Auditing of Information Systems

[Exam importance- 24 marks; easiest chapter of the ISCA course; LBH]

- **Need for Audit of Information Systems:**
  - Factors that influence org. towards control and audit of computers:
    1. Cost of Data Loss
    2. Cost of Incorrect Decision Making
    3. Cost of Computer Abuse
    4. Value of Computer H/w, S/w and Personnel
    5. High Cost of Computer Error
    6. Maintenance of Privacy
    7. Controlled evolution of Computer Use

  - Objectives of IS Audit:
    1. Asset Safeguarding objectives
    2. Data Integrity objectives
    3. System Effectiveness objectives
    4. System Efficiency objectives

  - Effects of Computers on Audit:
    - Changes to Evidence **Collection**:
      1. Absence of Input Documents
      2. Audit Evidence in case of Automated Transactions
      3. Lack of Availability of printed Output
      4. Data Retention & Storage
      5. Non-availability of Audit Trails
      6. Legal Issues

    - Changes to Evidence **Evaluation**:
      1. System Generated Transactions
      2. Automated Transaction Processing Systems
      3. Systematic Error

- **Information System (IS) Audit:**
  - Skill set of IS Auditor:
    1. Professional Technical Qualification
    2. Knowledge of Professional Standards and Best Practices
    3. Knowledge of IT Strategies, Policy & Procedural Controls
    4. Knowledge of Business Operations, practices & compliance requirements
    1. Understanding of Information Risks and Controls
    2. Understanding of Technical and Manual Controls

  - Functions of IS Auditor: (***Review risks relating to*** IT systems and processes, like)
    1. Inadequate Information Security
    2. Inefficient use of Corporate Resources or Poor Governance
    3. Ineffective IT Strategies, Policies & Practices
    4. IT-related Frauds

  - Categories/Types of IS Audit: (audit to verify…)
    1. Management of IT and Enterprise Architecture
    2. Information Processing Facilities (Data Centers)
    3. Telecommunications and Networks

4. Systems Development (SDLC)
5. Systems and Applications

- Steps in IS Audit: (draw diagram in exam)
  1. Scoping and pre-audit survey
  2. Planning
  3. Fieldwork (technical testing of IS Controls)
  4. Analysis
  5. Reporting
  6. Closure

- Audit Standards and Best Practices
  1. ISACA (Information System Audit and Control Association)
     a. IS Auditing Standards
     b. IS Auditing Guidelines
     c. IS Auditing Procedures
     d. COBIT (Control Objectives for Information and Related Technology)
  2. ISO 27001
  3. Internal Audit Standards
  4. Standards of Internal Audit issued by ICAI
  5. Information Technology Infrastructure Library (ITIL)

- **Performing IS Audit:**
  - Checking validity of information obtained by IS auditor:
    1. Asking different personnel the same question and comparing answers
    2. Asking same question in different ways at different times
    3. Comparing checklist answers to Work Papers, documentations, and other results
    4. Comparing checklist answers to observations and actual system results
    5. Conducting mini-studies of critical phases of the operation

  - Basic Plan: (important points to be noted)
    1. Extent of planning will vary acc. to size of entity, complexity of audit and auditor's experience with the entity and knowledge of its business.
    2. Obtaining knowledge of business is imp. part of planning, as it helps auditor to identify events, transactions and practices which have material effect.
    3. Auditor may discuss elements of overall audit plan with entity's Audit committee, mgt., and staff to improve effectiveness & efficiency of audit; however overall audit plan and program remains the responsibility of the auditor.
    4. Auditor should develop and document the overall audit plan describing the scope and conduct of audit.
    5. Audit should be guided by overall audit plan and underlying audit program & methodology. Also auditor is expected to modify the audit plan as warranted by the circumstances.

