AUDITING OF INFORMATION SYSTEMS

- Organisations rely more on technology for their day to day activities
- The Usage of technology and information system is increasing, associated risk with technology is also imposing threats to the information systems

Need for Audit of Information Systems

- Organisational Cost of data loss:-Data is critical resource of the organisation- for present and future process
- Cost of Incorrect Decision Making:-High Level Decisions of management like detection, investigation and correction of process require accurate data
- Costs of Computer abuse:-Unauthorised access to information systems can lead to destruction of assets
- Value of computer hardware, software and personnel:-Critical resources of the organisation which has a credible impact on the infrastructure and competitiveness
- High Costs of Computer error:- Many Critical, business processes are performed in a computerized environment, a data entry error could cause great damage
- Maintenance of Privacy:-Data Collected in a business process contains private information about an individual, now there is a fear of privacy getting eroded
- Controlled evolution of computer use:-Reliability of complex systems cannot be guaranteed and consequences of using unreliable systems can be destructive

Information System Auditing

Process of attesting objectives that focus on asset safeguarding, data integrity and management objectives that includes effectiveness and efficiency both

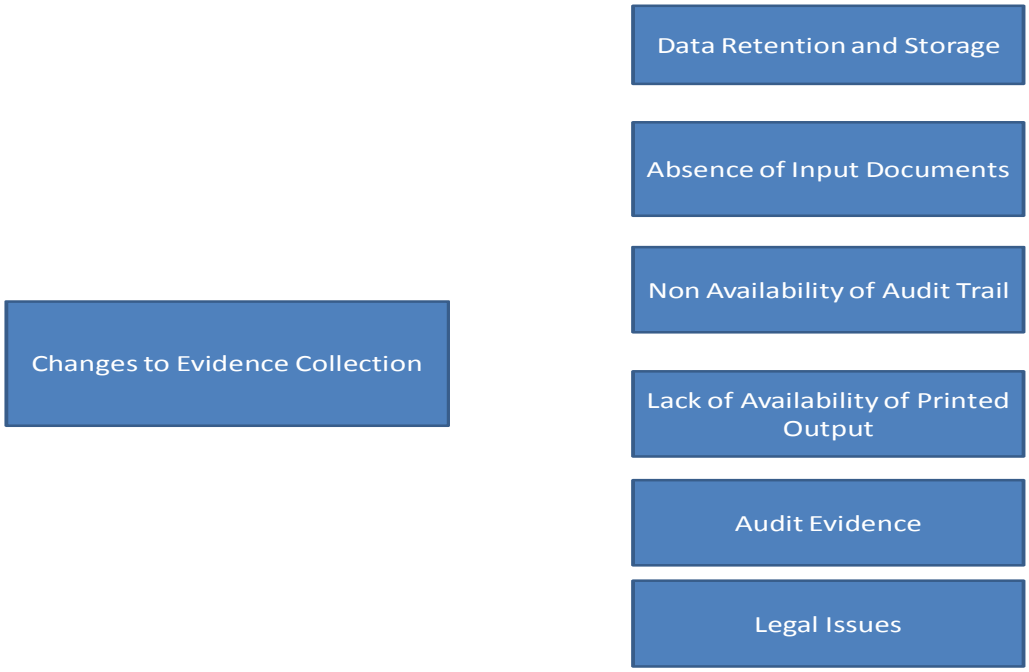
This enables the organisation to achieve the four major objectives as follows

- Asset Safeguarding Objectives-Safeguard Information system assets
- Data Integrity Objectives –Maintain integrity is required all time
- System Effectiveness Objectives:-Effectiveness of system is evaluated by auditing its characteristics and objectives
- System Efficiency Objectives:-Optimise the use of the various information system resources

Effect of Computers on Audit

- Auditor to evaluate whether the business process activities are recorded and reported according to the established standards or criteria
- Two functions carried out to evaluate these changes are
    - Changes to evidence collection, and

- Changes to evidence evaluation



Changes to Evidence Collection

Existence of audit trail is essential for the auditor to gather sufficient, appropriate audit evidence to validate the figures in the client's accounts. The performance of the evidence collection and understanding of the reliability of controls involves issues like

- Data retention and storage:-Storage Capabilities may restrict the amount of historical data to be retained online and accessible to the auditor
- Absence of Input Documents:-Transaction may be entered into the system without the presence of supporting documentation
- Non -Availability of audit trail:-Audit trail may exist only for short period making the auditor call for an approach which involves audit around computer seeking other sources of evidence
- Lack of availability of Printed output:- Results of processing may not produce a hard copy form of output, in absence of these auditor needs to directly access the electronic data retained in the client's computer
- Audit Evidence:-Certain transactions are generated automatically, i.e., depreciation be transferred to the fixed assets register
- Legal Issues:- Use of computers to carry out the activities is also increasing. Many organisations try to make use of the EDI and electronic trading over the internet.

