Recent Revisions in the ISCA Course Material

Dear student,

Over the next few pages, I have provided the recently amended chapter-4 content. A sincere effort has been made to cover all the aspects of this revised chapter in easy to understand form. However, some concepts may require further improvements and your suggestions are most welcome in this regard.

Best Wishes for Exams

Chapter-4

Testing General and Automated Controls

What will we study in this chapter?

This chapter has been, almost, completely revised by the Institute in the revised study material of ISCA released in January, 2011. If I summarize the key revisions in this chapter relative to the previous chapter, I will say previously this chapter was having more of software testing content and now as per the name of this chapter this is more focused on testing of controls. So good revisions done! However, we will not study the technical testing of actual controls; we will get an overview on procedural aspects of controls testing.

Let us now understand the key content of this chapter before getting to the detail content of this chapter.

Key Topics of This Chapter:

As the name of this chapter suggests, this chapter primarily explains about the testing of information system (IS) controls. Testing of IS controls is part of information system audit process. With the testing of controls, an auditor provides his/her opinion on adequacy and effectiveness of applied controls: The audit process in this chapter explains about the testing of two types of controls: General and Application Controls. Here general controls means controls applied to system development, data communication and access of IT resources etc; and application controls means controls applied to data processing application for inputs, processing and outputs. However, please note that we are not explained the specific testing (technical aspects), we are explained a simple overview of general and application controls. Additionally, in this chapter, we will learn about complete audit process of controls i.e. audit planning, testing, reporting etc.

We will learn about the following key concepts in this chapter:

Introduction to controls testing and key phases of Audit of Controls

(i) Audit Planning
(ii) Audit Testing
(iii) Audit Reporting

There are some additional topics other than phases of Audit of Controls:

(1) Concurrent or Continuous Audit and Embedded Audit Modules
(2) Hardware Testing
(3) Operating System Review
(4) Network Review

Introduction to Testing and key phases of Audit of Controls:

Testing:

Testing is a scientific method to check the accuracy and effectiveness of any product or process. Here, testing is performed to determine whether the applied controls ensure the information system effectiveness and efficiency. An accurate testing involves understanding about the testing process and expected results i.e. an auditor should have knowledge of testing procedures and what expected results will be there when auditor will perform testing. Testing of entire data or transaction volume is not possible due to time and cost constraints, therefore sampling of data volume is used in adequate quantity and quality to accurately represent entire data volume, and results are extrapolated to represent the complete system.

Tests of controls are audit procedures performed to:

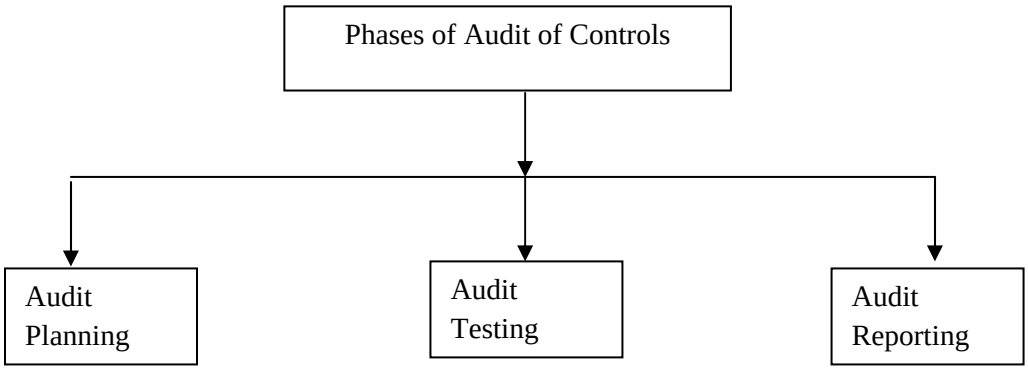
- Evaluate the effectiveness of either the design of internal controls; or,
- Evaluate the effectiveness of operation of internal controls.

Tests of controls directed toward the design of the control focuses on evaluating whether the control is suitably designed to prevent material weaknesses. Tests of controls directed toward the operation of the control focuses on assessing how effectively the control are applied and working to prevent errors and frauds.

Testing of controls can either be performed by using selected test data or it can be performed by using audit tools. Testing of controls can be done by using systematic procedures known as "Phases of Audit of Controls"

Phases of Audit of Controls:

The audit of information system controls includes the following three phases:



(1) Planning: This is the first phase of the Information System controls audit. In this phase, the auditors plan the effective and efficient methods for conducting the audits to meet objectives of the IS controls audit and the audit report.

(2) Testing: In this phase, auditors test the effectiveness and adequacy of the Information System (IS) controls which are relevant to achieve the audit objectives

(3) Reporting: This phase includes the reporting of audit results. In this phase, auditor concludes on adequacy and effectiveness of the IS controls relevant to audit objectives including and material weaknesses and deficiencies of controls

Audit Planning:

The audit planning is very important phase of audit of controls. This phase includes the activities which help to conduct an effective and efficient audit. Although planning occurs throughout the audit as an iterative process i.e. auditor can change planning based on results obtained during testing phase; it includes the following key activities:

- Obtaining understanding about entity and its operation
- Obtaining understating about internal controls mainly related to information system
- Indentifying the significant issues in audit process
- Assess the various risks for entity operation
- Design the audit procedures
- Plan for timing and extent of audit procedures, etc.

Additionally, in planning the IS controls audit, the auditor uses the concepts of materiality and significance to plan effective and efficient audit procedures. The materiality and significance are the concepts that auditors uses to determine the nature, timing and extent of audit procedures. The key theme of these concepts is that auditor is not required to spend resources on the audit of controls areas which have little importance for the audit judgment and objectives i.e. areas which are not material and significant.

Audit Testing:

Auditor should devise a testing plan and testing methodology to determine the effectiveness of controls. For example:

- Auditor can use mix of manual and automated methods to test the controls.
- In the testing of controls, the auditor primarily performs tests for general and application controls.