  - Preliminary Review: (***critical factors to be considered*** by IS Auditor as part of his PR)
    1. Knowledge of Business
       i. Economic factors and industry conditions affecting entity's business
       ii. Nature of business, its products & services
       iii. General exposure to business
       iv. Its clients, vendors, strategic partners, outsourced service providers

v. Level of competence of Top mgt. and IT management
vi. Set up and organization of IT department

2. Understanding the Technology
   i. Analysis of business process and the extent of Automation of these processes
   ii. Assessing the dependence of the enterprise on IT to carry on its business
   iii. Understanding Technology Architecture of the entity
   iv. Studying network diagrams to understand connectivity
   v. Understanding Enterprise Architecture; whether org's systems are further connected to vendor, customers, etc.
   vi. Knowledge of various technologies along with its pros and cons is critical competence requirement for the auditor
   vii. Knowledge of entity's IT policies, standards, guidelines and procedures.

3. Understanding Internal Control systems

4. Legal Considerations and Audit Standards
   i. Auditor should carefully evaluate legal and statutory implications of his audit work
   ii. In case IS Audit is to be carried out as part of statutory requirement, then related regulations and guidelines (e.g. SEBI, RBI guidelines) should be taken into consideration for conduct of the audit
   iii. Sometimes regulatory framework MAY impose stipulations as regards to minimum set of control objectives to be achieved, etc.
   iv. IS Auditor should also consider the Audit Standards applicable to his audit work. Non-compliance would result in violation of professional ethics and also with an adverse impact on his audit work.

5. Risk Assessment and Materiality:
   i. Risk Assessment helps in planning decisions like:
      i. Nature, extent and timing of audit procedures
      ii. Areas to be audited in detail
      iii. Amount of time and audit resource to be allocated to an audit
   ii. Risk based approach to make an audit plan: (Steps):
      i. Make a list of ISs used in the organization
      ii. Determine which of these can impact critical functions or assets of the company; and how close they operate in real time
      iii. Assess what kind of Risks affect these systems along with their impact on the business {impact analysis}
      iv. Based on above decide: Audit priority, resources, schedule and frequency
   iii. Categories of risk:
      i. Inherent Risk (… assuming there are No internal controls)
      ii. Control Risk (a measure of auditor's assessment of the likelihood that risk may exceed a tolerable level which would have a material effect)
      iii. Detection Risk (risk that the IT Auditor's substantive procedures will not detect an error which could be material in nature)

- **<u>IS Audit and Audit Evidence:</u>**
  - Opinion formed by IS Auditor is subject to Inherent (built in) Limitations of an Audit: (Same as audit; pg-6.10 JC Book)

  - Concurrent or Continuous Audit Techniques (CAT):
    - They use Embedded modules in the system and Special Audit Records in order to collect audit evidence.

    - Need for CAT:
      1. Insufficient audit trails
      2. Live evidence collection
      3. Difficult to stop the system

4. Heavy volume of data
5. Continual monitoring

- CAT is a broader concept, which focuses on simultaneous audit activity along with business processes. In can be done manually or automatically. When it is carried out automatically using a s/w then it is termed as CAAT (Computer Assisted Auditing Techniques/Tools) or Audit using embedded audit modules.

- Types of *Audit Tools/Techniques/ CAAT*:
  1. Snapshots:
     a. Built into the system at those points where important processing takes occurs.
     b. Takes Before and After Images of the flow of transactions as it moves through an application.
     c. Auditor reviews these images to ensure that the processing logic is executed properly, its authenticity, accuracy and completeness.
     d. Key areas to focus while using snapshots are:
        i. Choosing right location/ points based on the materiality of transactions
        ii. Deciding on the time of capture
        iii. Reporting system design to present data in a meaningful way for auditors to understand.

  2. Integrated Test Facilities (ITF):
     a. Small sets of fictitious (dummy) records are processed along with regular records.
     b. They do not affect the regular records and employees are unaware of the testing taking place.
     c. At the end of the processing, the system collects ITF Dummy records and the processing results. The auditor compares with expected results to verify if controls are working as desired.
     d. Methods of Entering and Removing Test Data. *[Draw the diagram in the exam and explain in short]*

