manual controls.
- Knowledge of – IT strategies
  – policy and
  – procedural controls.
- Good knowledge of professional standards and best practices of IT controls and security.

5. **Explain the functions of IS Auditor.** **OR**
What are the risks reviewed by you as an IS Auditor as a part of the IT Systems and processes.
   - IS Auditor often is the assessor of business risk.
   - The auditor can check the technicalities well enough to understand the risk and make a sound assessment and present risk oriented advice to management.
   - IS Auditor's review risks related to IT system and processes.
   - Some of the review risks are
     - Inadequate information security controls
     - Inefficient use of resources
     - Ineffective IT strategies, policies and practices
     - IT related frauds.

6. **Explain briefly the steps involved in Information System Audit. (SPF-RC)**
   a) **Scoping and pre-audit survey:**
      - Auditor determines the main areas of focus and any areas that are explicitly out of scope.
   b) **Planning and preparation:**
      - During which the scope is broken into greater levels of details.
      - It usually involves the generation of audit work plan and risk-control-matrix.
   c) **Fieldwork:**
      - This step involves gathering of evidence by
        - interviewing staff and managers
        - reviewing documents and
        - observing processes etc.
   d) **Reporting:**
      - Reporting to management is done after analysis of evidence is gathered and analysed.
   e) **Closure:**
      - Closure involves preparing notes for future audit and follow up with management to complete the actions they promised after previous audits.

7. Explain the inherent limitations with respect to IS Audit

As per SA 200, any opinion formed by the Auditor is subject to inherent limitations of an audit which include:

- The nature of financial reporting
- The nature of audit procedures
- The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
- Fraud, particularly fraud involving senior management or collusion.
- The existence and completeness of related party relationships and transactions
- The occurrence of non compliance with laws and regulations
- Future events or conditions that may cause an entity to cease to continue as a going concern.

8. Explain the categories of Information System Audit. (SIS-MT)

a) Systems and Application:

- - An audit to verify that systems and applications are appropriate, efficient and adequately controlled
  - To ensure valid, reliable, and timely and secure input, processing and output at all levels of a system's activity.

b) Information Processing Facilities:

- - An audit to verify that the processing facility is controlled.
  - To ensure timely, accurate and efficient processing of applications.
  - Under normal and potentially disruptive conditions.

c) System Development:

- - An audit to verify that the systems under development meet the objectives of the organization and
  - To ensure that the systems are developed in accordance with generally accepted standards for system development.

d) Management of IT and Enterprise Architecture:

- - An audit to verify that IT management has developed an organizational structure and procedures.
  - To ensure a controlled and efficient environment for information processing.

e) Telecommunication, Intranet and Extranet:

- An audit to verify that controls are in place on the client, server and on the network connecting the client and server.

9. Explain the types of Audit Tools with respect to IS Audit. (SIS-CA)

a) Snapshots:

- Tracing a transaction in a computerised system can be performed with the help of snapshots or extended records.
- The snapshot software is built into the system at those points where material processing occurs which takes the image of the flow of any transaction as it moves through the application.

b) Integrated Test Facility (ITF):

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

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 systems transaction.
- The information collected is written on a special audit file known as the SCARF master files.

d) Continuous Intermittent Simulation (CIS):

- This is the variation of the SCARF technique.
- It can be used to trap exceptions whenever the application system uses a database management system.

e) Audit Hooks:

- These are audit routines that flag suspicious transactions.
- When audit hooks are employed, auditors can be informed of questionable transaction as soon as they occur.
- This approach of real-time notification displays a message on the auditor's terminal.

10. Explain the important points in the planning phase of an IS Audit

- Planning is one of the primary and important phase in an IS Audit.
- It ensures that the audit is performed in an effective manner.
- Important points are as follows:
  - The extent of planning will vary as per – The size of the entity
    - Auditor's experience
    - Knowledge of business.
  - Obtaining knowledge of the business is an important part of planning the work.
  - The auditor may wish to discuss elements of the overall audit plan and certain procedures with the entity's – audit committee
    - management and
    - staff

    to improve the effectiveness and efficiency of the audit.
  - The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit.
  - The audit should be guided by an overall audit plan and underlying audit programme and methodology.