- Auditor should use both valid and invalid tests data for testing i.e. valid test data should be accepted and invalid test data should not be accepted, as expected test results by system.
- Auditor should also determine the intensity and extent of testing based on the sensitivity and importance of controls to the application and system.
- Auditor should not spend too much time on testing of all the controls and should limit his/her tests to those controls which cover most of the key risks, exposures and error types i.e. auditor should test critical controls and processes.
- Auditor can use review of evidence, interview, personal observations and data tests as testing approach.
- Auditor can select the Generalized Audit Software (GAS) packages such as IDEA, ACL, EXCEL and MS-Access to do sampling, data extraction, testing and summarizing of results.

The audit testing involves the following activities and tests for the IS controls:

(1) Understanding the IS controls Audit Process:

This involves the following aspects

- Obtaining an understanding of an entity operation and its key business processes
- Obtaining a general understanding of entity's network
- Indentifying key areas of audit interest
- Assessing IT risks on primary basis
- Indentifying critical controls
- Obtaining an understanding of controls

If the IS controls audit is performed as part of financial audit, the auditor needs to obtain understanding of controls over financial reporting and needs to evaluate the ***design of controls relevant to an audit of financial statements.*** Auditor also needs to determine whether the controls have been properly implemented.

If the IS controls audit is performed as part of performance audit, auditors should then evaluate ***deign and operating effectiveness*** of such controls. This evaluation includes those controls which impact effectiveness and reliability of information system.

Finally, the IS auditor also needs to determine which audit procedures are required to obtain sufficient and appropriate evidences to support audit findings and conclusions.

(2) Indentifying Key Areas of Audit Interests:

It is very important that auditor should determine key areas of audit interests which are critical to achieve audit objectives. For financial audit, these areas may include key financial applications

and related input/output systems. For a performance audit, it would include areas that are likely to be significant for operation and reliability like access controls etc. For each area and supporting system auditor should develop appropriate documentation, including:

- Operational Location
- Related hardware and software (like firewall, server and operating system)
- Prior audit problems

By identifying key areas the auditor can focus more on these areas and can spend less time on other work and areas. The auditor may review / collect / document the following information for understanding the key areas of audit interests and related systems:

- Identification of entity wide and system levels controls
- Identification of business process level controls

We will understand these in the next topic

- Any internal or third party information system review and audit tests etc performed last year
- Status of prior years audit findings
- Documentation of any computer security related incidents
- Documentation of security plans
- Review of any system certification like ISO 27001
- Review of documentation of BCP or DRP
- Outsourcing services used by organization
- Audit resources planned by organization
- Any multiyears testing plans
- Audit plan that adequately describe the audit objectives, scope and methodologies
- Auditor plans to use the work of others

(3) Performing Information System Controls Review:

In this step, the auditor review the IS controls relevant to audit. With this review, the auditor determines the different controls at the following levels:

- **Entity wide or Component Level (General Controls):** Entity-Level Controls are internal controls that help to ensure that management directives pertaining to the entire entity are carried out. The controls at entity wide level are for those activities or processes which are designed to achieve the control objectives of entire organization. For example, a company has an entity wide policy and procedure for condition of connection, access of IT system, use of internet etc. The weaknesses in the entity wide controls can be the main reason of inconsistent controls i.e. IS controls are not applied consistently across organization.

- **System Level (General Controls):**
  These controls are more specific than those at entity wide level and are generally related to a single technology. There are three main sub-levels at this level which auditor should assess:
  - **Network Controls**: A network is connection of various computers and devices established for sharing of information and resources. There should be adequate controls to protect the network resources from unauthorized use
  - **Operating System Controls:** Operating system is considered as a gateway for access and use of computer resources. It provides an interface to user for working on computer. Therefore, adequate controls should be there at operating system level to provide access of computers and resources to authorized users only.
  - **Infrastructure Applications Controls:** These represent those applications which are used for day-to-day computer operation such as emails, web browsers and database application. The adequate controls should be there to avoid the misuse of these applications.

  Primarily above system level controls include the configuration management i.e. network, operating system and infrastructure applications should be installed and used as per the configuration recommended by their suppliers or as per the best practices available for these in markets.

- **Business Process Application Level:**
  Here, business process application means those applications which are used for data processing tasks e.g. Tally, Railway Reservation, Banking Application etc.

  The controls at business process application level contain specific procedures and rules to ensure correct and efficient use of business applications. Additionally, the controls at this level ensure that correct inputs, processing and outputs are used for application.

The entity wide controls are mainly applicable at all the three levels i.e. at entity wide, system and business process levels. For example:

- Security Management Controls
- Access Controls
- Segregation of Duties
- Configuration Management
- Contingency Planning

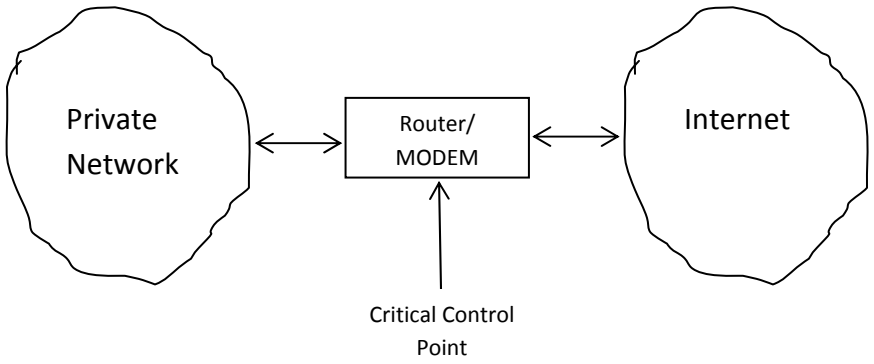
	Controls Types	Entity Wide Level	System Level			Business Process Application Level
			Network	Operating System	Infrastructure application / utility	
General Controls	Security Management	→	→	→	→	→
	Access Controls	→	→	→	→	→
	Configuration Management	→	→	→	→	→
	Contingency Planning	→	→	→	→	→
	Segregation of Duties	→	→	→	→	→
Application Controls	Inputs, Processing and Outputs					→
	Interfaces					→
	Data Management					→

