PAPER 6

CA FINAL

INFORMATION SYSTEMS CONTROL AND AUDIT

PREPARED BY:

CA AKHIL MITTAL
ACA, B.COM (H) [SRCC]
E-MAIL ID: caakhil24.srcc@gmail.com

CHAPTER 4 (AS PER ICAI MODULE)
TESTING – GENERAL AND AUTOMATED CONTROLS

I. BASICS OF TESTING:

1.) Meaning of the TESTING→

It is a systematic process performed to determine whether the controls ensure the system design is effective.

2.) Methods of TESTING→

SUBSTANTIVE TESTING	COMPLIANCE TESTING
↓	↓
Used to ensure that **PROCESSES** are working as per **DESIGN OF CONTROL**	Used to ensure that **CONTROLS** are working as designed

II. IS AUDIT CONTROLS AUDIT PROCESSES:

Code to remember: US, CRIC

1.) **U**nderstanding of entity & its operation & key business processes.
2.) **S**tructure of the entity's network to be understood.
3.) **C**ritical area of audit [files, application, systems, locations]
4.) **R**isk assessment on a preliminary basis.
5.) **I**S controls understanding.
6.) **C**ritical controls point to be identified i.e. external points to the networks.

III. IDENTIFYING KEY AREAS OF AUDIT INTEREST & DOCUMENTATION:

The auditor must identify the key areas of audit interest which are critical. The auditor must document relevant to each key area of audit interest.

Code to remember: L-COP

1.) **L**ocation of each system or file.
2.) **C**omponents (significant) of the associated hardware & software.
3.) **O**ther significant systems or system level resources that support areas of audit.
4.) **P**rior audit problems reported.

II. PERFORMING INFORMATION CONTROLS AUDIT TESTS:

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

A.) Entity wide or Component level:

-- Constitutes the processes designed to achieve the control objectives of entire organization.

-- For example: **Company has entity wide processes for access to IT systems, establishment of accountability & responsibilities.**

B.) System Level (General controls):

-- These controls are **specific** & relate to a single type of technology.

-- Manages specific managing system resources.

-- The auditor must assess the further 3 levels:

Code to remember: N.O.I

Network	Operating System	Infrastructure Application
↓	↓	↓
It is an inter-connected system of components	Controls execution of computer programs	These are software that is used to assist in performing system operations

C.) Business Process Application Level:

-- It consists of various **policies and procedures** for controlling **specific business processes.**

-- **For example: That the management ensures that all changes to application systems are fully tested & authorized.**

The auditor should develop more detailed audit steps on the entity's specific software and control techniques, after consulting with the financial/ performance auditor about audit objective & significant areas of the audit interest.

III. TEST EFFECTIVENESS OF INFORMATION SYSYTEM CONTROLS:

If the auditors identifies IS controls for testing, the auditor should evaluate the effectiveness of:

- General controls at the **entitywide and system level;**

The auditor must test general controls through a combination of procedures, including **observations, inquiry and inspection.**

