Audit and Testing of Controls

Chapter 4

Contents

Testing and Testing of Controls

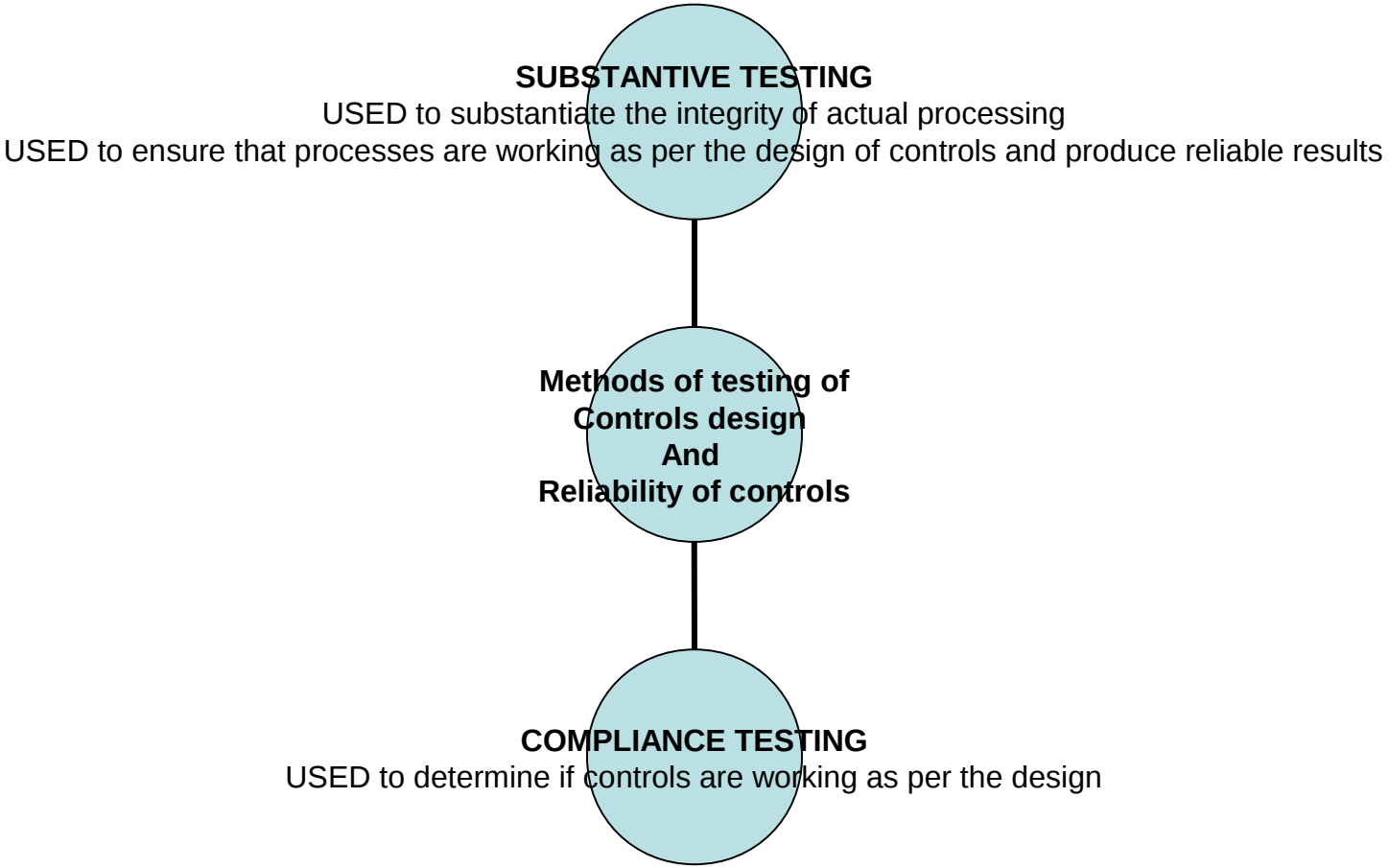
This involves understanding process and its expected results

- Testing
  - Its is a scientific process
  - To determine
  - whether controls ensure effectiveness of
    - system design
    - Implemented system Controls’
- Testing of controls
  - It involves
    - Obtaining the population
    - Conduction compliance test on
      - Entire population or
      - Selected sample from population