11. Explain the steps that can be followed for a risk-based approach to make an audit plan.

- Inventory the information systems in use in the organisation and categorize them.
- Determine which of the systems impact critical functions or assets.
- Assess what risks affect these systems and the severity of the impact on the business.
- Based on the above assessment, decide the
  - audit priority
  - resources
  - schedule and
  - frequency.

12. Explain some of the critical factors, which should be considered by an IS Auditor as a part of the preliminary review.

a) Knowledge of the business:

- General economic factors and industry conditions.
- Nature of business, its products and services.
- General exposure to business.
- Its clientele, vendors and strategic business partners.
- Level of competence of the top management and IT management.
- Set up and organization of IT department.

b) Understanding the Technology: It includes the following considerations

- Analysis of business processes and level of automation.
- Role of IT in the success and survival of business.
- Understanding the technology architecture.
- Understanding the extended enterprise architecture.
- Knowledge of various technologies and their advantages and limitations.
- Studying IT policies, standards, guidelines and procedures.

c) Understanding the Internal Control System:

- For gaining understanding of internal control system emphasis to be placed on compliance and substantive testing.

d) Legal considerations and Audit Standards:

- The auditor should carefully evaluate the legal as well as statutory implications on his audit work.
- - The IS audit work could be required as part of a statutory requirement
  - In which case he should take into consideration the related stipulations, guidelines and regulations.
- - The statutes or regulatory framework may impose stipulations
  - As regards minimum set of control objectives to be achieved by the subject organisation.
- The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work.

e) Risk Assessment and Materiality:

- Risk assessment is a critical and inherent part of the Information systems Auditor's planning and audit implementation.
- The Risk assessment will aid in planning decisions such as:
  - The nature, extent and timing of audit procedures.
  - The areas or business functions to be audited.
  - The amount of time and resources to be allocated to an audit etc.

13. Write a short note on SCARF

- For meaning refer **QNO.9**
- Auditors might use SCARF technique to collect the following types of information:

  a) Application system errors:

  - SCARF audit routines provide an independent check on the quality of the system processing.
  - Whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.

b) Policy and procedural variances:

- SCARF audit routines can be used to check when variations from the applicable policies, procedures and standards have occurred.

c) System exception:

- SCARF can be used to monitor different types of application system exceptions

d) Statistical sample:

- SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

e) Snapshots and Extended records:

- It can be returned into the SCARF file and printed when required.

f) Profiling data:

- Auditors can use embedded audit routines to collect data to build profiles of system users.

14. <u>Write a short note on Continuous and Intermittent Simulation (CIS)</u>

- This is a variation of the SCARF techniques.
- It can be used to trap exceptions whenever the application system uses a Database management system.
- During application system processing CIS executes in the following way:

a) – The DBMS reads an application system transaction.
- It is passed to the CIS
- CIS then determines whether it wants to examine the transaction further.

b) CIS replicates or simulates the application system processing.

c) – Every update to the database that arises from processing the selected transaction will be checked by the CIS
- to determine the whether discrepancies exist or not.

d) Exceptions identified by CIS are written to an exception log file.

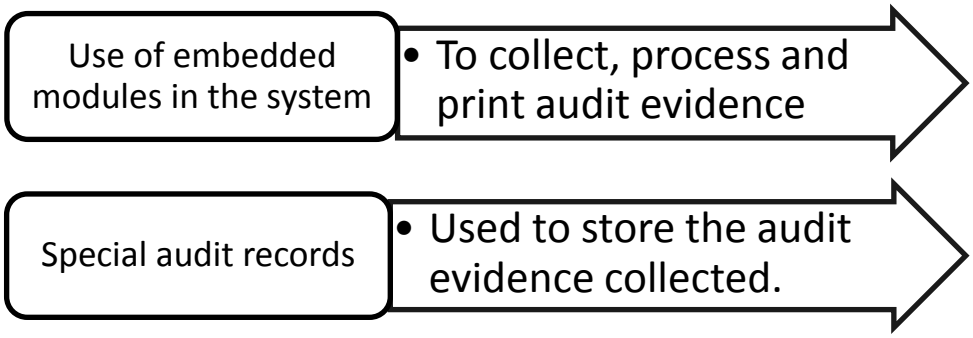
e) – The advantage of CIS is that it does not require modifications to the application system and yet provide an online auditing capability.