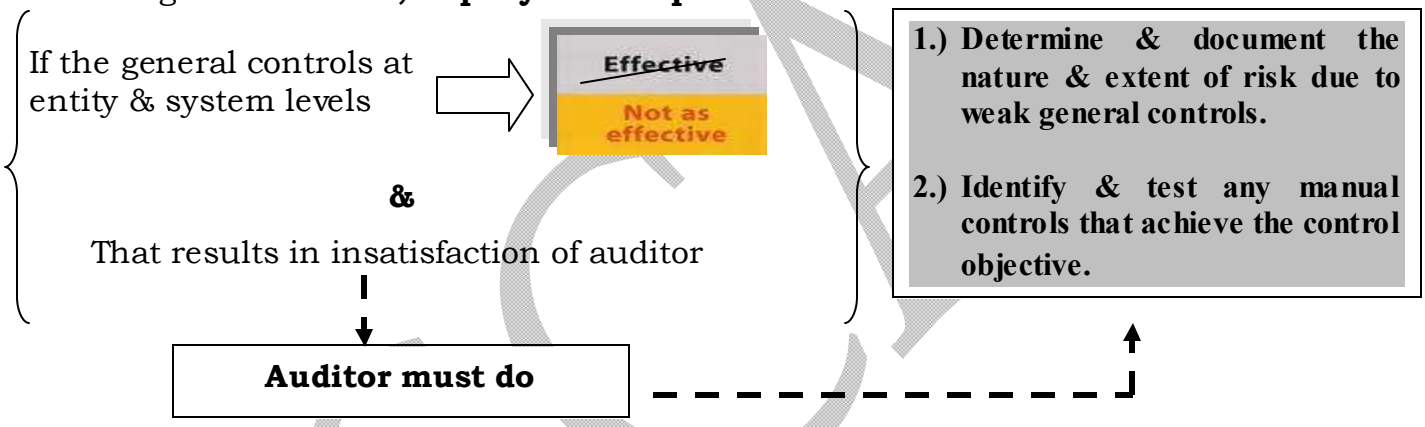


Figure 1

- General controls at the **business process application level and;**

If the auditor reaches a favorable conclusion on general controls at the entity wide & system i.e. **where controls at entity and system level are effective**

The auditor must evaluate & test the effectiveness of general controls

Within which application controls are

To be tested

IV. TEST EFFECTIVENESS OF INFORMATION SYSYTEM CONTROLS:

Audit procedure to be performed by the auditor to obtain sufficient & appropriate evidence to support their conclusion.

Code to remember: Q-OP-D.I.D

1.) **Q**uestionnaire**: It can be used to obtain information on controls & how they are designed.**

2.) **O**bservations **: It can be reliable source of evidences. For example auditor may observe the verification of edit checks & password controls.**

3.) **P**ersonnel Inquiry**:** Inquiries of IT & management personnel able auditor to gather a wide variety of info. about operating efficiency of control techniques.

4.) **D**ocumentation Review**:** The auditor may review documentation of control policies and the procedures.

5.) **I**nspection of Approvals **:** Through this auditor is able to ascertain that management is performing appropriate control checks.

6.) **D**ata Review & Analysis**:** Auditor through this review & analysis may gather evidences about the accuracy of processing.

V. MULTIYEAR TESTING PLAN:

In case an IS auditor perform audit for various years i.e. **regular audit** then it will be appropriate testing plan. Under this plan auditor covers **key applications, systems and processing centres.**

FEATURES OF MULTIYEAR TESTING PLANS:

- This plan should not cover period of more than 3 years.
- Should include schedule & scope of assessment to be performed.

BENEFITS OF MULTIYEAR TESTING PLANS:

Code to remember: PARA

- **P**lans to conduct the comprehensive tests for significant business process applications by dividing audit process on multiyear basis.
- **A**gency system & locations are considered in IS control evaluation processes.
- **R**elative risk is considered & prioritize the audit time.
- **A**nnual audit resources & cost is reduced.

LIMITATIONS OF MULTIYEAR TESTING PLANS:

Code to remember: C.A.T

- Not applicable to those organization which don't have strong entity wide **C**ontrols.
- Not suitable for First time **A**udit. It is so because it might be possible that some critical business process applications or general controls have not been tested in the recent past years.
- **T**ests which are being used by the auditor are limited.

VI. DOCUMENTATION OF CONTROL TESTING PHASE:

Information developed in the testing phase that the auditor should document includes the following:

- **Understanding of the INFORMATION SYSYTEM** that is relevant to audit objective.
- **IS control objectives & activities** relevant to audit objective.
- **Description of the control techniques** used by the entity to achieve IS objective & activities.
- **Specific tests** performed at level & sublevel.
- Related a document that describes the **nature, timing & extent of the tests.**
- **Evidences of effective operation of** control technique or lack thereof.
- **Compensation controls** if the controls are not achieved.
- **Auditor's conclusion** about the effectiveness of the entity's IS control in achieving the control objectives.

- **For each weakness,** whether the weakness is material or not. It's cause & effect if necessary to achieve the audit objective.

VII. AUDIT REPORTING:

After completing the testing phase, the next phase is **AUDIT REPORTING.** Here audit phase means:

- The auditor **summarizes** the results of the audit.
- Draw conclusions on individual & aggregate effect of all identified IS control weaknesses on audit objectives.
- Report the results of the audit.

Auditor must evaluate the potential impact of any identical weaknesses on the completeness, accuracy, validity & confidentially of application data relevant to the audit objectives.