Audit Objective

- For each relevant IS Control
  - It has been implemented
  - Determine whether it is suitably designed to achieve critical activity
  - Perform test to determine
    - Whether such control technique are operating effectively
    - Identify potential weakness in IS Control
    - Whether to consider compensating controls

Methods of Testing of Controls



Phases and Process of Information Systems control Audit

- **Phases**
  - **Planning**
    - Determination of effective and efficient way to obtain evidential matter to achieve the objectives of
      - IS Control Audit
      - Audit Plan
  - **Testing**
    - Testing the effectiveness of IS Controls that are relevant to the audit objectives
  - **Reporting**
    - Conclusion on the effect of any identified IS Control weakness and reporting the results including any
      - Material weakness
      - Significant deficiencies

- **Process**

1. *Planning Phase*
   - Obtaining an understanding of
     - an entity
     - Its operations
     - Key business processes
   - Obtaining a general understanding of
     - Structure of entity's network
   - Identifying key areas of audit interest
   - Assessing IS Risk on a preliminary basis
   - Performing other audit planning procedures
1. *Testing Phase*

   - Identifying critical control points

Planning

- Planning activities concentrates on
  - Obtaining an understanding of
    - Entity
    - Its Operations
    - Its Internal Controls
    - Key business processes
  - Identify significant issues
  - Assess Risks
  - *Design nature timing and extent of audit procedures*

  Auditor uses the concept of
  1. Materiality and
  2. Significance

  Including both quantitative and qualitative factors.

  The underlying principle is
  - Not to spend resources on items of little importance
  - Which will not affect the judgment/conduct of a reasonable user of audit report.

Identifying key of audit interest critical to achieving audit objectives

- Key areas are those which are critical to achieve audit objectives

- For each key area the auditor should document
  - The operational location of each key system
  - Significant components of associated hardware and software
  - Other significant systems that support the key areas
  - Prior audit problems reporting
- Identify all access paths into and out of key areas of audit

- Prioritize important systems, files and locations in order of importance to audit objectives
- Characterize them by its sensitivity to business process applications

Preliminary understanding of IS Controls

- Includes documentation of
  1. Identification of for key applications
     1. entity wide level control
     2. business process level controls
  2. Description of entity's use of third party IT services
  3. Any internal or third party information systems review/audit performed during last year
  4. Status of prior audit findings
  5. Management actions/milestones for correction of identified IS/IS Control weakness
  6. Documented
     1. security plan
     2. risk assessments for relevant systems
     3. BCP and DRP
     4. Communication with management
     5. Computer security incidents identified and reported last year
  7. Relevant laws and regulations
  8. Current multi year testing plans
  9. Audit plan that describes audit objectives, scope and methodology