Admissibility of computer evidence in the courts varies from country to country and also from court to court

Changes to Evidence Evaluation

- System Generated Transactions:-Financial systems may have the ability to initiate, approve and record financial transactions
- Automated Transaction Processing Systems:-e.g when the stock falls below the certain level, the system automatically generates a purchase order
- Systemic Error:-Computers are designed to carry out the processing on a consistent basis-same inputs produce the same output

Responsibility for Controls

Management is responsible for the establishing and maintaining controls to achieve the objectives of effective and efficient operations and reliable information systems

- Senior Management:- Responsible for strategic planning
- Middle Management:-Develops the tactical plans, activities and functions
- Supervisory Management:- Oversees and controls the daily activities

IS Audit

IS Audit of Information System environment may include one or both of the following

- Assessment of Internal Controls within the IS environment to assure validity, reliability and security of information and information systems
- Assessment of the efficiency and effectiveness of the IS environment

Skill Set of IS Auditor

The set of skills that is generally expected to be with an IS auditor include

- Sound knowledge of the busines operations, practice and compliance requirements
- Should possess the requisite professional qualifications and certifications
- A good understanding of the Information Risks and Controls
- Knowledge of IT strategy, policy and procedural controls
- Ability to understand technical and manual controls relating to business continuity
- Good knowledge of professional standards and best practices of IT controls and security

Functions of IS Auditor

IS Auditor reviews risks relating to the IT systems and processes, some of them are

- Inadequate information system controls (E.g. Missing or out of date antivirus controls)

- Inefficient use of resources, or poor governance (huge spending on unnecessary IT projects)
- Ineffective IT strategies, policies and practices (including a lack of policy for the use of information and communication technology) resources
- IT related frauds

Categories of Information System Audits

Information Systems Audit has been categorised into five types

- Systems and Application
- Information Processing Facilities
- Systems Development
- Management of IT and Enterprise Architecture
- Telecommunications, Intranets and Extranets

System and Application:- Audit to verify that systems and applications are appropriate are efficient and are adequately controlled

Information Processing Facilities:-Processing facility is controlled to ensure timely, accurate and efficient processing of applications

Systems Development:-Systems under development meet the objectives of the organisation

Management of IT and Enterprise Architecture:-IT management has developed an organisational structure and procedures to ensure a controlled and efficient environment for information processing

Telecommunications, Intranets and Extranets:-Controls are in place on the client, server and on the network connecting the clients and servers

Steps in Information Systems Audit

- Scoping and Pre-Audit Strategy
- Planning and Preparation
- Fieldwork
- Analysis
- Reporting
- Closure

Scoping and Pre-Audit Strategy:-Auditors determine the main areas of focus and any areas that are out of scope

Planning and Preparation:- Scope is broken down into greater levels of detail

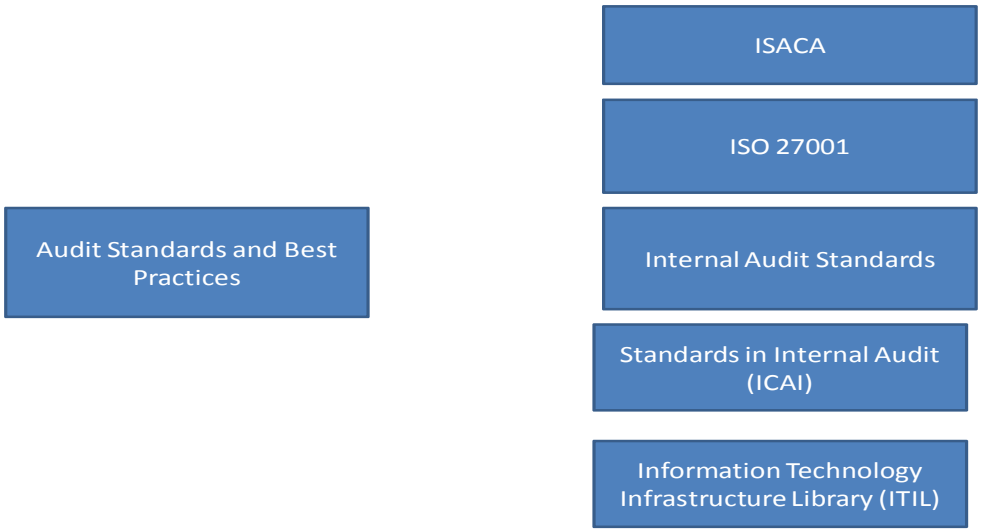
Fieldwork:-gathering of evidence by interviewing staff and managers, reviewing documents and observing processes