→ *Levels at which controls are Applicable*

Categories of Controls

(4) Testing Critical Control Points:

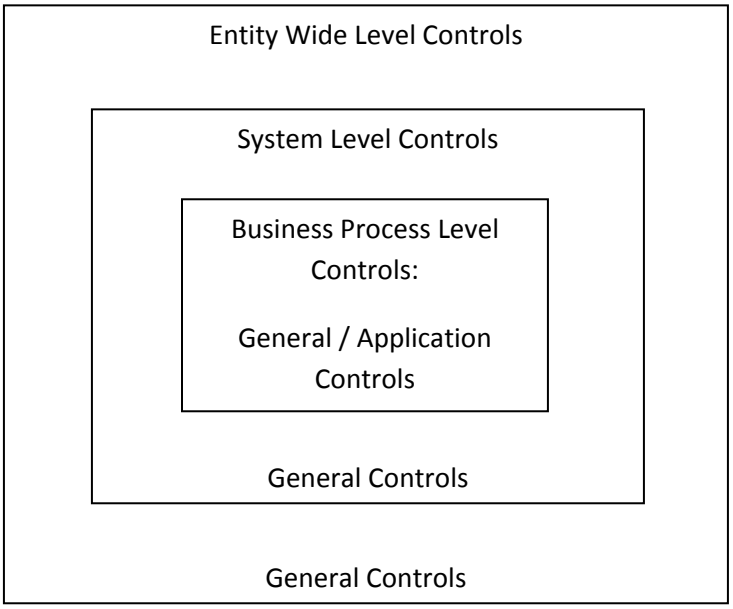
There may be certain critical controls points in the Information system which auditor should evaluate in all aspects. For example, Router or MODEM can be a critical control point for an Information System. Therefore, these should be tested in all aspects i.e. at individual component level, for its operating system and its network application:



Weaknesses in the critical controls points may expose the entire system for problems. Therefore the auditor should indentify and tests such points' controls appropriately.

(5) Test Effectiveness of Information System Controls:

There should be a systematic approach from the auditor to test the effectiveness of Information System Controls. The auditor should design and conduct tests of controls in such a way that the tests should be able to determine the effectiveness of design and operation of controls. It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with general controls testing at the entity wide level and finally testing application controls at business process levels



Tiers of controls testing:

(6) Tests of General Controls at the Entity wide and System Levels:

In this testing, the auditor tests the general controls applied at entity wide and system levels. The auditor may use combination of procedures for these tests, including observation, enquiry, inspection and use of appropriate test software. Sampling is generally not required for the tests of general controls except in some of those general controls which involve frequent approvals.

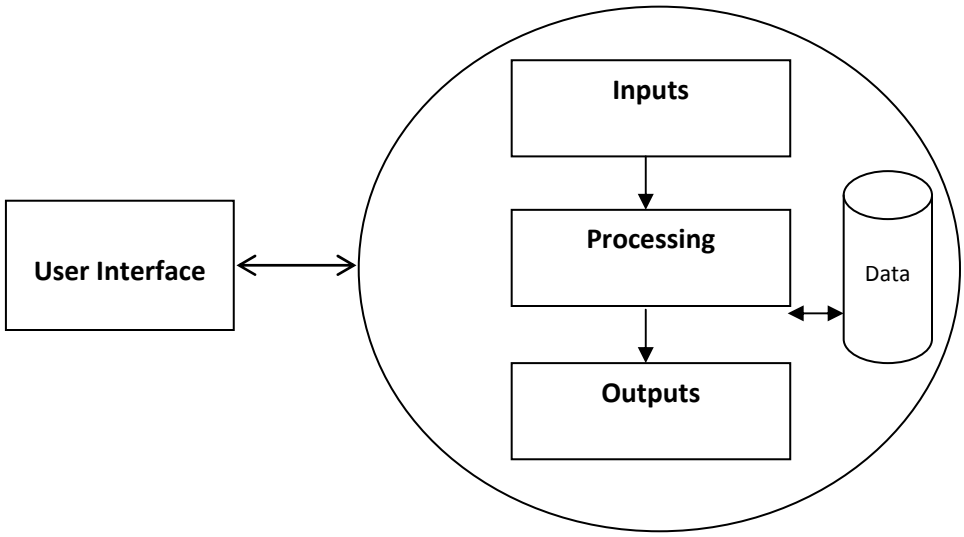
If the controls at entity wide and system levels are not effectively designed and operating, the auditor will generally not find the controls effectiveness at business process levels. If general controls are not designed and operating satisfactorily then auditor should do the following:
(1) Document the types and degree of risks resulting from ineffective general controls
(2) Develop appropriate findings from the tests of IS controls
(3) Provide Recommendation to improve the controls

(7) Tests of General Controls at Business Process Level:

If auditor reaches a favorable conclusion on general controls at the entity wide and system levels controls, the auditor should test the effectiveness of general controls at business process levels. These controls are generally related with the business process application security. The business process application is that application which will have data processing capability and will have the application components for inputs, processing and outputs e.g. tally and banking application.

If the ***general controls*** at business process levels are not effectively designed and operating, the auditor will generally not find the ***application controls*** effectiveness at business process levels.

(8) Tests of Business Process Application Controls and User Controls:



Business Process Application

In this testing of controls, the auditor test controls for user interface, business process i.e. inputs, processing, outputs and data management to determine their effectiveness to ensure an error free and efficient business application. The auditor normally test the business process application when auditor finds the entity wide, system and business process levels general controls are effective in terms of their design and operation.