Following are the aspects covered under the audit reporting:

Code to remember: O.R.-T.D.

- **O**bjective of Audit:

  -- ***Auditor lists the objectives of IS controls testing or audit***

  -- ***Determines which IS control techniques are relevant to the audit objectives.***

  -- ***Performs test to determine whether such control techniques are operating effectively.***

- **R**eporting of audit results:

  -- ***Evaluate the effects of identified IS control weaknesses.***

  -- ***Financial audits, attestation engagements and performance audit***

  -- ***Consider other audit reporting requirements and related reporting responsibilities.***

- **T**esting (Substantive):

  -- ***It is required to determine whether there is material issue with the resulting financial information.***

  -- ***Substantive testing is used to determine the accuracy of information being generated by a process or application.***

  -- ***The auditor selects and uses computer aided audit tools to gather information & conduct the planned tests.***

- **D**ocumenting Results:

-- ***This is final step which involves the results of the work & preparing a report on findings.***
-- ***The audit results should include the audit finding, conclusions & recommendations.***

Following are some definitions & their explanations:

1.) AUDIT FINDINGS:

The audit findings should be formally documented & includes-

- The process area audited.
- The objective of the process.
- The control Objective
- The result of the test of that control.
- Recommendations in case of a control deficiency.

An audit finding form serves the purpose of documenting both control strength & weaknesses.

2.) ANALYSIS:

Analysis is the most important factor in converting raw material into finished product ready for inclusion in audit report. Complete analysis of test information should provide the auditor with all necessary information to write an audit report.

Following are the steps involved in the analysis part:

- Reexamine the standards and the facts.
- Determine the cause of the deviation.
- Determine the materiality and exposure of the deviation.
- Determine possible recommendations for corrective actions.

Following is the discussion of the four steps in details:

REEXAMINATION:

-- The auditor has the requisite data to make a judgment & formulate opinion.

-- Here 2 factors are considered i.e. **standards(for comparing data) & facts(to compare to standards).**

STANDARD COMPLIANCE:

-- Standards are procedures, operating guidelines, regulations, good business practices or predefined methodologies.

-- It defines how an operation under audit should function.

-- Standards must b clearly understood by the auditor & there must be sufficient confidence that the correct standard is used.

FACTS:

-- After standards are reviewed, auditor must evaluate the gathered facts.

-- Auditor must re-verify deviations, which are representative of current control environment.

-- To ensure that findings are accurate & descriptive, samples should be-- >

- ***Large enough to reflect behavior of population(Data).***
- ***Representative of all types of individual in the population.***

VERIFICATION:

-- The auditor must compare findings to reexamined standards,

-- to determine discrepancies, if any.

CAUSE:

-- Once auditor is sure of the understanding of standards, the next step is to identify the cause of deviation.

-- This is based on reexamination of the standards involved.

-- Determining cause of the deviation is the answering the:

- Who, what
- What, why, when

VIII. CONCURRENT OR CONTINOUS AUDIT AND EMBEDDED AUDIT MODULES:

Organization of 21st century produces information on real time basis, online basis. So real time recording of the information needs real-time auditing.

Errors in computerized systems are generated at high speeds & the cost to correct it is very high. Continuous auditing enables he auditor to detect the errors as when the transaction happens.

There are various continuous audit techniques may be used. Audit software is available which could be used for selecting & testing data. Some of the audit tools are explained as under:

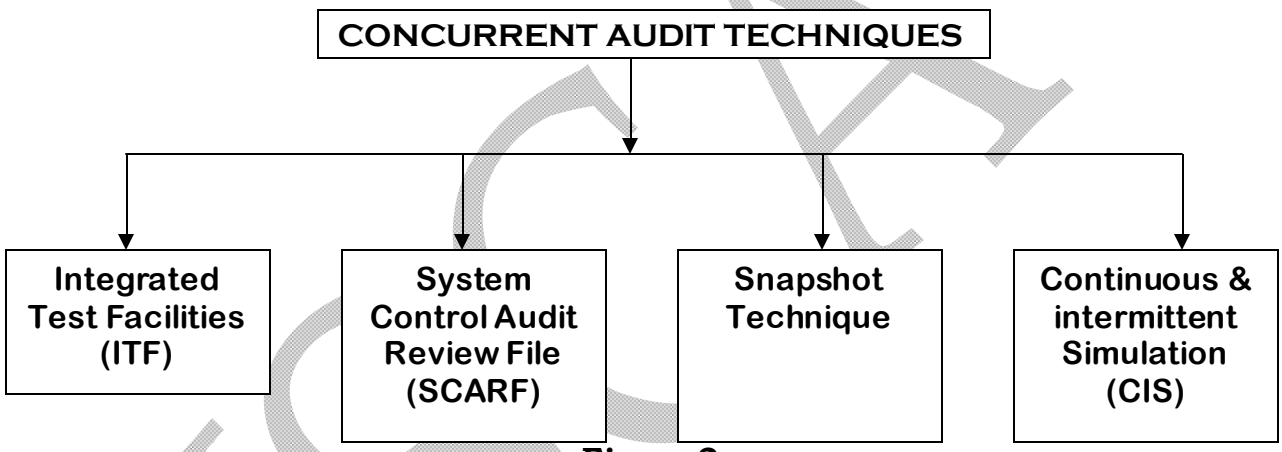


Figure 2

A. **INTEGRATED TEST FACILITIES:**

- Involves creation of dummy entity in the application system files.
- The dummy records entered by the auditor don't affect the actual records in system.
- Auditor after entering dummy records evaluate the processing & output of these transaction with the expected processing & output & verifies whether the system & its control are operating correctly or not.

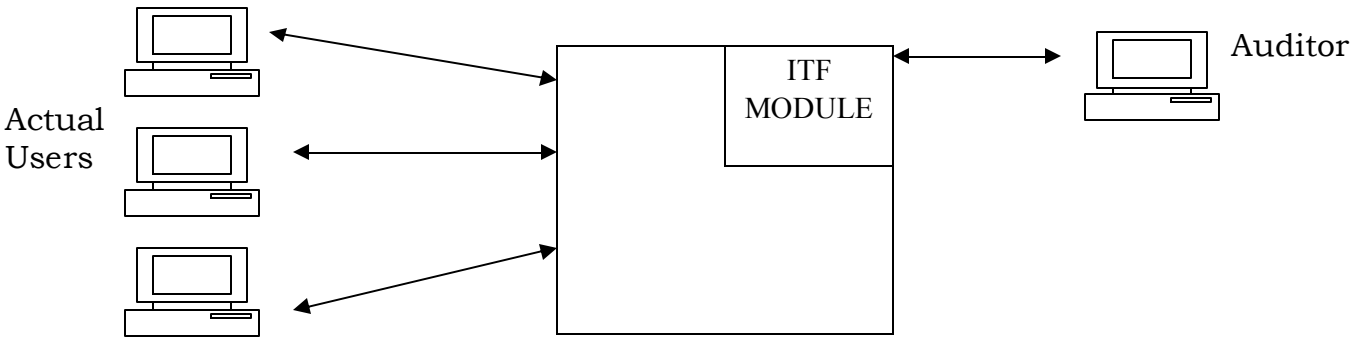
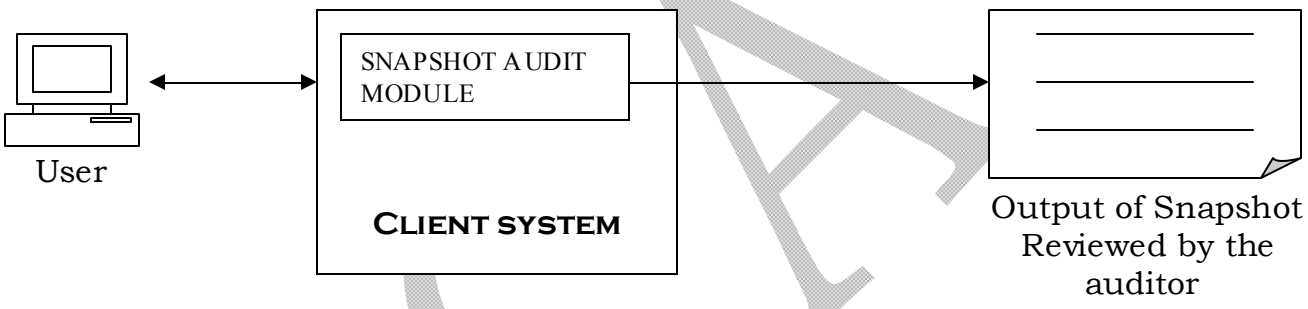


Figure 3: Online System with ITF Facility

B. **SNAPSHOTS:**

- The snapshot is built into the system at those points where material processing occurs which take images of the flow of transaction as it moves through application.
- These images then used to assess the **accuracy, authenticity & completeness** of the processing carried out on the transaction.
- All the snapshot data related to a transaction can be collected in records at one place thereby facilitating audit evaluation work.