Factors to determine the audit procedure

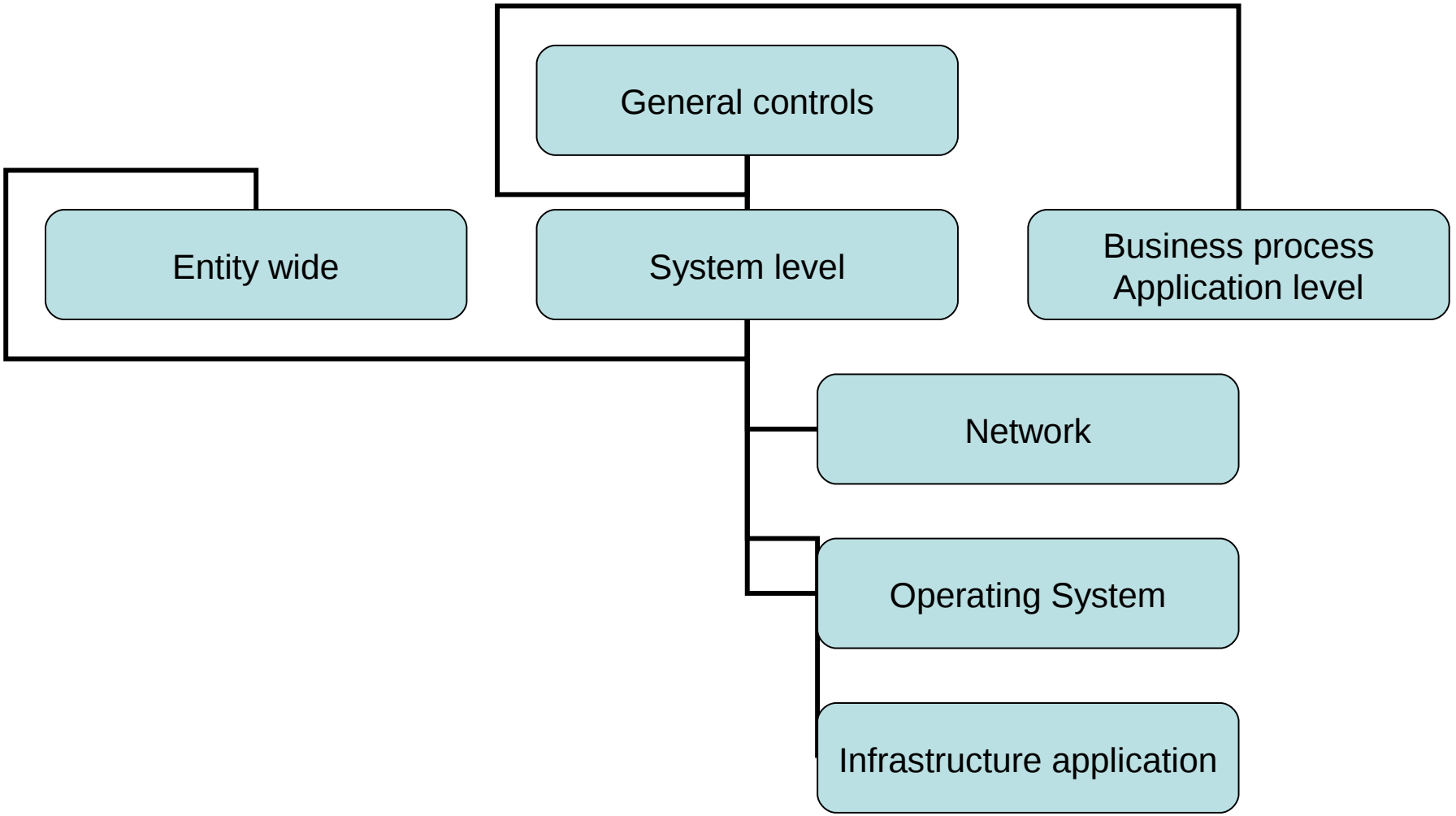
- The auditor needs to determine which audit procedures related to information systems controls are needed to obtain sufficient and appropriate audit evidence to support the audit findings and conclusions
  - The extent to which the internal controls are significant to audit
  - The availability of evidence outside the information system to support the audit findings and conclusions
  - The relationship of information systems controls to data reliability
  - Assessing the effectiveness of information systems controls as an audit objective which is directly a part of audit objectives

Testing

- The auditor must address considerations such as
  - nature,
  - timing and
  - extent of testing
- He should test the
  - critical controls,
  - processes and
  - apparent exposures
- Testing is performed by using
  - documentary evidence,
  - corroborating interviews and
  - personal observation
- Validation of information obtained on testing is prescribed by auditor's work program

- Validation can be done by
  - Asking different personnel the same question and comparing the answer
  - Asking the same question in different ways at different times
  - Comparing checklist to work papers, programs, documentation, tests
  - Comparing checklist answers to observations and actual system results
  - Conducting mini-studies of critical phases of operation

Levels of controls



Levels of controls and Audit

- **If auditor identifies IS Control for weakness, the auditor should evaluate the effectiveness of**
  - General controls at
    - Entity wide levels
    - system level
    - business process application level
- **If the IS Controls identified as general controls, do not help in achieving the control objective than also evaluate the effectiveness of**
  - Specific business process applications and
  - user controls
- The auditor should determine whether these controls are
  - implemented and
  - operating effectively by
    - Identifying the applicable controls
    - Whether they have been placed in operation
    - Determining how those controls function
    - Evaluating and testing the effectiveness of the identified controls

Levels of control and testing

- Where
  - entity-wide,
  - system level and
  - application level controls are determined to be effective,

  auditor performs test of those
  - business process application controls and
  - user controls