If auditors find ***the design*** of business process application controls are not effective then the auditor should not test ***the operation*** of application controls for effectiveness. Additionally, if auditors find these controls are not effective then the auditor should determine the risks arising due to ineffectiveness of these controls and should provide findings on the tests of controls with recommendation to improve the effectiveness of these controls.

(9) Appropriateness of Control Tests:

Testing is an endless process i.e. the auditor cannot say with certainty that all aspects of a particular system have been tested. However, for concluding on operating effectiveness of the IS controls, the auditor can perform the best of audit procedures to obtain sufficient and appropriate evidence to support his/her conclusions. For example:

- Personal observation and testing for operation of controls: e.g. the auditor can personally verify the password controls by using combination of passwords to tests their effectiveness.
- Review of controls' documentation: to understand design and applicability of controls
- Inspection and verifications of approvals processes to check that the management is performing appropriate checks.
- Analysis of system configuration i.e. checking configuration setting of components and access control lists
- Review of data and processing outputs: this provides evidence that system processing is accurate
- Use of CAAT to tests application processing accuracy and efficiency
- Use of test data with correct and incorrect data values to check that system should accept the correct data for processing and should reject the incorrect data for processing
- Interviews with IT users and management to gather information on operating effectiveness of IT systems
- Questionnaire can be designed to obtain information from IT users and management for controls effectiveness

Based on the results from above audit procedures, the auditor should determine whether the controls are operating effectively. If controls are not operating effectively then reasons for ineffectiveness should be determined i.e. design weaknesses or operating weaknesses are the reasons. For each potential weakness, the auditor can also determine whether there are

appropriate compensatory controls or other factors that can mitigate the weakness and can help to achieve the audit objectives.

Auditor can communicate the findings on above aspects with recommendations to achieve the effectiveness of controls.

(10) Multiyear Testing Plans:

This type of testing plan is used when auditor regularly perform the IS controls audit; for example, annual financial audits. In this type of audit, the auditor can prepare a multiyear audit plan, and such plan covers the organization key relevant applications, systems and processing centers for audit on multi-years basis. But such audit plan should not cover audit aspects for more than the three years period and should include schedule and scope of IS audit during this period and should also include a rational for this approach.

The auditor typically reviews these plans on annual basis and adjusts them as per the results of prior audits, and for significant changes in the IT environment and for implemented new systems.

Benefits of Multiyears testing plan:

Multiyears audit plan is a long-term plan and it includes the following benefits:

- All systems and locations can be appropriately considered for audit
- Help to prioritize the audit time and resources based on system risks.
- Help to reduce annual audit resources use and cost
- Can plan to conduct comprehensive tests for significant business process applications by dividing audit process on multiyears basis.

However, multiyears testing plans are not suitable in all situations. For example, they are not appropriate for the first time audit where some significant business process applications or general controls have not been tested in the recent past period. Additionally, it is not applicable for organizations which do not have strong entity wide controls. Also, using by this plan, the auditor conducts some limited tests and activities annually for those controls for which full comprehensive testing is not selected.

(11) Documentation of Controls Testing:

The following documents can be developed by auditors for the information developed/collected during the testing phase.

- An understanding of the information system components that is relevant to the audit objectives.
- IS controls objectives

- Description of control techniques used by level and sub-levels i.e. entity wide, system and business process levels, and network, operating system and application sub-levels.
- Description of tests performed by levels and sub-levels
- Description of tests in terms of timing, nature and extent of tests
- Description of evidences of controls in terms of their effectiveness or ineffectiveness
- Description about any compensating controls which help to achieve control objectives when direct IS controls are not able to achieve the desired control objectives.
- Commenting of auditor on weakness i.e. weakness is immaterial, material or there is significant deficiency

Audit Reporting:

After the testing phase the auditor prepare the following as a part of audit reporting phase:
(i) Summarizes the audit results
(ii) Draws conclusions on individual and aggregates effect of identified IS control weaknesses on audit objectives
(iii) Reports the results of audit.

Audit report is an end product of audit of controls and it should be systematic organized to communicate all aspects of audit.

Audit reporting includes the following key aspects:

(1) Audit Objectives:

In this auditor lists the objectives of IS controls testing or audit. The auditor lists the audit objectives with the relevant controls i.e. the controls which are to be tested. For each relevant control, the auditor determines whether the control is suitably designed and implemented.

(2) Reporting of Audit Results:

The auditor reports the audit results in terms of:

- Evaluation of controls for effectiveness (and weaknesses)
- Financial audits and performance audits
- Other audit reporting requirements and related reporting responsibilities

(3) Substantive Testing:

Where controls are determined as not effective there substantive testing may be required to determine the whether there is material issue with resulting information. In an information system audit, substantive testing is performed to determine the accuracy of information generated by a process or application. Audit tests are designed and conducted to verify the functional accuracy and efficiency of controls. It is important to list the types of tests performed for checking the effectiveness of controls and accuracy of information produced. Auditor can select the computerized tools to conduct the tests.

(4) Documenting the results

This includes the appropriate reporting of audit findings, analysis, conclusions and recommendations.

(I) Audit Findings:

Audit findings should be formally documented and should include the controls audited and results of test of controls with recommendations.

- An audit finding serves the purpose of documenting controls objectives and communicating strengths and weaknesses of controls.
- It can be used to review the issues with IT managers to take the corrective actions.
- The information on audit findings can then be used to prepare the formal audit report including corrective actions and follow-up

(II) Audit Analysis:

At the time of preparation of audit report, it is important that there should be an adequate analysis of data collected during testing phase for inclusions into audit report. For example, test data and test results, data complied during interviews and observations processes etc should be analyzed to prepare a quality report. If due analysis is not done then audit report may have low quality content with a classic case of Garbage in Garbage out i.e. low quality data will provide low quality report.

