CHAPTER 4

TESTING – GENERAL AND AUTOMATED CONTROLS

⇨ MEANING & OBJECTIVE OF TESTING

Explain software testing and state its objectives. *(N'08- 5 Marks)*

☞ Meaning:

- ✳ Testing is a process used to **IDENTIFY THE CORRECTNESS, COMPLETENESS AND QUALITY OF DEVELOPED COMPUTER SOFTWARE**.
- ✳ In other words, testing is nothing but **CRITICISM or COMPARISON**, i.e. comparing the actual value with expected one.
- ✳ The word testing means the dynamic analysis of the product—putting the product through its paces.
- ✳ Testing helps in verifying and validating if the software is working as it is intended to be working.

☞ Objectives of Software Testing include:

- ✳ Testing is a process of executing a program with the **INTENT OF FINDING AN ERROR**.
- ✳ A good test case is one that has a **HIGH PROBABILITY OF FINDING A YET UNDISCOVERED ERROR**.
- ✳ A successful test is one that **UNCOVERS A YET UNDISCOVERED ERROR**.

The data collected through testing can also provide an indication of the software's **RELIABILITY AND QUALITY**. However, testing **CANNOT SHOW THE ABSENCE OF DEFECT, IT CAN ONLY SHOW THAT SOFTWARE DEFECTS ARE PRESENT**.

⇨ TESTING OF CONTROL

☞ Testing of Controls involves obtaining the **POPULATION AND CONDUCTING THE COMPLIANCE TESTS** either on the entire population and/or on selected samples from the population. It may also be conducted using utilities of audit tools. Testing of the controls design and the reliable results are done by one of the following methods:

I. Substantive Testing:

- ✳ This type of testing is used to **SUBSTANTIATE THE INTEGRITY OF THE ACTUAL PROCESSING**.
- ✳ It is used to ensure that processes, not controls, are working as per the design of the control and produce the reliable results.

II. Compliance Testing:

- ✳ A compliance test determines if **CONTROLS ARE WORKING AS DESIGNED**.
- ✳ As per the policies and procedures, compliance testing results into the adherence to management directives.

⇨ INFORMATION SYSTEM (IS) CONTROLS AUDIT

The Information System (IS) controls audit involves the following three phases:

- ☞ Planning:
  - ✳ The auditor determines an effective and efficient way to obtain the evidential matter necessary to achieve the objectives of the IS controls audit and the audit report.
  - ✳ For financial audits, the auditor develops an **AUDIT STRATEGY AND AN AUDIT PLAN**.
  - ✳ For performance audits, the auditor develops an audit plan.
- ☞ Testing: The auditor **TESTS THE EFFECTIVENESS** of IS controls that are relevant to the audit objectives.
- ☞ Reporting: The auditor concludes on the effect of any identified IS control weaknesses with respect to the audit objectives and reports the **RESULTS OF THE AUDIT**, including any **MATERIAL WEAKNESSES** and other significant deficiencies.

⇨ AUDIT TEST

- ☞ The auditor must address many considerations that cover the nature, timing, and extent of testing.
- ☞ The auditor must devise an auditing testing plan and a testing methodology to determine whether the previously identified controls are effective.
- ☞ The auditor also tests whether the end-user applications are producing valid and accurate information.
- ☞ The auditor should also conduct several tests with both valid and invalid data to test the ability and extent of error detection, correction, and prevention within the application.
- ☞ The auditor should look for controls such as input balancing and record or hash totals to ensure that the end user reconciles any differences between input and output.
- ☞ The intensity and extent of the testing should be related to the sensitivity and importance of the application.
- ☞ The auditor should be wary of too much testing and limit his or her tests to controls that cover all the key risk exposures and possible error types.
- ☞ The key audit concern is that the testing should reveal any type of exposure of sensitive data and that the information produced by the application is valid, intact, and correct.
- ☞ One should test the critical controls, processes, and apparent exposures.
- ☞ The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.
- ☞ Secondly, we may test the critical controls, processes, and apparent exposures.
- ☞ The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.
- ☞ Validation of the information obtained is prescribed by the auditor's work program. Again, this work program is the organized, written, and pre-planned approach to the study of the IT department. It calls for validation in several ways as follows:
  - ✳ Asking different personnel the same question and comparing the answers
  - ✳ Asking the same question in different ways at different times

- ✳ Comparing checklist answers to work papers, programs, documentation, tests, or other verifiable results
- ✳ Comparing checklist answers to observations and actual system results
- ✳ Conducting mini-studies of critical phases of the operation

- ☞ Such an intensive program allows an auditor to become informed about the operation in a short time.
- ☞ Programs are run on the computer to test and authenticate application programs that are run in normal processing.
- ☞ The audit team selects one of the many generalized audit software (GAS) packages such as Microsoft Access or Excel, IDEA, or ACL and determineswhat changes are necessary to run the software at the installation.
- ☞ The auditor is to use one of these software's to do sampling, data extraction, exception reporting, summarize and foot totals, and other tasks to perform in-depth analysis and reporting capability.