- If IS Controls are not effective,
- The auditor should obtain understanding of control risk to
  - Identify the impact of audit objectives
  - Design audit procedures
  - Develop appropriate audit findings

Levels of control and testing

General Controls

Entity wide/

Component Level

They consist of entity-wide or component-wide processes to achieve control objectives

They are focused on how the entity or component manages information system related to each control activity

Testing includes combination of procedures, including

1. observation,
2. inquiry,
3. inspection and
4. re-performance

If general controls at entity level are

- not effectively designed and
- not effectively operating as intended

than auditor should

for achieving IS control objectives

1. Determine and document the nature and extent of risks resulting there from
2. Identify and test manual controls

If manual control do not achieve objectives,

auditor should determine whether any specific controls are designed

If there are no specific controls auditor should

1. develop appropriate findings and
2. recommend to improve internal control

If the specific controls are designed but ineffective than

testing is not necessary

except to support the findings

Levels of control and testing

General Controls System level They are more specific than general controls at entity-wide level	They consist of processes for managing specific system resources related to either general support system or major application There are three further level Network – It is interconnected configuration of components Operating System – It is a software that controls the execution of computer programs and provides various services Infrastructure Applications – They are soft wares that are used to assist in performing the systems operations, including management network devices .	Same as testing of General Control of entity wide level

Levels of control and testing

General Controls Business Process Application level These controls as well as categories of these controls are applicable to controls are entity-wide level and system level	They consist of policies and procedures for controlling specific business processes	If auditor reaches a favorable conclusion on general controls at • entity wide and •system level, than the auditor should test the effectiveness of general controls of •applications which are within the business process application controls These are referred to as Application Security Controls

Appropriateness of control test

- **To assess the operating effectiveness of IS controls, auditor should perform appropriate mix of audit procedures.**

- **These procedures are**
  - *Those relate to gathering information*

1. Inquires from IT and management personnel can enable the auditor to gather wide variety of information
2. Questionnaires can be used to obtain information
3. Auditor may review documentation of control policies and procedures

- *Those relate to evidence gathering*

1. Observation of operation of controls can be a reliable source of evidence
2. Inspection of approvals enables the auditor with evidence that management is performing appropriate control checks

- *Those relate to system*

1. Analysis of system information through specialized software
2. Data review and analysis of output of application processing provides for accuracy of processing
3. Re-performance of the control to test the effectiveness of controls through use of test data

After obtaining results of audit and testing

- Controls that are not working effectively are potential IS control weakness
- For each potential weakness, auditor should determine whether are specific compensating controls to mitigate the weakness

If the auditor believes that compensating controls adequately mitigate the weakness, he should obtain •evidence for the same and •conclude that control activity is achieved	If auditor believes that compensating controls are not adequately mitigating the weakness and the potential weakness is actual weakness, than •the auditor evaluates is effects on IS control in reporting phase

Documentation of Testing Phase

- It includes
  - Understanding of information systems and relevant audit objectives
  - IS Control objectives relevant to audit objectives
  - A description of control technique by level and sub-level used
  - Specific tests performs on them
  - Nature, timing and extent of such test
  - Evidence of effective operation of such control technique
  - Auditor’s conclusion on effectiveness of controls
  - If control is not achieved than determination of compensating control
  - For each weakness, whether there is
    - Material weakness
    - Significant deficiency or
    - Just deficiency
    - Its effect to achieve audit objectives

Multiyear Testing Plan

- Used when auditor regularly performs IS control audits
- For system with high risk, auditor should perform annual testing, such multi-year testing is not appropriate in all situations
- Different controls are comprehensively tested each year
- **It covers relevant**
  - key applications,
  - systems and
  - processing centres
- They should cover a period of not more than three years
- **They should include**
  - schedule,
  - scope of assessment and
  - rationale for planned approach

- It allows auditor to test computer related general controls and business process application controls **on risk basis rather on year to year basis**

- **They help to assure**
  - All systems and locations are considered in evaluation process
  - Relative audit risk and prioritization of system is covered
  - Will provide sufficient evidence to support IS Control effectiveness