Further, a complete and timely analysis of tests data and results is very important to write a good audit report.

Complete analysis includes a clear understanding of the standards (best practices) of controls and causes of the deviation or weaknesses that led to deviation. A complete analysis also provides the risks involved, in terms of materiality and exposure, due to deviation of applied controls from their required standards. Additionally, it is important that recommendations based on analysis of results as corrective actions should be included.

Timely analysis helps auditor to determine the causes and exposure of findings early in the audit. This provides auditor time to conduct further tests, if required, and allows auditor to take timely corrective actions.

The audit analysis needs four steps:

- **Re-examine the standards and facts:** This includes analyzing the standards (best practices) and actual facts related to controls.

Standards: these are procedures, operating guidelines, regulation and best practices and other predefined methodologies that define how controls should functions. Using wrong standards could lead to use of inefficient practices. Four situations may occur while evaluating standards:

- No standard exists (this may imply high degree of risks)
- A standard exists but is not formal
- A standard is formal but no longer appropriate (i.e. not cost effective and not necessary)
- A standard is formal and appropriate

Auditor should use the formal and appropriate standards for evaluating the controls.

Facts: Actual values of controls are facts. After evaluating standards the auditor must evaluate the collected facts. Auditor should find the deviations between facts and its standards and should ensure that findings are accurate.

- **Determine the cause of deviation**:

Once the auditor is sure of standard then auditor should indentify the cause of the deviation between facts and standards. Determining the cause helps to indentify the exposures and also helps in formulation the recommendations

- **Determining the Exposure and Materiality of Deviation:**

This step helps to examine the potential consequences of deviations. This provides the material impact of deviation between a standard for control and its actual observed/tested value. This also provides the extent/severity `of risks due to deviation between required and applied controls. Severity of risks also refers to potential amount of loss due to each deviation.

Materiality is a quantitative judgment which indicates whether the frequency and degree of exposure are significant enough for the deviations that these should be corrected and included in the final audit report.

With the understanding of exposure and materiality the auditor can mention about:

- Existing and potential exposure or risks due to deviation
- Significance of deviation in term of money, time, person injury etc
- Existing and potential frequency of deviation i.e. how frequent deviation is observed
- What caused the deviations to occur
- Required methods or measures to control the deviations

Based on above, the auditor will have sufficient data to make an informed decision about the state of controls and efficiency of their operation.

- **Determine possible recommendation for corrective actions**

This is the last step of the Audit Analysis. This includes determining the possible recommendations for correction of deviations.

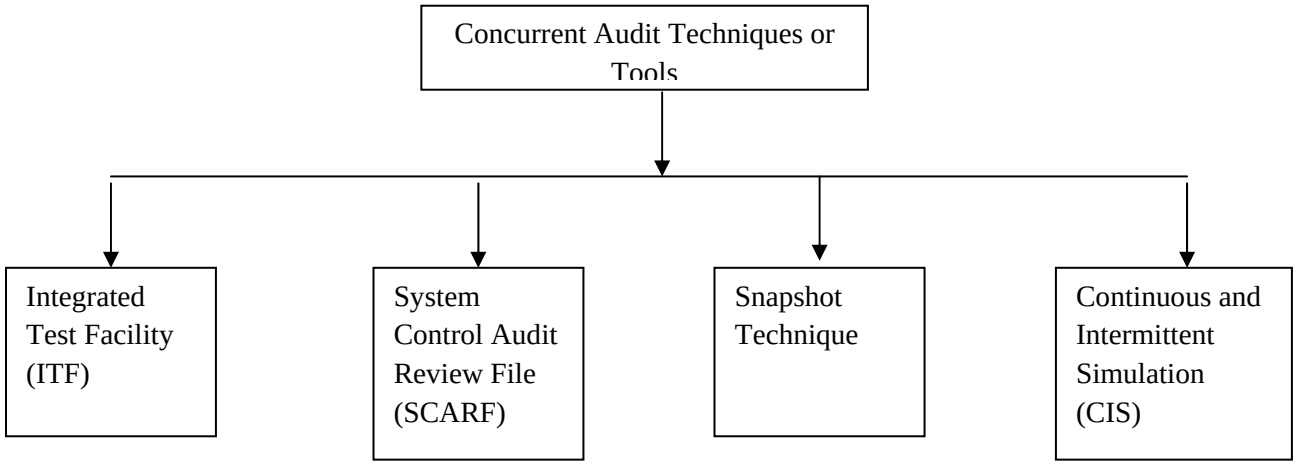
(III) Audit Conclusion:

Conclusion includes the auditor opinion, based on above documented evidences, whether an audit area meets the audit objectives or not. An auditor should provide audit conclusion based on factual data obtained and based on audit activities which auditor performed during the audit assignment. The conclusions should be supported by proper evidences.

Concurrent or Continuous and Embedded Audit Modules:

In online system normally transaction are processed without the use of source voucher. In such cases evidence gathered after data processing is insufficient for audit purposes. And in online systems transactions are happened continuously and in sequence, it is difficult or impossible to stop system in order to perform audit tests.

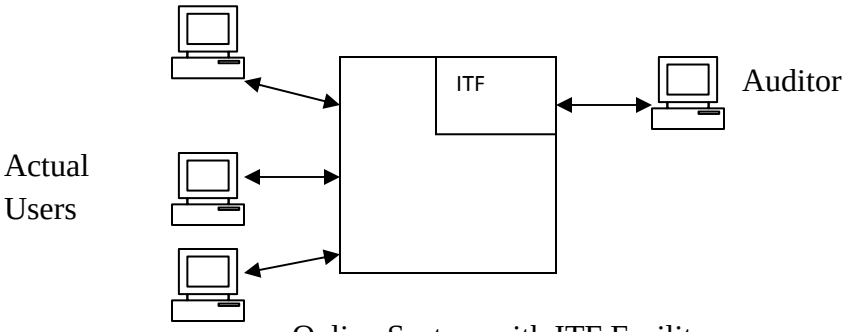
Thus, the auditor uses concurrent audit techniques to continuously monitor the system and collect audit evidence while live data are processed during regular operating hours. Concurrent Audit techniques uses embedded audit modules, which are segments of program code that perform audit functions. These programs also report results to auditors and store the collected evidence, for auditor's review. Though concurrent audit techniques are time consuming and difficult to develop, but once implemented these save lots of time and are also less complicated for audit.