Analysis:-Sorting out all the evidence gathered earlier, i.e., SWOT Techniques can be used –also include use of Data analysis tools like ACL, Idea

Reporting:-After analysis of evidence is gathered and analysed, reporting to management is done

Closure:-Preparing notes for future audits and follow up with the management to complete the actions they promised after previous audits

Audit Standards and Best Practices



ISACA (Information Systems Audit and Control Association:-ISACA is a global leader in Information Governance control and it developed the following to assist the IS auditor while carrying out the IS Audit

- IS Auditing Standards:- 16 Auditing Standards defining the mandatory requirements for IS Auditing and reporting
- IS Auditing Guidelines:-39 Auditing Guidelines, proving guideline for applying IS Auditing standards
- IS Auditing Procedures:- 11 Auditing Procedures, provide examples of procedure IS auditor need to follow while conducting IS auditing for complying with IS auditing standards

- COBIT:- Framework containing good business practices relating to information technology

ISO 27001:-International Best Practice and Certification Standard for an Information Security Management System (ISMS). It is a systematic approach to manage information system in an IS environment

Internal Audit Standards:-Institute of Internal Auditors issued Global Technology Audit Guide (GTAG) provides management of Information Technology Management control and Security and IS Auditors with guidance on various information technology associated risks

Standards on Internal Audit Issued by ICAI:- Standards issued by ICAI to be adopted by the auditor in the specific situations

Information Technology Infrastructure Library (ITIL):-It is a set of practices for IT Service Management focusing on aligning the IT services with the needs of the business

Performing an IS Audit

- Auditor uses concept of materiality in financial audits and significance in performance audits to plan efficient and effective audit procedures
- Auditor is not to spend resources on items of lesser importance
- Auditor to conduct the tests with both valid and invalid data to test the ability of error detection, correction and prevention within the application
- Testing of the Critical Controls, Processes and apparent exposures
- Validation of information received is done in the following ways
    - Asking different personnel the same question
    - Asking the same question in different ways at different times
    - Comparing checklist answers to work papers, programs and documentation
    - Comparing checklist answers to observations and actual system results
    - Conducting mini studies of critical phases of the operation

Basic Plan

- Planning is an important phase in information system audit
- Important points
    - Extent of planning varies according to the size of the entity
    - Obtaining knowledge is a part of audit work
    - Auditor may wish to communicate the elements of overall audit plan with the audit committee, management and staff to improve the effectiveness and efficiency of audit
    - Auditor to develop and document the overall audit plan-which should be sufficiently detailed

- Audit to be guided by overall audit program and methodology. Audit planning is mistaken as onetime activity, while it is a continuous activity which goes on throughout the entire audit cycle

Preliminary Review

- The preliminary review of the audit environment enables an auditor to gain understanding of the business, technology and control environment and also gain understanding of the business, technology and control environment and also gain clarity on the objectives and scope of the audit
- Critical factors to be considered by an IS auditor as part of his/her preliminary review
  - Knowledge of the Business
  - Understanding the Technology
  - Understanding the Internal Control Systems
  - Legal Considerations and Audit Standards
  - Risk Assessment and Materiality
- Knowledge of the Business
  - General economic factors and industry conditions
  - Nature of Businesses, its products and services
  - General exposure to business
  - Clientele, Vendors and strategic business partners
  - Setup and Organisation of IT Department
- Understanding the Technology
  - Analysis of the business process and level of automation
  - Understand the technology architecture
  - Studying Network diagrams to understand physical and logical connectivity
  - Understanding extended enterprise architecture
  - Knowledge of various technologies and their advantages and limitations
- Understanding the Internal Control Systems
  - Emphasis to be placed on the Compliance and Substantive testing
- Legal Considerations and Audit Standards
  - Auditor to evaluate the legal as well as statutory implications on the audit work
  - Information System Audit work to be considered as a part of the statutory requirement
  - Regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organisation
  - IS auditor should consider the Audit Standards applicable to the conduct and performance of audit work
- Risk assessment and materiality
  - Risk is a critical and inherent part of Information System Auditor's planning and audit implementation