Reporting

- Auditor summarizes the results of audit
- Auditor draws conclusions on IS Control weakness (individual and aggregate)
  - on audit risk and
  - on audit objectives
- For each critical element, auditor should make a summary determination as to effectiveness of controls
- Auditor evaluates
  - Audit objectives
  - IS Control weakness (individual and aggregate)
  - Potential control dependencies
  - Conclusions drawn
  - The effect of weakness on entity's ability to achieve critical elements
  - The effect of weakness on entity's ability on risk of unauthorized access to key system

Continuous/Concurrent Audit

- If errors can be detected and corrected at
  - the point of occurrence or
  - closet to the point of occurrence,

  the impact thereof would be least
- Therefore continuous auditing enables auditor to significantly reduce the time between
  - occurrence of client's events and
  - auditor's assurance service thereon

- It enables auditors to shift their focus from
  - traditional 'transaction' audit to
  - audit of 'systems and operations

- They use two bases for collecting audit evidence

1. Use of embedded modules in the system
2. Special audit records

Continuous/Concurrent Audit

- **Potential Benefits**

1. **Reduces the cost of**
    1. basic audit assignment and
    2. time and cost spend on manual examination
2. **Allows the auditor to focus more on**
    1. understanding the client's business and
    2. its internal control
3. **Enables the auditor to test larger samples of client's transaction**
4. **Helps to**
    1. examine data
        1. faster and
        2. more efficiently
    2. perform test throughout the year by specifying transaction selection criteria
5. **Increases the quality of audit**

- **Advantages**

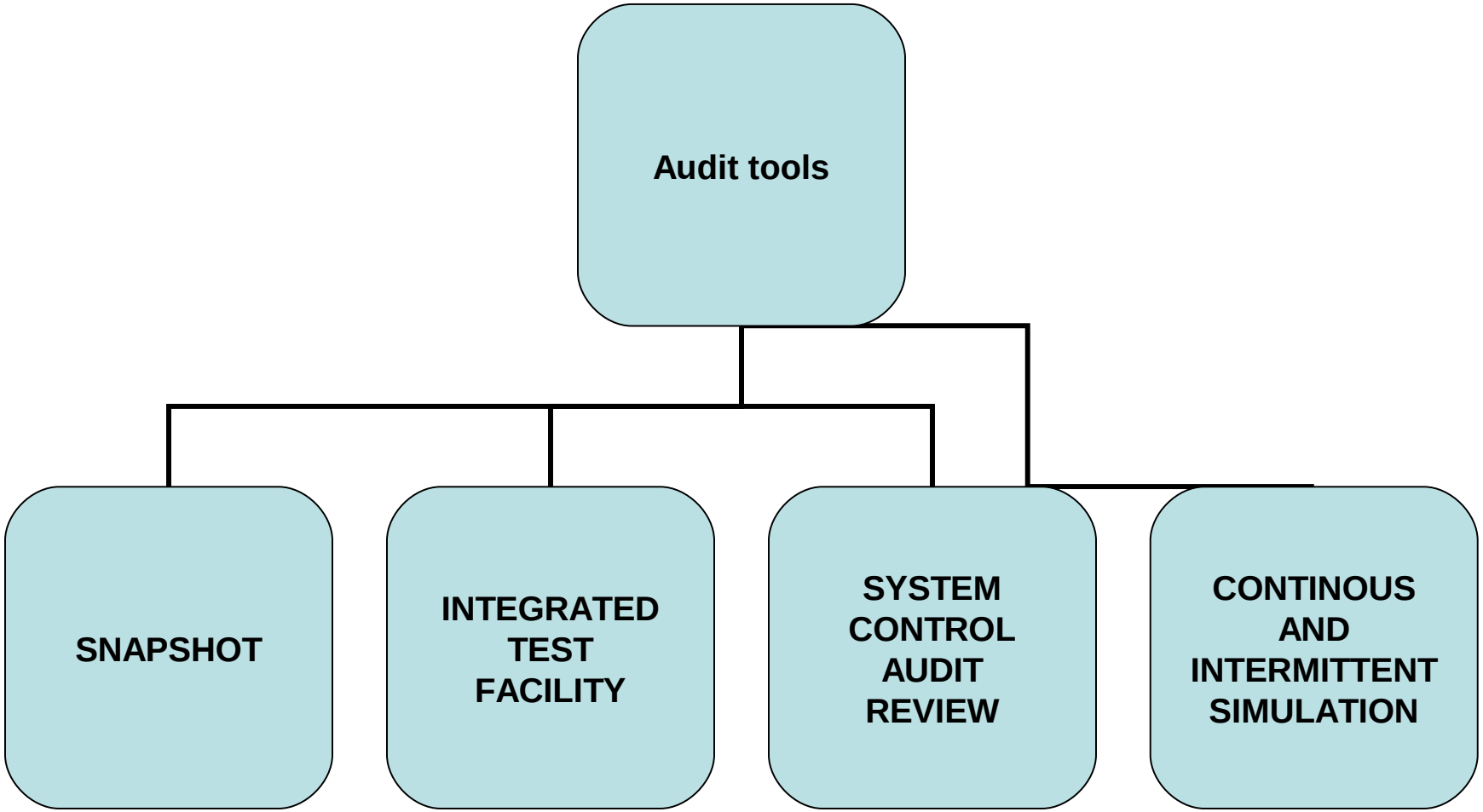
1. Processing can be evaluated and analyzed rather than examining inputs and output only
2. Evidence will be available more timely and in comprehensive manner
3. Auditor gets evidence without the system staff and the users are aware that evidence is being collected
4. It provides system staff a test vehicle to evaluate whether systems meets its objectives
5. Users can submit data to application and obtain feedback on errors