15. Write a note on Audit Evidence in relation to IS Audit:

- According to SA 230, Audit documentation refers to the record of
  - Audit procedures performed
  - Relevant audit evidence obtained and
  - Conclusions the auditor reached.
- The objects of auditor's working papers are to record and demonstrate the audit work from one year to another.
- Evidences are also necessary for the following purposes:
  a) means of controlling current audit work.
  b) Evidence of audit work performed.
  c) Schedules supporting or additional items in the accounts and
  d) Information about the business being audited, including the recent istory.
- In IS environment, a critical issue is that evidences are not available in physical form but are in electronic form.

16. Write a short note on concurrent or continuous audit

- It enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the events at the client and auditors assurance services thereon.
- Continuous auditing techniques uses two basis for collecting audit evidence:



17. Explain briefly the advantages and disadvantages of Continuous Auditing

- Reducing the cost of the basic audit assignment by enabling auditor to test a larger sample and examine data faster and more efficiently.
- Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions.
- Increasing the quality of audits by allowing auditors to focus more on understanding – A clients business
  - industry
  - External control structure.
- Specifying transaction selection criteria to choose transaction and perform both test of controls and substantive tests throughout the year on an ongoing basis.

Other advantages of Continuous Audit Techniques (CATs):

- Timely, comprehensive and detailed auditing
- Surprise test capability
- Information to system staff on meeting objectives
- Training for new users

Disadvantages of Continuous Auditing:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation and maintenance of CATs.
- These are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer system to be able to use CATs effectively and efficiently.
- These are more likely to be used where the audit trail is less visible and the cost of errors and irregularities are high.
- These are unlikely to be effective unless they are implemented in an application system that is relatively stable.

18. Write a note on Audit Trails:

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

19. Explain the Three major ways by which audit trails can be used to support security objectives.

a) Detecting Unauthorised Access:

- It can occur in real time or after the fact.
- The primary objective of real time detection is to protect the system from outsiders.

b) Reconstructing Events:

- Audit analysis can be used to reconstruct the steps that led to the events such as – system failures
  - security violations from individuals or
  - application processing errors.
- Audit trail analysis also plays an important role in accounting control.

c) Personal Accountability:

- Audit trails can be used to monitor user activity at the lowest level of detail.
- This capability is a preventive control that can be used to influence behaviour.

20. Explain the role of an IS Auditor in Physical Access Controls.

- Auditing physical access requires the auditor to review the physical access risk and controls to form opinion on the effectiveness of the physical access controls.
- This involves the following:

a) Risk Assessment:

- The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely – assessment of all assets
  - physical access threats
  - vulnerabilities of safeguards
  - exposures there from.

b) Controls Assessment:

- Auditor based on the risk profile evaluates whether physical access controls are in place and adequate to protect the IS assets against the risks.

c) Review Documents:

- It requires examination of relevant documentation such as
  - the security policy and procedure
  - premises plans
  - building plans etc.

21. Explain the role of an IS Auditor in Environment Control:

- Audit of environmental controls should form a critical part of every IS Audit plan.
- The IS Auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against all acceptable risks.
- Some of the critical audit considerations that an IS Auditor should take into account while conducting the audit is:

a) **Audit planning and Assessment:** As part of risk assessment

- The risk profile should include the different kinds of environmental risks that the organisation is exposed to.
- The control assessment must ascertain that controls safeguard the organisation against all acceptable risks.

- The security policy of the organisation should be reviewed to assess policies and procedures that safeguard the organisation.
- Building plans and wiring plans need to be reviewed.
- Administrative procedures need to be reviewed.

b) **Audit of Environmental Controls:** The auditor should verify that

- The Infrastructure Planning and Facilities (IPF) and the construction.
- The presence of – water and smoke detectors
  - power supply arrangements
  - testing logs.
- The location of – fire extinguishers
  - fire fighting equipment.
- Emergency procedures, evacuation plans and marking of fire exists.
- Documents for compliance with legal and regulatory requirements with regard to – fire safety equipment
  - external inspection certificate &
  - short comings pointed out by other inspectors/auditors.
- Power sources and conduct tests to assure the quality of power effectiveness of power conditioning equipment and generators.
- Environmental control equipments such as air conditioning, heaters, dehumidifiers, ionizers etc.
- Identify undesired activities such as smoking, consumption of eatables etc.

c) Documentation:

- As part of the audit procedures, IS Auditor should also document all findings.
- The working papers could include – Audit assessment6s
  - audit plans
  - audit procedures
  - questionnaires
  - interview sheets
  - inspection charts etc.