⇨ INFORMATION SYSTEM (IS) CONTROLS AUDIT PROCESS

Auditors need to determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. It also provides some factors to assist the auditor in making this determination. Explain those factors, in brief.

These factors are given as follows:

- ☞ The extent to which internal controls that are significant to the audit depend on the **RELIABILITY OF INFORMATION PROCESSED** or generated by information systems.
- ☞ <u>The availability of evidence outside the information system to support the findings and conclusions</u>:
  - ✳ It may not be possible for auditors **TO OBTAIN SUFFICIENT, APPROPRIATE EVIDENCE** without assessing the effectiveness of relevant information systems controls.
  - ✳ For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls; there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.
- ☞ <u>The relationship of information systems controls to data reliability</u>:
  - ✳ To obtain evidence about the **RELIABILITY OF COMPUTER GENERATED INFORMATION**, auditors may decide to assess the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data.
  - ✳ If the auditor concludes that information systems controls are effective, the auditor may **REDUCE THE EXTENT OF DIRECT TESTING** of data.
- ☞ <u>Assessing the effectiveness of information systems controls as an audit objective</u>:
  - ✳ When assessing the effectiveness of information systems controls is directly a part of audit objective, auditors should test information systems controls necessary to address the audit objectives.

- For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.

Explain the information which should be included by auditors in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives.

The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:

- Identification of entity wide level controls (and appropriate system level controls):
  - designed to achieve the control activities for each critical element within each general control area and
  - a determination of whether they are designed effectively and implemented (placed in operation),
  - including identification of control activities for which there are no or ineffective controls at the entity wide level and the related risks;
- Identification of business process level controls:
  - for key applications identified as key areas of audit interest,
  - determination of where those controls are implemented (placed in operation) within the entity's systems, and
  - the auditor's conclusion about whether the controls are designed effectively,
  - including identification of control activities for which there are no or ineffective controls and the related risks and
  - the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data;
- Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year;
- Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS weaknesses and IS control weaknesses;

Status of the prior years' audit findings;

- Documentation for any significant computer security related incidents identified and reported for the last year;
- Documented security plans;
- Documented risk assessments for relevant systems (e.g., general support systems and major applications);
- System certification and accreditation documentation or equivalent for relevant systems;
- Documented business continuity of operations plans and disaster recovery plans; and
- A description of the entity's use of third-party IT services
- Relevant laws and regulations and their relation to the audit objectives.
- Description of the auditor's procedures to consider the risk of fraud, any fraud risk factors that the auditor believes could affect the audit objectives, and planned audit

procedures to detect any fraud significant to the audit objectives.

- ☞ Audit resources planned.
- ☞ Current multiyear testing plans.
- ☞ Documentation of communications with entity management.
- ☞ If IS controls are performed by service organizations, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports)
- ☞ If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- ☞ Audit plan that adequately describes the objectives, scope, and methodology of the audit.
- ☞ Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

☞ PERFORMING INFORMATION SYSTEM CONTROLS AUDIT TESTS

"An auditor Identifies control techniques and determines the effectiveness of control at various levels". Explain those levels brief.

The auditor identifies control techniques and determines the effectiveness of controls at each of the following levels:

i. Entity wide or Component Level (General control):
   - ✳ Controls at the entity or component level consist of the entity-wide or component-wide (IS system modules) processes designed to achieve the control activities.
   - ✳ They are focused on how the entity or component manages IS related to each control activity.

ii. System level (General controls):
   - ✳ Controls at the system level consist of processes for managing specific system resources related to either a general support system or major application.
   - ✳ These controls are more **SPECIFIC** than those at the entity or component level and generally relate to a **SINGLE TYPE OF TECHNOLOGY**.
   - ✳ Within the system level are three further levels that the auditor should assess: network, operating system, and infrastructure application. The three sublevels can be defined as follows:
     a. Network: A network is an interconnected or intersecting configuration or system of components.
     b. Operating system: An operating system is software that controls the execution of computer programs and may provide various services.
     c. Infrastructure applications:
        - ✳ Infrastructure applications are software that is used to assist in performing systems operations, including management of network devices.
        - ✳ These applications include databases, e-mail, browsers, plug-ins, utilities, and applications not directly related to business processes. .

iii. Business process application level: Controls at the business process application level

consist of policies and procedures for controlling specific business processes.