An Integrated Test Facility:

In this technique, an embedded audit module known as ITF is used in the information system to be audited. This technique allows auditor to open a dummy A/c or branch in the information system with the help of ITF audit module. And, the auditor enters the test (dummy) transactions to this dummy A/c or branch and reviews the processing and outputs of these transactions for correctness (with expected results). The dummy records entered by auditor for testing purpose do not affect the actual records in the system.

Because dummy and actual records are processed together, company employees usually remain unaware that such testing or auditing is taking place. The auditor compares the processed and expected results to verify that the system and its controls are operating correctly.



Online System with ITF Facility

This technique is mainly used in online system, and in this test transactions can be submitted with actual transactions on frequent basis without disrupting the regular processing operation.

The best part of ITF is automatic removal of dummy transactions impact from the working/client system. This is possible due to appropriate programming of the following:

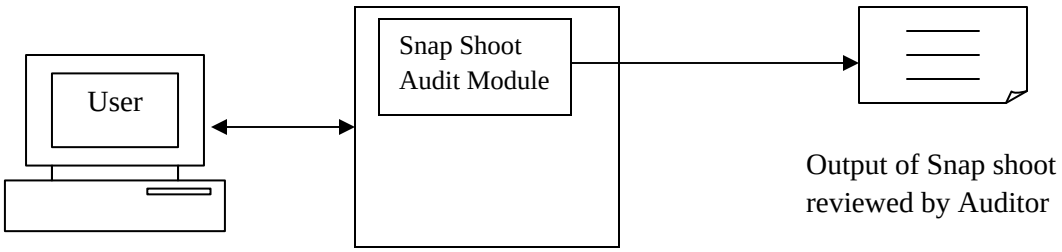
(1) Method of Entering Test Data: the dummy transactions or tests transactions are tagged separately or provided the unique identifications different from the actual transactions. Thus the test transactions are processed with the client applications just like actual transactions but they don't get mixed up with the actual data being processed by the system users. This is possible with appropriate programming of ITF audit module.

(2) Methods of removing the effects of ITF transactions: The impact of ITF transactions from the system must be removed after the testing. The client application system is programmed in such a way that it ignores the impact of the test/dummy transactions and removes the test transactions automatically. However, in the ITF modules where automatic removal facilities are not there than auditor need to remove the transactions manually.

The Snapshot Technique:

In this technique, the audit software take pictures of the transactions as transactions flow through an application system. In this, the auditor embeds the audit software at those points where they think that material processing is occurring. To validate processing at various snapshot points, both before-processing and after-processing images of the transactions are captured. The auditor can assess the authenticity, accuracy and completeness of the processing carried out on the transaction by checking the before-processing and after-processing images of transactions. However the auditor has to take decision regarding the location of snapshot points, time of capturing snapshots and reporting of the snapshot data captured.

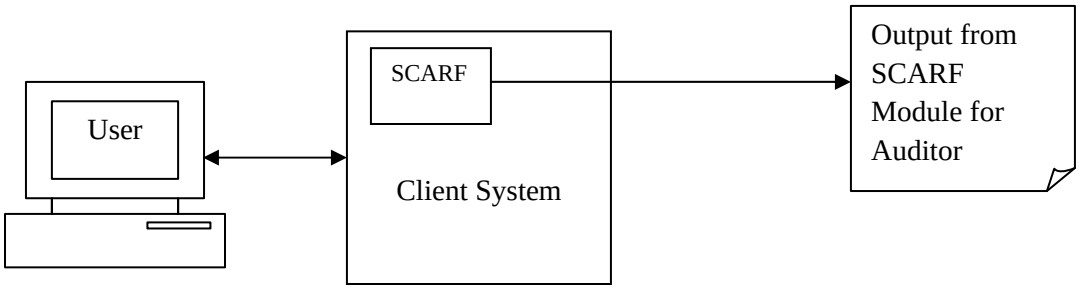
All the snapshot data related to a transaction can be collected in records at one place thereby facilitating efficient audit evaluation work.



SCARF: System Control Audit Review File:

This is also like Snapshot technique but in this technique an embedded audit module is used to continuously monitor transactions and collect data on transactions with special audit significance. In this technique, audit significant data/facts are recorded in a SCARF file or Audit Log. Only those transactions are recorded in a SCARF file that are of special audit significance such as transactions exceeding a specified limit or transactions related to inactive accounts, etc. Periodically the auditor receives a printout of the SCARF file, examines the information to identify any questionable transactions, and perform any necessary follow-up investigation.

This technique is considered as one of the most complex techniques of online auditing. It involves embedded audit software modules within the host application system to provide continuous monitoring of system's transactions. These audit modules are placed at predetermined points to gather information about transactions the auditor considers as material information. The information collected is written onto a special audit file, the SCARF master file, which the auditor examines for audit purposes. The two important decisions which the auditor needs to take while using this technique are: what information to be collected and the reporting system to be used.