C. **SCARF: System Control Audit Review File**

- It involves embedding audit software modules within a HOST application system.
- The data are recorded in a SCARF file or audit log.
- Auditor then examines the information contained in this file to see if some aspect of the application system needs follow-up.
- Following types of information is collected by using SCAF:
  -- Application system errors **-- System Exception** **-- Profiling Data**
  -- Policy & procedure Variance **-- Statistical Sample** **-- Snapshot & extended Records**

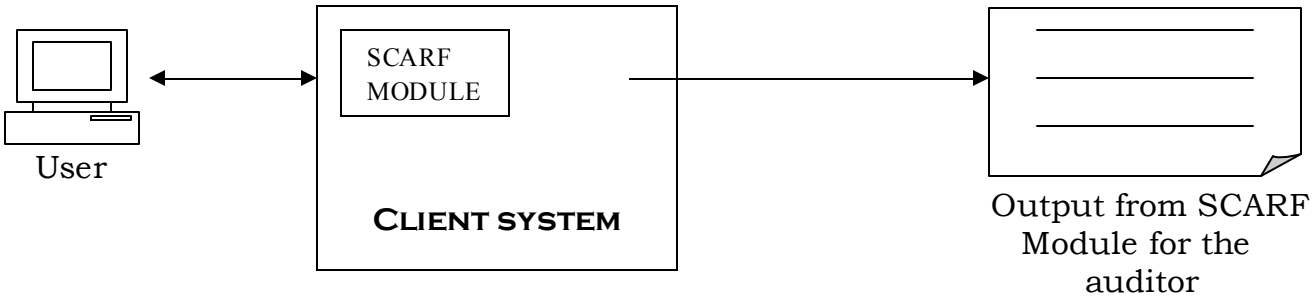


Figure 4

D. **CONTINUOUS & INTERMITTENT SIMULATION (CIS):**

- This is a variation of the SCARF continuous audit technique.
- It is used to trap exceptions wherever the application system uses a database management system. **CIS** executes in the following way:
  - ☑ The database management system reads an application system transaction. It is passed to CIS.
  - ☑ CIS then determine whether it wants to examine transaction further.
  - ☑ CIS replicates the application system processing.
  - ☑ Every update to database that arises from processing the selected transaction will be checked by CIS to determine any difference between the results by CIS & application system.
  - ☑ Exceptions identified by CIS are written to EXCEPTION LOG FILE.