General control activities that are applicable to the entity wide and system levels, includes the general controls applied at the business process application level (also referred to as application security) as well as the three categories of business process application controls.

- TEST EFFECTIVENESS OF INFORMATION SYSTEM CONTROLS
  - The auditor should design and conduct tests of relevant control techniques that are effective in design to determine their effectiveness in operation.
  - It is generally more efficient for the auditor to test IS controls on
    - a tiered basis,
    - starting with the general controls at the entity wide and system levels,
    - followed by the general controls at the business process application level, and
    - Concluding with tests of business process application, interface, and
    - Data management system controls at the business process application level.
  - Such a testing strategy may be used because ineffective IS controls at each tier generally preclude effective controls at the subsequent tier.
  - If the auditor identifies IS controls for testing, the auditor should evaluate the effectiveness of
    - general controls at the entity wide and system level;
    - general controls at the business process application level; and
    - specific business process application controls (business process controls, interface controls, data management system controls), and/or user controls, unless the IS controls that achieve the control objectives are general controls.
  - The auditor should determine whether entity wide and system level general controls are effectively designed, implemented, and operating effectively by:
    - identifying applicable general controls;
    - determining how those controls function, and whether they have been placed in operation; and
    - Evaluating and testing the effectiveness of the identified controls.
  - The auditor generally should use knowledge obtained in the planning phase.
  - The auditor should document the understanding of general controls and should conclude whether such controls are effectively designed, placed in operation, and, for those controls tested, operating as intended.

- TEST EFFECTIVENESS OF INFORMATION SYSTEM CONTROLS

To assess the operating effectiveness of IS controls; auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Explain these procedures, in brief.

To assess the operating effectiveness of IS controls; auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Such procedures could include the following:

- Inquiries of IT and management personnel :

- ✳ Inquiries of IT and management personnel can enable the auditor **TO GATHER A WIDE VARIETY OF INFORMATION** about the operating effectiveness of control techniques.
- ✳ The auditor should corroborate responses to inquiries with other techniques.

☞ Questionnaires: can be used to **OBTAIN INFORMATION** on controls and how they are designed.

☞ Observation:
- ✳ Observation of the operation of controls can be a **RELIABLE SOURCE** of evidence.
- ✳ For example, the auditor may observe the verification of edit checks and password controls.
- ✳ However, observation provides evidence about controls only **WHEN THE AUDITOR WAS PRESENT**.
- ✳ The auditor needs other evidence to be satisfied controls functioned the same way throughout the period.

☞ Review Documentation:
- ✳ The auditor may review documentation of control polices and procedures.
- ✳ For example, the entity may have written policies regarding confidentiality or logical access.
- ✳ Review of documents will allow the auditors to **UNDERSTAND AND ASSESS THE DESIGN OF CONTROLS.**

☞ Inspection of approvals/reviews:
- ✳ It provides the auditor with evidence that management is performing **APPROPRIATE CONTROL CHECKS.**
- ✳ The auditor may combine these tests with discussions and observations.

☞ Analysis of system information (e.g., configuration settings, access control lists, etc.) obtained through system or **SPECIALIZED SOFTWARE** provides the auditor with evidence about actual system configuration.

☞ Data review and analysis of the output of the application processing:
- ✳ It may provide evidence about the **ACCURACY OF PROCESSING**.
- ✳ For example, a detailed review of the data elements or analytical procedures of the data as a whole may reveal the existence of errors.
- ✳ Computer- assisted audit techniques (CAAT) may be used to test data files to determine whether invalid transactions were identified and corrected by programmed controls.
- ✳ However, the absence of invalid transactions alone is insufficient evidence that the controls effectively operated.

☞ Re-performance of the control:
- ✳ It could be used to test the **EFFECTIVENESS OF SOME PROGRAMMED** controls by reapplying the control through the use of test data.
- ✳ For example, the auditor could prepare a file of transactions that contains known errors and determine if the application successfully captures and reports the known errors.