- It implies identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level
- Risk assessment will aid in planning decisions such as
  - Nature , extent and timing of audit procedures
  - Areas or business functions to be audited
  - Amount of time and resources to be allocated to audit
- Steps that can be followed for the risk based approach to make an audit plan are as follows
  - Inventory the information for use in the organisation and categorise them
  - Determine which all functions affect the critical functions or assets
  - Assess what risks affect these systems and severity of impact on business
  - Decide the audit priority, resources, schedule and frequency based on the above assessment
- Risks are categorised as follows
  - Inherent Risk:-
    - Inherent risk is the risk posed by an error or omission in a financial statement due to a factor other than a failure of control.
    - In a financial audit, inherent risk is most likely to occur when transactions are complex, or in situations that require a high degree of judgment in regards to financial estimates.
    - E.g.:-Fair Value Estimates
  - Control Risk:-
    - Control risk, which is the risk that a misstatement due to error or fraud that could occur in an assertion and that could be material, individually or in combination with other misstatements, will not be prevented or detected on a timely basis by the company's internal control.
    - E.g. Small firms not having the accounts department, financial statements would be prepared by the unskilled force
  - Detection Risk
    - Detection Risk (DR) is the risk that the auditor will not detect a misstatement that exists in an assertion that could be material (significant), either individually or when aggregated with other misstatements
    - E.g.Auditors take samples of the transactions which may not indicate all the risks

IS Audit and Audit Evidence

Audit evidences are necessary for the following purposes

- Means of controlling audit work
- Evidence of audit work performed
- Schedules supporting or additional items in the accounts
- Information about the business being audited, including the recent history

Inherent Limitations of Audit

- For preparing the proper report, the auditor needs documented evidences, problem of the documents not available in physical form is always highlighted . List of actions auditor needs to take to address the problems
    - Use of special audit techniques like CAAT for documenting evidences
    - Audit timing can also be planned that auditor is able to validate transactions

Provisions related to Digital Evidence

As per the Indian Evidence Act, Evidence means and includes

- All statements which the court permits ot requires to be made before it by witnesses
- Documentary evidence for the inspection of the court

Documentary evidence includes the electronic records

Concurrent or Continuous audit

Organisations produce information on a real-time online basis

Types of Audit Tools

Different types of audit techniques be used. Some of the audit tools are as follows

Snapshots

- As the name implies, it involves taking “snapshots” or “pictures” of a transaction as it winds its way through an application system
- Snapshots are taken at material processing points in the application system.
- Auditors must first identify these points and then embed audit modules within the application system at these points.
- At each of these points, the audit modules typically take a snapshot of the transaction just prior to processing and a snapshot just after processing

Integrated Test Facility

- The integrated test facility technique (ITF) involves auditors establishing a mini company or dummy company on the live files processed by an application system.

- For example, in a payroll system, auditors might establish a master-file record for a fictitious employee. Auditors then submit test data to the application system as part of the normal transaction data entered into the system. They monitor the effects of their test data on the dummy entity they have established.

SCARF (System Control Audit Review File)

- SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system transactions
- Information collected is written on to a special audit file-the SCARF master files .
- Auditors then examine the information contained in this file to see if some aspect of the application system needs follow up
- Auditors may use the SCARF to collect the following types of information
  - Application System Errors
  - Policy and Procedure variation
  - System Exception
  - Statistical Sample
  - Snapshots and Extended Records
  - Profiling Data
  - Performance Measurement

Continuous and Intermittent Simulation (CIS)

- Continuous and intermittent simulation (CIS) is a means of collecting audit evidence concurrently withapplication system processing when the application system uses a databasemanagement system to support updating and querying of application files.
- CIS has two major components.
  - First, like SCARF, the database managementsystem must be able to trap transactions that are of interest to the auditor.
  - Second, auditors must write software modules that will replicate the application systemprocessing that is of interest
    - The database management system then passes the transactions it captures across to these modules.
    - These modules in turn determine the results that should be produced as a result of the transaction.
    - The results produced by the audit modules are then compared with the results produced by the application system.
    - Deviations are written to a file for scrutiny by the auditor.