  3. SCARF (System Control and Audit Review File):
     a. Involves embedding audit modules to continuously monitor transaction activities, which the auditor feels is material.
     b. Data deemed important by auditor are recorded in a SCARF file or audit log.
     c. Auditors then examine the SCARF file to so see if any transactions require follow up or not.
     d. Types of information (/evidence) which might be collected using SCARF:
        i. System Exceptions/ overrides
        ii. Application System Errors
        iii. User Profiling
        iv. Statistical Sampling
        v. Performance Measurement
        vi. Policy & procedural variances
        vii. Snapshots and extended records

  4. Continuous and Intermittent Simulation (CIS):
     a. Is a variation of SCARF technique

b. Can be used to Trap Exceptions whenever the application system uses a Database Management System
c. Steps of CIS:
   i. DBMS reads an application system transaction and passes it on to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next step; else CIS waits for further transactions from DBMS.
   ii. CIS replicates/ simulates the application system processing.
   iii. CIS then checks this processed transaction to determine whether any discrepancies exist between the results it produces and those the application system produces.
   iv. Exceptions identified by CIS are written on the exception file.
   v. The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

5. Audit Hooks:
   i. These are audit routines that flag suspicious transactions, by devising a system that tags records.
   ii. The internal audit department will investigate these tagged records for detecting fraud. Auditors are informed of questionable transactions as soon as they occur.
   iii. This approach displays real time notification on auditor's terminal. And is mainly helpful in the case of crores of transactions of Insurance cos.

- Advantages of Continuous Auditing:
  1. Reducing the amount of Time and Cost that auditors spend on manual examination of transactions.
  2. Enabling auditors to test larger sample of transactions at reduced costs.
  3. Increasing the quality of audits by allowing auditors to focus more on understanding the client's business and its internal control structure.
  4. Specify transaction selection criteria for performance of test throughout the year.

- Advantages of Continuous Audit Techniques/Tools:
  1. Timely, comprehensive and detailed auditing
  2. Surprise Test Capability
  3. Information to Staff on Meeting Objectives
  4. Training for new users

- Disadvantages (Considerations) of Continuous Audit Techniques/ Tools:
  1. Auditors should be able to obtain resources from the organization to support development, implementation, operation and maintenance of CAT.
  2. CAT is more likely to be used if Auditor is involved in development work of new application system.
  3. Auditors need the knowledge and experience of working with computer systems to be able to use the CAT effectively & efficiently.
  4. CAT is more likely to be used where audit trail is less visible and the cost of errors is high.
  5. CAT is unlikely to be effective, unless they are implemented in an application system that is relatively stable.

- Audit trails and its objectives:
  - Audit trails are logs that can be designed to record activity at system, application and user level. When properly implemented, it provides an important detective control to accomplish security policy objectives.

- They ensure that "chronological record of all events" that have occurred in a system is maintained.
- Objectives of Audit Trails: (DRA)
  - (i) Detecting Unauthorized Access
  - (ii) Reconstructing Events
  - (iii) Personal Accountability

➢ **<u>Audit and Evaluation Techniques for Physical and Environmental Controls:</u>**

- Role of IS Auditor in Physical Access Controls:
  1. Risk Assessment
  2. Controls Assessment
  3. Review of Documents

- Audit of Environmental Controls:
  - Audit Planning and Assessment:
    1. Risk Profile
    2. Control Assessment
    3. Security Policy
    4. Building plans and wiring plans
    5. Interview personnel
    6. Administrative procedures

  - <u>Audit of Environmental Controls:</u> requires IS Auditor to conduct physical inspections and observe practices:
    1. Infrastructure Planning & Facilities (IPF) and the construction with regard to the type of materials used for construction.
    2. Presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
    3. Location of fire extinguishers, firefighting equips. and re-filling dates.
    4. Emergency procedures, evacuation plans and marking of fire exists and half yearly fire drills to test readiness.
    5. Documents for compliance with legal and regulatory requirements with regards to fire safety equip., external inspection certificate and shortcoming if any.
    6. Power sources and test to assure the quality & reliability of power and generators.
    7. Environmental control equipments like A/c, dehumidifiers, heaters, etc.
    8. Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (To Repair) are within Acceptable levels.
    9. Identify undesired activities such as smoking, consumption of eatables, etc.