22. Explain the types of managerial controls.

a) **Top Management and Information Systems Management Controls:**
   - Discusses the top management's role in planning, organizing, leading and controlling the IS functions.

b) **System Development Management Controls:**
   - It provides a contingency perspective on models of the information systems development process, that auditor can use as a basis for evidence collection and evaluation.

c) **Programming Management Controls:**
   - Discusses the major phases in the program life cycle and the controls that should be exercised in each phase.

d) **Data Resource Management Controls:**
   - Discusses the role of database administrator and the controls that should be exercised in each phase.

e) **Quality Assurance Management Controls:**
   - Discusses the major functions that quality assurance management should perform to ensure that the development, implementation, operation and maintenance of IS conforming to quality standards.

f) **Security Management Controls:**
   - Discusses the major functions performed by operations by security administrators to identify major threats to the IS functions and to design, implement, operate and maintain controls.

g) **Operations Management Controls:**
   - Discusses the major functions performed by operations management to ensure the day to day operations of the IS functions are well controlled.

23. Write a note on Audit Trail with respect to Managerial Controls.

MANAGERIAL CONTROLS	AUDIT TRAILS
1.TOP MANAGEMENT AND INFORMATION SYSTEM MANAGEMENT CONTROLS	❖ **Planning:** • Auditors need to evaluate whether top management has formulated a high-quality IS's plan that is appropriate to the needs of an organization or not. ❖ **Organising:** • Auditor should be concerned about how well top management acquires and manages staff resources. ❖ **Leading:** • Auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. ❖ **Controlling:** • Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.
2.SYSTEM DEVELOPMENT MANAGEMENT CONTROLS	❖ **Concurrent Audit:** • Auditors assist the team in improving the quality of system development for the specific system they are building and implementing. ❖ **Post-implementation Audit:** • Auditors seek to help an organisation learn from its experience in the development of a specific application system. ❖ **General Audit:** • Auditors seek to determine whether they can reduce extent of substantive testing needed to form an audit opinion about management's assertions relating to financial statements for system effectiveness & efficiency.
3.PROGRAMMING MANAGEMENT CONTROLS	❖ **Planning:** • Auditors must evaluate how well the planning work is being undertaken. ❖ **Control:** • Auditor must evaluate whether the nature of and extent of control activities undertaken are appropriate for different types of software that are developed or acquired.

	❖ **Design:** • Auditors should find out whether programmers use some type of systematic approach to design. ❖ **Coding:** • Auditors should seek evidence to check whether programmers employ automated facilities to assist them with their coding work. ❖ **Testing:** • Auditor's primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed. ❖ **Operation and Maintenance:** • Auditors need to ensure effectively and timely reporting of maintenance is carried out in a well-controlled manner.
4.DATA RESOURCE MANAGEMENT CONTROLS	❖ Auditor should determine what controls are exercised to maintain data integrity. ❖ They might also interview database users to determine their level of awareness of these controls. ❖ Auditors might employ test data to evaluate whether access controls and update controls are working.
5.QUALITY ASSURANCE MANAGEMENT CONTROLS	❖ Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance personnel perform their monitoring and reporting functions.
6.SECURITY MANAGEMENT CONTROLS	❖ Auditors must evaluate whether security administrators are conducting ongoing high quality security reviews or not. ❖ Auditors check whether the organizations have opted appropriate Disaster Recovery and Insurance plan or not.
7.OPERATIONS MANAGEMENT CONTROLS	❖ Auditors should pay concern to see whether the documentation is maintained securely and that it is used only to authorised personnel.

24. Explain briefly the types of Application Controls.

a) Boundary Controls:

- Establishes interface between the user of the system and the system itself.
- The system must ensure that it has an authentic user.
- Users allowed using resources in restricted ways.

b) Input Controls:

- Responsible for bringing both the data and instructions in to the information system.
- They are validation and error detection of data input into the system.

c) Communication Controls:

- Responsible for controls over – Physical components
  - communication line errors
  - flows and links
  - topological controls
  - channel access controls
  - internetworking controls
  - existence controls and
  - audit trail controls.

d) Processing Controls:

- Responsible for computing, sorting, classifying and summarising data.
- It maintains the chronology of events from the time data is received from input to the time data is stored into database.

e) Output Controls:

- To provide functions that determine
  - the data content available
  - data format
  - timeliness of data &
  - how data is prepared and routed to users.

f) Database controls:

- Responsible to provide functions to define, create, modify, delete & read data in an IS.
- It maintains procedural data set of rules to perform operations on the data.