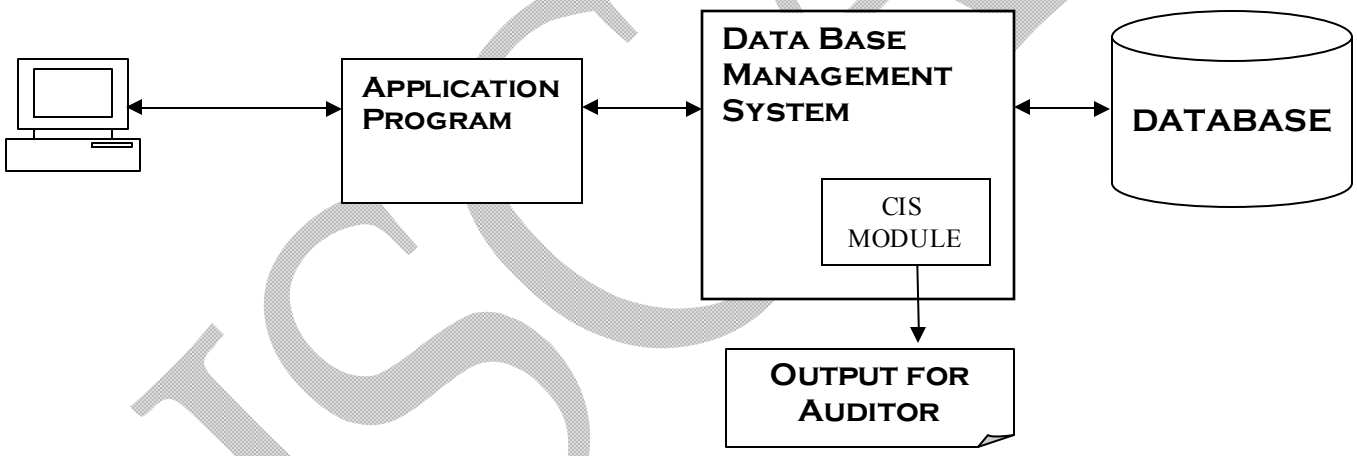


Figure 5

Code	Advantages of CIS	Code	Disadvantages of CIS
I	**Information** system whether capable of meeting the set objective i.e. Data integrity.	**K**	**Knowledge** of expert is needed by the auditor about the information system working.
T	**Test(surprise)** can be done by auditor without the system staff & users being aware that evidences is collected.	**A**	**Audit** Trails is less visible under this & costs of the error & irregularities is very high.
A	**Audit** is conducted in time & in very comprehensive manner. Entire process can be evaluated.	**U**	In **unstable** application system CIS is not effective.
T	**Training** for new users.	**R**	All **resources** has to be obtained by the auditor from organization to support audit techniques.

IX. HARDWARE TESTING AND REVIEW:

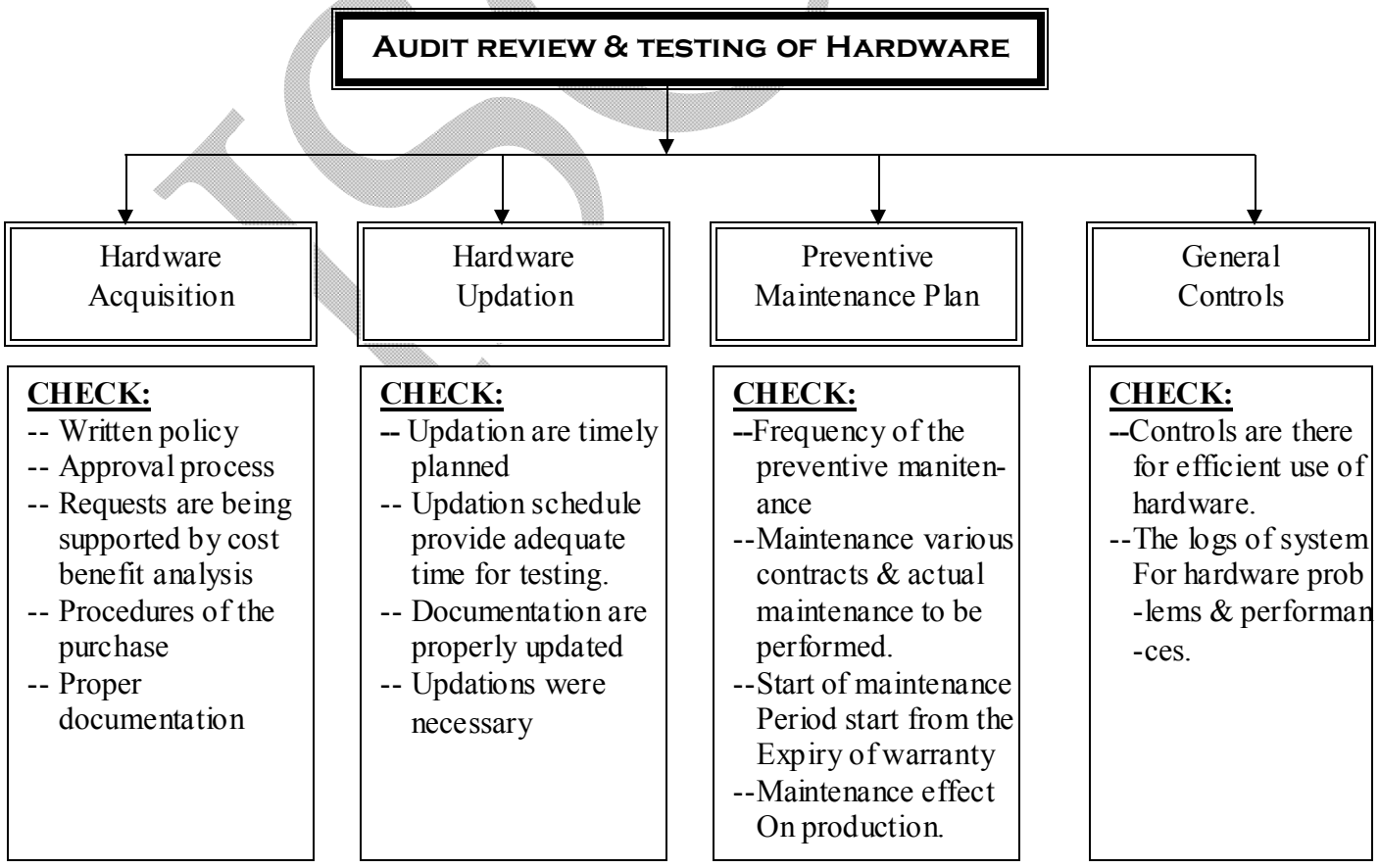
Hardware test & review is also important part of the information system. Hardware to be tested for the following:

☑ **Performance**	☑ **Error Handling**
☑ **Memory Capacity**	☑ **Nos. of users simultaneously**
☑ **Security**	☑ **Maintenance Support**
☑ **Reliability**	☑ **Accessibility Testing**

The auditor should review and audit the procedures for following hardware related risk:

- ☑ **Hardware Acquisition**
- ☑ **Hardware Updation**
- ☑ **Preventive Maintenance Plan**
- ☑ **General controls used for efficient & reliable working of hardware**

Following is the diagrammatic representation of the audit of hardware:



X. OPERATING SYSTEM REVIEW:

In this auditor review the **procurement, implementation, execution & 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 system documentation specifically in the areas of:
  - ☑ Operating documents
  - ☑ Maintenance Documents
  - ☑ Users instruction etc.
- Review and test systems software implementation to determine adequacy of control:
  - ☑ Authorization procedures
  - ☑ Access security features
  - ☑ Documentation requirements
  - ☑ Documentation of system testing
  - ☑ Audit Trails
- Review system software security procedures etc.

XI. REVIEWING THE NETWORK:

The review of controls over LANs is done to ensure that the standards are in place for designing and selecting a LAN.

PRE-REQUISITE FROM AUDITOR FOR NETWORK AUDIT:

- LAN components (servers, modems, routers & communication channels)
- Network Topologies (such as STAR, MESH etc) & LAN configuration in terms of interconnection to other LANs, WANs etc.
- LAN technicalities like communication or traffic type.
- Authorized user group of LAN.

REVIEW AND TEST OF CONTROLS IN NETWORK AUDIT:

The auditor review, test & validate the following controls fro network:

- Physical Controls
- Logical Controls
- Environment Controls

TEST OF PHYSICAL CONTROLS:

Code to remember: US - LAB

1.) **U**PS working

2.) **S**erver:

- Server Access.
- Server room access (restricted to administrator).
- Server room remains properly locked & keys are used in controlled manner.
- Server protection from electric surge.

3.) **L**AN:

- LAN documentation access.
- LAN components Access.
- LAN wiring/ cabling/ telecommunication links.

3.) **A**ccess :

- Workstation Access.

4.) **B**ack up:

- Backup diskettes ad tapes access.

TEST OF LOGICAL CONTROLS:

Code to remember: FD- PAN (means for Fixed Deposit need PAN)

1.) **F**irewall

2.) **D**ata encryption

3.) **P**assword (Login ID)

4.) **A**ccess controls (access of applications & programs)

5.) **N**etwork Monitoring

TEST OF ENVIRONMENTAL CONTROLS:

Code to remember: F.E.L.T.

1.) Fire:

- Facilities are protected from fire by having protected power cables.
- Fire Extinguishers are placed at correct locations.
- Fire alarm and smoke detectors are working properly.

2.) Electric surge protectors are in place.

3.) LAN:

- LAN file server facilities are protected from water damage/flood.
- LAN workstation should be disabled automatically after a short period of inactivity.

4.) Temperature and humidity are adequate.