Advantages and Disadvantages of Continuous Auditing

Continuous Auditing has a number of benefits such as

- Reducing the cost of basic audit assignment-auditor can test a larger sample
- Reducing the time and cost spend on the manual transactions
- Increasing the quality of audits by allowing auditor to focus more on understanding the client's business
- Specifying the transaction selection criteria to choose transactions and perform both test of controls and substantive tests

Audit evidence gathered by performing test of controls can be used as a basis for reducing costlier substantive tests, analytical procedures

Advantages of Continuous Audit Techniques are

- Timely, Comprehensive and Detailed Auditing: -Entire process can be evaluated
- Surprise Test Capability: -Gather evidence without the staff being made aware that evidence is gathered
- Information to system staff on meeting the objectives: -Test Vehicle to be used to evaluate whether an application meets the objectives of asset safeguarding, data integrity, effectiveness and efficiency
- Training for new users: -Using ITF's, users can submit data to the application system and obtain feedback on any mistakes they make via system error reports

Disadvantages and Limitations of Continuous Audit System

- Auditors should be able to obtain the resources from the organisation
- More likely only when the auditors are involved with the development of the new system
- Auditors need the knowledge and experience of working with the computer systems
- Used when audit trail is less visible, and cost of errors and irregularities are high
- Unlikely to be effective unless implemented in an application system that is relatively unstable

Audit Trail

- An audit trail can be either a paper or electronically based trail that provides documented history of a transaction within a company.
- An audit trail allows an auditor to trace the financial data from the general ledger to the source document (invoice, receipt, voucher, etc.) and view the full process of a given transaction.
- An audit trail will include the chronological list of steps that were required in order to begin a transaction and bring it to completion.

- An audit trail usually begins with the invoice receipt.
- The transaction is then followed back through accounts payable and finally through to the check or electronic payment made to settle the amount.
- However, an audit trail may contain many more steps and be difficult to follow, depending on the company and the transaction.

Audit Trail Objectives

- Detecting Unauthorised access
- Reconstructing Events
- Personal Accountability

Detecting unauthorised access

Real time detection to protect the system from outsiders who are trying to breach system controls

If properly designed this can be used to find whether unauthorized access was accomplished, or attempted and failed

Reconstructing events

Reconstruct events that lead to the security failure, security violations or application errors. Audit trail also plays an important role in accounting control

Personal Accountability

Monitor the activity at the lowest level of detail. Capability is a preventive control that can be used to influence behavior.

Implementing an Audit Trail

Measuring the potential damage and financial loss associated with application errors, abuse of authority or unauthorized access by outside intruders.

Also provide the valuable evidence for accessing the adequacies of controls in place and need for additional controls

Audit and Evaluation Controls for Physical and Environmental Controls

Role of IS Auditor in Physical Access Controls

- *Risk Assessment*
- *Controls Assessment*
- *Review of Documents*

Risk assessment: - Risk assessment procedure is covering all the assessment of all assets, physical access threats

Controls Assessment: -Whether the physical access controls are in place and adequate to protect the assets against the risks

Review of Documents: -Examination of Documents like Security Policy and Procedures, Premises plans, building plans, inventory list and cabling diagrams

Audit of Environmental Controls

IS Auditor should satisfy not only the effectiveness of various technical controls but also overall controls safeguarding the business against environmental risks

Audit planning and assessment

- Risk profile include different kinds of environmental risks the organisation is exposed to -both natural and man-made threats
- Controls assessment to ensure that the controls safeguard the organisation against all the acceptable risks
- Security policy to be reviewed to access policies and procedures that safeguard the organisation against the risks
- Building plans and writing plans to be reviewed to determine the appropriateness of the location of IPF, review of surroundings, power and cabling, etc.
- Interview personnel to satisfy himself about the employee's awareness of environmental threats and controls
- Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling, inspection and testing plan and procedures