25. Discuss the Audit trails for Application Controls.

The two types of Audit Trails that exist in each application Controls are

- An **Accounting Audit Trail** – To maintain a record of events within the subsystem.
- An **Operation Audit Trail** – To maintain a record of the resource consumption associated with each event in the subsystem.

APPLICATION CONTROLS	ACCOUNTING AUDIT TRAIL	OPERATION AUDIT TRAIL
BOUNDARY CONTROL	• Action privileges allowed/denied	• Resource usage from log-on to log-out time • Log of resource consumption
INPUT CONTROLS	• The identity of the person who was the source of the data. • The identity of the person who entered the data into the system. • The time and date when the data was captured. • The details of the transaction.	• Time to key in a source document or an instrument at a terminal. • Number of read errors made by an optical scanning device. • Number of keying errors identified during verification.
COMMUNICATION CONTROLS	• Unique identifier of the source/sink node. • Time and date at which the message was received by the sink node. • Time and date at which node in the network was traversed by the message.	• Number of messages that have traversed each link and each node. • Log of system restarts. • Message transit times between nodes and at nodes.
PROCESSING CONTROLS	• To trace and replicate the processing performed on a data item. • Triggered transactions to monitor input data entry, intermediate results & output data values	• A comprehensive log on hardware consumption. • A comprehensive log on software consumption.

DATABASE CONTROLS	• To attach a unique time stamp to all transactions. • To attach before-images & after-images of the data item. • Any modifications or corrections to audit trail transactions.	• To maintain a chronology of resource consumption events.
OUTPUT CONTROLS	• What output was presented to users • Who receive the output • When the output was received & • What actions were taken with the output	• To maintain the record or resource consumed.

26. <u>Explain different layers in an application security audit.</u>

a) <u>Operational Layer:</u>

➢ The basic layer, where user access decision are generally put in place.

b) <u>Tactical Layer:</u>

➢ The next is management layer, which includes supporting functions such as – Security administrator
- IT risk management and
- Patch management.

c) <u>Strategic Layer:</u>

➢ This is the layer used by top management and it includes
- Overall information governance
- Security awareness
- Supporting information security policies and standards
- Overarching an application security perspective.

27. Write a note an approach to Application Security Audit.

- It is being looked from the usage perspective.
- A layered approach is used based on the functions and approach of each layer.
- This approach is in line with the management structure which follows top-down approach.
- For this auditor need to have a clear understanding of the following:

  a) Business process for which the application has been designed.
  b) The source of data input to and output from the application.
  c) The various interfaces of the application under audit with other applications.
  d) The various methods that may be used to login to application.
  e) The roles, descriptions, user profiles and user groups that can be created in an application &
  f) The policy of the organization for user access and supporting standards.

28. Discuss major audit issues of operational layer with reference to application security audit.

a) User Accounts and Access Rights:

- This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities.
- Auditor needs to ensure the use of unique user ID's.
- In case guest ID's are used and then these should be tested.
- Vendor accounts and third party accounts should be reviewed.
- In essence, users and applications should be uniquely identifiable.

b) Password Controls:

- Auditor needs to check whether there are applications where password controls are weak.
- In case such instances are found, then auditor may look for compensating controls against such issues.

c) **Segregation of Duties:**

- It is a basic internal control that prevents or detects errors and irregularities.
- Example – Record keeper of asset must not be asset keeper
  - Maker must not be a checker.
- Auditor needs to check that there is no violation.
- Any violation may have serious repercussions, the same needs to be immediately communicated to TCWG.

29. Explain the categories of risks which should be taken into consideration at the time of assessment or audit of information system.

a) **Inherent Risk:**

- It is the susceptibility of information resources or resources controlled by the information system to – material theft
  - destruction
  - disclosure
  - unauthorised modification or
  - other impairment

  assuming that there are no related internal controls.

b) **Control Risk:**

- – It is the risk that could occur in an audit area and
  - which could be material individually or in combination with other errors
  - will not be prevented or detected and corrected on a timely basis by the internal control system.

c) **Detection Risk:**

- – It is the risk that the IT auditor's substantive procedures will not detect an error
  - which could be material individually or in combination with other errors.