  - Documentation: IS Auditor should document all the findings:
    1. Safeguards against the risks of heating, ventilation and air-conditioning systems.
    2. Control of radio emissions affect on computer systems.
    3. Establish adequate interior security based on risk.
    4. Adequately protect against emerging threats, based on risk.
    5. Adequate environmental controls have been implemented.
    6. Staff has been trained to react to emergencies.

➢ **<u>Managerial Controls and their audit trails:</u>** (covered in Ch-3) [Areas IS Auditor should pay attention while evaluating managerial controls and its types]

1. Top Management and IS Management Controls:
   a. Planning

b. Organizing
c. Leading
d. Controlling

2. System Development Management Controls (SDLC)
    a. Concurrent Audit
    b. Post-implementation Audit
    c. General Audit
3. Programming Management Controls (PDLC)
    a. Planning
    b. Control
    c. Design
    d. Coding
    e. Testing
    f. Operation & Maintenance
4. Data Resource Management Controls
5. Quality Assurance Management Controls
6. Security Management Controls
7. Operations Management Controls

- **<u>Application Controls and their Audit Trails:</u>** (covered in detail in Ch-3) (Types)
    1. Boundary Controls
    2. Input Controls
    3. Processing Controls
    4. Output Controls
    5. Database Controls
    6. Communication Controls

    - Audit Trail Controls: 2 types of audit trails that should exist in each sub-system:
        1. Accounting audit trail- to maintain <u>records of events</u> within the subsystem (basic evidences; like identity, date & time)
        2. Operations audit trail- to maintain <u>records of the resource consumption</u> associated with each event in the subsystem (detailed evidences; like performance records, errors/ integrity, resource consumption)

    - Boundary Controls:
        - They maintain chronology of events that occur when a user attempts to gain access to and employ system's resources.
        - Accounting audit trail …
        - Operations audit trail …

    - Input Controls:
        - They maintain 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.
        - Accounting audit trail …
        - Operations audit trail …

    - Processing Controls:
        - They maintain chronology of events from the time data is received from the input/ comm. system to the time data is dispatched to the database, comm., or output subsystems.
        - Accounting audit trail …
        - Operations audit trail …

- Output Controls:
  - They maintain 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.
  - Accounting audit trail …
  - Operations audit trail …

- Database Controls:
  - They maintain chronology of events that occur either to the database definition or the database itself.
  - Accounting audit trail …
  - Operations audit trail …

- Communication Controls:
  - They maintain chronology of events from the time a sender dispatches a message to the time a receiver obtains the message.
  - Accounting audit trail …
  - Operations audit trail …

➢ **<u>Audit of Application Security Controls:</u>**

- Approach to Application Security Audit:
  - Should be based on a layered approach, i.e. on the basis of activities undertaken at various levels of management.
  - Auditors *need to have clear understanding* of:
    1. Business process for which application has been designed.
    2. Source of input to and output from the application.
    3. Various interfaces of that application with other applications.
    4. Various methods used to login into application, other than normal user id and password.
    5. User profiles and user groups that can be created in the application.
    6. Policy of the organization for user access.

- Various Layers:

i. Operational Layer:
   1. User Accounts and Access Rights
   2. Password Controls
   3. Segregation of Duties

ii. Tactical Layer
   1. Timely updates to user profiles and changing of user accounts
   2. IT Risk Management
   3. Interface Security
   4. Audit Logging and Monitoring

iii. Strategic Layer
   1. Security Standards
   2. Security Guidelines
   3. Core Objectives
   4. Governance
   5. Procedures

Extra:

Information System Controls

b. General Controls:
    i. Types of General Controls: (apply to a wide range of exposures/threats)
        1. Organizational Controls
        2. Management Controls
        3. Financial Controls
        4. Computer Center (Data Center) Controls
        5. Personal Computer Controls
        6. Operating System Controls
        7. Internet & Intranet Controls
        8. System Development Controls
        9. Data Management Controls
        10. BCP Controls

c. Application Controls:
    i. Types of Application Controls: (covered in detail in Chapter 3)