Audit of Environmental Controls

Auditor to verify that

- IPF (Infrastructure Planning and Facilities) and the construction with regard to materials used for construction
- Presence of water and smoke detectors, power supply arrangements
- Location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers
- Emergency plans, Evacuation plans and marking of fire exits
- Documents for compliance with legal and statutory requirements with respect to fire and safety equipment, external inspection certificate

- Power sources and conduct tests to ensure that quality of power, effectiveness of power conditioning equipment
- Environmental Control equipment like Air conditioning equipment, dehumidifiers, heaters
- Identify undesirable activities like smoking, consumption of eatables

Documentation of Findings

As a part of the audit findings an IS Auditor has to document all findings

Control Activity	Control Technique	Audit Procedure
Safeguard against the risk of heating, ventilation and air conditioning	Systems providing constant temperature and humidity levels	Review heating ventilation and air conditioning design
Control of radio emissions	Evaluate electronic shielding to control radio emissions	Review Shielding Strategies
Establish adequate interior security based on risk	Critical systems have emergency power supplies for alarm systems	Verify critical systems Identify backup Procedures
Adequately protect against emergency threats based on risk	Shelter in place for an emergency attack (CBR-Chemical Biological and Radio Active attack) Restricting public access and protect critical entry points	Interview officials, review planning documents and related test results Observe and document the controls on place to mitigate emerging threats Verify the controls existence and intrusion detection sensors
Adequate Environmental controls have been implemented	Fire detection and suppression devices are installed and working Controls are implemented to mitigate disasters such as floods and earthquakes Humidity, temperature and voltage control are maintained at acceptable levels	Interview managers and scrutinise that operations staff are aware of the locations of fire alarms, extinguishers, emergency power off switches Determine that the humidity,temperature and voltage are controlled within the accepted levels
Staff has been trained to react to emergencies	Operational and support staff are trained and understand the emergency procedures Emergency procedures are documented periodically and	Interview security personnel to ensure their awareness and responsibilities Review training records and documentation.Determine the

	tested-incident plan, inspection plan and maintenance plan	scope and adequacy of training Review incident handling procedures and maintenance and inspection plan

Managerial Controls and their Audit Trails

- *Top Management and Information Systems Management Controls:*-Discusses the top management's role in planning, organizing, leading and controlling the information system function
- *System Development Management Controls:*-Contingency perspective on models of information system development process
- *Programming Management Controls:*-Discusses the major phases on the program life cycle and the important controls that should be exercised in each phase
- *Data Resource Management controls:*-Role of database administrator and controls to be exercised in each phase
- *Quality Assurance Management Controls:*-Major functions that the quality assurance management should perform to ensure that the development, implementation, operation and maintenance of information system confirm to quality standards
- *Security Management Controls:*-Major functions performed by security administrators to identify major threats to the IS Functions
- *Operation Management Controls:*-Functions performed by operations management to ensure the day to day operations of the IS function are well controlled

Top Management and Information System Management Controls

Major activities that senior management must perform are planning, organizing, controlling and leading. The Role of auditor at each activity is discussed below

- Planning:-Top management has formulated a plan appropriate to the needs of the organisation
- Organising:- How well top management acquires and manages staff resources for three reasons
    - Effectiveness of the IS function depends primarily on the quality of its staff. IS staff need to remain updated and motivated in their jobs
    - Intense Competition and turnover has made acquiring and retaining good information system staff a complex activity
    - Empirical Research indicates employees are most likely persons to perpetrate irregularities

- Leading:-Auditor examines variables that often indicate when motivation problems exist or suggest poor leadership
- Controlling:- Ensuring that the information systems achieve their objectives at a global level

System Development Management Controls

- Concurrent Audit:- Auditors as members of the System Development team
- Post implementation audit:-Auditors seek to help an organisation learn from its experiences in the development of a specific application system
- General Audit:-Auditors evaluate system development controls overall. They seek to determine whether they can reduce the extent of substantive testing

Programming Management Controls

- Planning:- Nature and extent of planning are appropriate to different types of software acquired or developed
- Control:- Obtain evidence whether the control procedures are operating reliably
- Design:-Whether programmers use some type of systematic approach to design
- Coding:- Level of care exercised by the programming management in choosing a module implementation and integration strategy
- Testing:-Auditor conduct interviews to evaluate how the unit testing is conducted. Auditor's concern is to see that whole of the program tests have been undertaken for all material programs
- Operation and Maintenance:-Management has implemented a review system and assigned responsibility for monitoring the status of operational programs