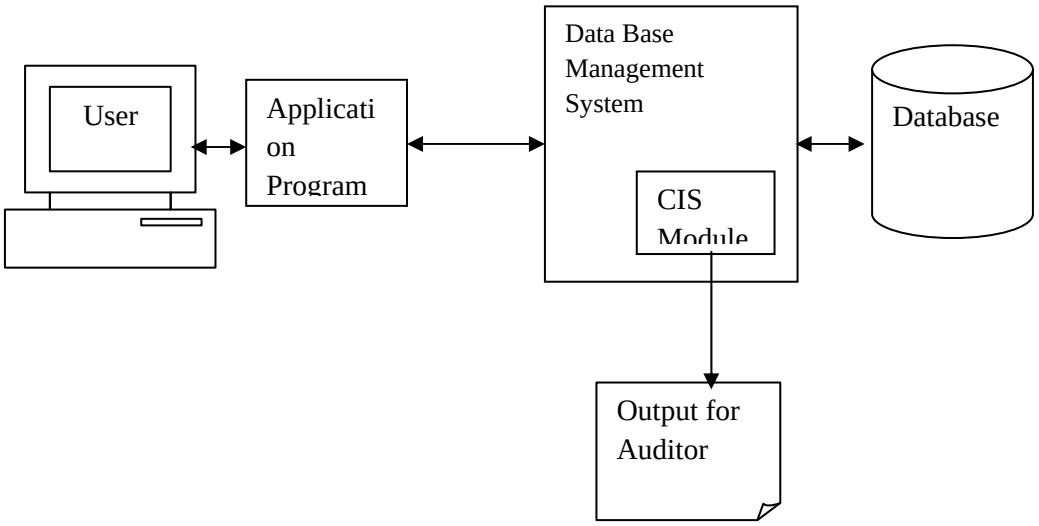


Auditor can use the SCARF technique to collect the different types of information:

- Application system errors:
- Policy and procedural variances
- System exception e.g. values out of standard range
- Statistical sampling: SCARF outputs act as samples
- Profile data e.g. information about system users activities
- Performance measurements information

Continuous and Intermittent Simulation (CIS):

This technique embeds an audit module in a Data Base Management Systems.



This technique is a variation of SCARF method; this can be used when application system uses database management system. This method uses the database management system to trap exceptions that are of interest to the auditors. First, a transaction is selected which has significance for audit by using some sampling method. The database management system provides CIS all the procedures and data required by the application system to process the selected transaction. CIS now process the transaction by replicating the application system processing by way of parallel simulation. Every update to the database that arises from the processing of the selected transaction will be checked by CIS to determine whether discrepancies exist between the results produced by the two methods i.e. by application and CIS module. Exceptions identified are then written to a log file like SCARF for subsequent investigation.

Advantages and Disadvantages of Concurrent Auditing Techniques:

Advantages:

Some of the advantages of concurrent audit techniques are as under:

- **Timely Audit:** helps to conduct audit in timely manner,

- **Comprehensive and detailed auditing** – Audit can be performed in a more comprehensive manner I in comparison to manual audit, and the entire processing can be evaluated and analysed rather than examining the some inputs and the outputs only.

- **Surprise test capability** - Auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

- **Assess whether Information system meets the set objectives** – This technique is used as a vehicle to inform system staff whether the information system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

- **Training for new users** – Techniques like ITFs can be used to provide training to new users who can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports without effecting the actual system working

Disadvantages:

The following are some of the disadvantages and limitations of the use of the concurrent audit system.

- **Availability of Resources:** Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of concurrent audit techniques.

- **Involvement in system development:** Concurrent or continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.

- **Expert knowledge of information system working:** Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.

- **Missing Audit Trail:** Concurrent or continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.

- **Stable Application System:** Concurrent audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

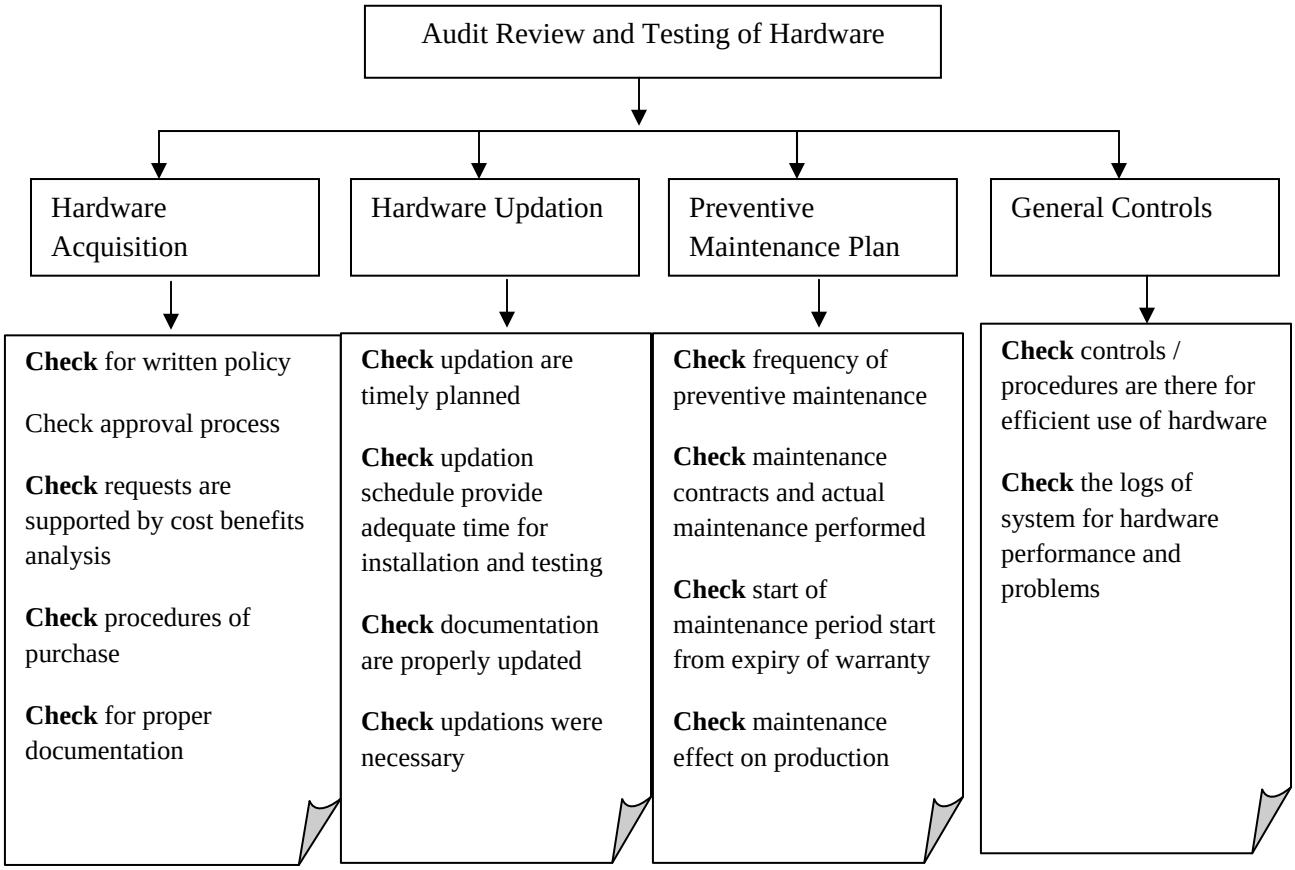
Hardware Testing and Review:

Hardware testing and review is also a very important part of information system evaluation and auditing. Hardware testing and review should be performed as per the specifications mentioned in requirement specifications documents, but for worst possible scenarios.
Normally, hardware should be tested for followings:

- Performance
- Memory capacity
- Security
- Reliability
- Error handling / exit testing
- Nos. of users supported simultaneously
- Maintenance Support
- Accessibility testing

The auditor should review and audit the procedures for followings hardware related tasks:

- Hardware Acquisition
- Hardware Updation
- Preventive Maintenance Plan
- General controls used for efficient and reliable working of hardware.



Operating System Review:

In this auditor review the procurement, implementation, execution and maintenance of system software such as operating system in terms of;

- Review the approval process of software selection
- Review cost /benefit analysis of system software procurement
- Review controls over the installation of system software
- Review systems documentation specifically in the areas of:
  - Operating documents
  - Maintenance documents
  - Users instructions, etc
- Review and test systems software implementation to determine adequacy of controls in:
  - Authorization procedures
  - Access security features
  - Documentation requirements
  - Documentation of system testing
  - Audit trails
- Review system software security procedures, etc

Reviewing of Network:

Network such as LAN and WAN are important resource of organization and these helps to provide an efficient working environment in the organization. Some organizations such as banks and telecom cannot function if their network is not operational, therefore review and testing of network is an essential audit requirement of IS audit in such organizations.

Network Audit Objectives:

The audit of network or LANs, etc is done to ensure:

- standards are in place for designing and selecting a LAN architecture,
- controls are there to ensure continuous working of LAN, and
- for ensuring that the costs of procuring and operating the LAN do not exceed the benefits.

Prerequisites from Auditor for Network Audit

The reviewer or auditor of network should have knowledge about followings;

- LAN components (such as servers, modems, routers, and communication channels)
- Network topology (such as STAR, MESH, etc) and LAN configuration in terms of interconnections to other LANs, WANs or public networks
- LAN technicalities like communication or traffic types
- LAN uses and applications i.e. main applications used over the network.
- Authorized user groups of LAN

Review and Test of Controls in Network Audit

The auditor review, test and validate the following controls for network:

- Physical Controls
- Logical Controls and
- Environment Controls

The review and test of above controls are similar to audit of Physical Access Controls, Logical Access Controls and Environment Controls discussed in the previous chapters

Test of Physical Controls

This includes inspections and observations of LAN from security point of view and auditor check that followings are with proper controls:

- LAN wiring / cabling/ telecommunication links
- Server / main-computer access
- Workstations access
- LAN documentations access
- LAN components access
- Server room access (primarily restricted to administrator)
- Server room remain properly locked and keys are used in controlled manner
- Backup diskettes and tapes access
- UPS working
- Server protection from electric surge

Test of Logical Controls

To test logical security, auditor should interview the person responsible for maintaining LAN security to ensure that followings logical controls are working properly.

- Login-id password
- Access controls (access of applications and programs)
- Data encryption
- Firewall
- Network Monitoring, etc

Test of Environment Controls

To test environmental controls, auditor should visit 1he LAN server facility and verify:

- Temperature and humidity are adequate.
- Electric surge protectors are in place.
- Facilities are protected from fire by having properly protected power cables
- Fire extinguishers are placed at correct locations.
- Fire alarm and smoke detectors are working properly
- LAN file server facilities are protected from water damage/flood.
- Storage methods and media for backup are protected from pollution / fire / water damage.
- A LAN workstation should be disabled automatically after a short period of inactivity.
- Communication links connected to the outside should be in duplicate form.

Review Questions:

Q.1: Describe Various Phases of IS Audit

Q.2: An Auditor indentifies control techniques and determines the effectiveness of controls at various levels. Explain those levels in breif

Q.3: Briefly explain the components that an auditor should document in the testing phase:

Q.4: Write a short note on Audit Tool?

Hint: GAS (Generalized Audit Software) like IDEA, ACL, EXCEL and MS-Access
Embedded Audit Modules like SCARF, ITF, SNAPSHOT and CIS

Q.5: What are the advantages and disadvantages of continuous auditing?

Q.6 Describe in short the review methodology for hardware?

Q.7 What are the various kinds of hardware testing?

Q.8 How would an operating system review be performed?

Q.8 Testing the LAN and its environment is a vital part of IS Audit? Give an overview of the procedure to do so?

Revisions in the Chapter-8

Some revisions have been done in the chapter-8. Most of the revisions are not significant except replacing audit standard AAS29 with SA 315 and SA330. Please read these audit standards, i.e. SA 315 and SA 330, from the audit subject course material.