Continuous/Concurrent Audit

- Disadvantages

1. Auditor should be able to obtain the resources
2. Auditors need to have the knowledge and experience
3. More likely to be used if auditors are involved in the development work of system
4. More likely to be used where the audit trail is less visible
5. More likely to be used where the cost of errors and irregularities are high
6. Unlikely to be effective unless they are implemented in a relatively stable application system

Continuous/Concurrent Audit



Audit tools - Snapshot

- It is a software
- It is built into the system
  - at the point where material processing occurs
- It takes the images of the flow of transaction
  - as it moves through application
- The can be uses to assess
  - authenticity,
  - accuracy,
  - completeness of processing

- Main areas to dwell are

1. Locate the
   - snapshot point based on materiality
1. Time
   - when snapshot will be captured
1. Design of
   - reporting system

Audit tools – Integrated Test Facility

- **It is creation of**
  - Dummy entity in application system and
  - Processing of audit test data against the entity
- **It is used as a means to verify**
  - authenticity,
  - accuracy,
  - completeness of

  Processing
- **The auditor has to decide**
  - Methods of entering test data
  - Methods of removing the effects of IFT Transactions
- **Methods of entering test data**
  - The transaction to be tested are tagged
  - The application system has to be recognized the tagged transactions
  - They have to be programmed to invoke two updates
    - Application system master file
    - ITF dummy entity
- **Method of removing the effects of ITF Transaction**
  - The application system are programmed to
    - recognize ITF transaction and
    - to ignore them in terms of processing that affect users
  - Another method of removal of effects is
    - by submitting additional inputs that reverse the effects of ITF transactions

Audit tool – System Control Audit Review File

- It involves
  - embedding audit software modules within host application system
  - to provide continuous monitoring
- The information collected is written onto
  - a special audit file called SCARF
- Auditors can than examine the information
  - to see
  - if some aspect in system needs follow-up

- SCARF can be used to collect information like
  - **Application system errors**
    - Scarf provides independent check on quality of system
  - **Policy and procedural variances**
    - Scarf is used to check the variations
  - **System exception**
    - Scarf is used to monitor different types of application exception
  - **Statistical sample**
    - Scarf provides a convenient way of collecting sample information to use analytical review tools
  - **Profiling data**
    - Scarf can be used to collect data to build profiles of system user
  - **Performance measurement**
    - Scarf can be used for measuring or improving performance of application system

Audit tool – Continuous Intermittent Simulation

- This is a variation to SCARF
- The advantage is that
  - it does not require modifications to application system and
  - yet provides an online auditing capability
- It is used to
  - trap exception
  - whenever
    - Application system uses DBMS
- Execution is done as follows
  - DBMS reads system transaction
  - It is passed to CIS
  - CIS determines if it wants to examine it
  - If yes, next step is performed or else it waits to receive further data from DBMS
  - CIS replicates system processing
  - Every update to database will be checked by CIS to determine discrepancies
  - Exceptions are written in log files