Data Resource Management Controls

- Auditor to determine what controls are exercised to maintain data integrity
- Auditors to employ test data to evaluate access controls and update controls are working

Quality Assurance Management Controls

- Use interviews, observations and review of documentation to evaluate how well Quality assurance personnel perform the monitoring role
- How Quality Assurance personnel make recommendations for improved standards or processes through interviews, observations and reviews of documentation
- How the QA personnel undertake the reporting function and training through interviews, observations and reviews of documentation

Security Management Controls

- Security Administrators are conducting ongoing , high quality security reviews or not
- Organisations have high disaster recovery plans in place
- Organisations have opted for insurance plan or not

Operations Management Controls

- Whether documentation is maintained securely and it is only issued to secured personnel
- Auditors use interviews, observations and review of documentation to evaluate
    - Activities of documentation librarians
    - How well operations management undertakes the capacity planning and performance monitoring function
    - Reliability of Outsourcing Vendor Controls
    - Whether operations management is monitoring compliance with the outsourcing contract
    - Operations management regularly assess the financial viability of any outsourcing vendors that an organisation uses

Application Controls and their Audit Trails

Types of Application Controls

- Boundary Controls
- Input Controls
- Communication Controls
- Processing Controls
- Output Controls
- Database Controls

Audit Trail Controls

Two types of audit trails that should exist in the subsystem are as follows

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

Audit Trails for Application Controls

Boundary Controls

Maintains chronology of events that occur when a user attempts to gain access to and employ system resources

- Identity of the would be user of the system

- Authentication information supplied
- Resources requested
- Action privileges requested
- Terminal identifier

    - Accounting Audit Trail:- Action Privileges allowed or denied
    - Operations Audit Trail:- Resource usage from time to time and log of resource consumption

Input Controls

Chronology of events from time data and instructions are captured and entered into the system

- Accounting Audit Trail:- Identity of person who was the source of data, who entered data into system, time and date when the data was captured, details of the transaction
- Operations Audit Trail:-Number of read errors identified during verification, number of keying errors identified during verification

Communication Controls

Chronology of events from the time a sender despatches the message to the time a receiver obtains the message

- Accounting Audit Trail:-Unique identifier of the source, unique identifier of each node in the network that traverses the message, time and date at which the message was reeived by the sink node
- Operations Audit Tool:-No of messages that have traversed each link and each node, queue lengths at each node

Processing Controls

It maintains the chronology of events from the time data is received from the input or communication system to the time it is dispatched to the output system

- Accounting Audit Trail:- To trace and replicate the processing performed, triggered transactions to monitor input data entry
- Operations Audit Tool:-CPU time used, secondary storage used, communication facilities

Database Controls

Chronology of events that occur either to the database definition or the database itself

- Accounting Audit Trail:- Unique time stamp to all transactions, modifications or corrections to audit trail transactions accommodating the changes
- Operations Audit Tool:-maintaining the chronology of resource consumption

Output Controls

From the time content of output is determined until the users complete their disposal of output

- Accounting Audit Trail:- what output was presented, who received output, when the output was received , what actions taken with the output
- Operations Audit Tool:-graphs, images, report pages, printing time and display rate to produce the various outputs

Audit of Application Security Controls

- Objective of this exercise is to establish whether the application security controls are operating effectively to protect the confidentiality, integrity and availability of information
- For Carrying out this audit the auditor needs to have a clear understanding of the following
    - Business Process for which the application was designed
    - Source of data input to and output from the application
    - Various interfaces of the application under audit with other applications
    - Various methods to login to the application other than user id and password
- Various Application Security Layers
    - Operational Layer:- User Access decisions are put in place
    - Tactical Layer:- Supporting functions such as security administration, IT risk management and patch management
    - Strategic Layer:- Layer used by the top management Includes overall information security governance, security awareness , supporting information security policies and standards

Layer	Audit Issues
Operational Layer	• User Accounts and Access Rights • Password Controls • Segregation of Duties
Tactical Layer	• Timely Updates to the user profiles • IT Risk Management • Interface Security • Audit Logging and Monitoring
Strategic Layer	• Security Policy to be supported and supplemented by

	detailed standards and guidelines