Based on the results of the IS controls audit tests, the auditor should determine whether

the control techniques are operating effectively to achieve the control activities. Controls that are not properly designed to achieve the control activities or that are not operating effectively are potential IS control weaknesses.

For each potential weakness, the auditor should determine whether there are specific compensating controls or other factors that could mitigate the potential weakness. If the auditor believes that the compensating controls or other factors could adequately mitigate the potential weakness and achieve the control activity, the auditor should obtain evidence that the compensating or other control is effectively operating and actually mitigates the potential weakness. If it effectively mitigates the potential weakness, the auditor can conclude that the control activity is achieved; however, the auditor may communicate such weaknesses to the entity. If the potential weakness is not effectively mitigated, the potential weakness is an actual weakness. The auditor evaluates its effects on IS controls in combination with other identified weaknesses in the reporting phase.

- 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.
  - Feature:
    - This plan should **NOT COVER PERIOD OF MORE THAN 3 YEARS**.
    - Should include **SCHEDULE & SCOPE OF ASSESSMENT** to be performed.
  - Advantage:
    - Plans to conduct the **COMPREHENSIVE TESTS** for significant business process applications by dividing audit process on multiyear basis.
    - **AGENCY SYSTEM & LOCATIONS** are considered in IS control evaluation processes.
    - **RELATIVE RISKS** are considered and prioritize the audit time.
    - **ANNUAL AUDIT RESOURCES & COST** is reduced.
  - Limitation:
    - Not applicable to those organization which don't have **STRONG ENTITY WIDE CONTROLS**.
    - Not suitable for **FIRST TIME AUDIT**. 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.
    - Tests which are being used by the **AUDITOR ARE LIMITED**.

- DOCUMENTATION OF CONTROL TESTING PHASE

  Information developed in the testing phase that the auditor should document includes the following:
  - **AN UNDERSTANDING OF THE INFORMATION SYSTEMS** that are relevant to the audit objectives
  - **IS CONTROL OBJECTIVES AND ACTIVITIES** relevant to the audit objectives
  - By level (e.g., entity wide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a **DESCRIPTION OF CONTROL TECHNIQUES** used by the entity to achieve the relevant IS control objectives

and activities

- By level and sublevel, **SPECIFIC TESTS PERFORMED**,
- related documentation that describes the **NATURE, TIMING, AND EXTENT OF THE TESTS**;
- **EVIDENCE OF THE EFFECTIVE OPERATION** of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
- if a control is not achieved, any **COMPENSATING CONTROLS** or other factors and the basis for determining whether they are effective;
- the **AUDITOR'S CONCLUSIONS** about the effectiveness of the entity's IS controls in achieving the control objective; and
- **FOR EACH WEAKNESS**, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

- 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, and VALIDITY and CONFIDENTIALLY OF APPLICATION DATA RELEVANT TO THE AUDIT OBJECTIVES.**
  - Following are the aspects covered under the audit reporting

a. Objective 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.

b. Reporting 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.

c. Testing (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. Documenting 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:

   a. 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).

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

   c. 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

   d. VERIFICATION:
      - ✳ The auditor must compare findings to reexamined standards,
      - ✳ To determine discrepancies, if any.

   e. 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

- CONCURRENT OR CONTINUOS AUDIT AND EMBEEDED AUDIT MODULES

  - Today, organizations produce information on a real-time, online basis. **A REAL-TIME RECORDING NEEDS REAL-TIME AUDITING** to provide **CONTINUOUS ASSURANCE** about the quality of the data.
  - Reduce time between **OCCURRENCE OF THE CLIENT'S EVENTS AND THE AUDITOR'S ASSURANCE** services thereon.
  - Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the **POINT OF THEIR OCCURRENCE** the impact thereof would be the least
  - Continuous auditing techniques use two bases for collecting audit evidence:
    - Use of **EMBEDDED MODULES** in the system to collect, process, and print audit evidence and
    - **SPECIAL AUDIT RECORDS** used to store the audit evidence collected.
  - Many audit tools are also available some of which are described below:
    1. Snapshot
    2. Integrated Test Facility (ITF)
    3. System Control Audit Review File (SCARF)
    4. Continuous and Intermitted Simulation (CIS)

1. SNAPSHOT:
   - It is used to Trace a transaction is computerized system.
   - The snapshot software is **BUILT INTO THE SYSTEM AT THOSE POINTS WHERE MATERIAL PROCESSING OCCURS**.
   - It takes **IMAGES** of the flow of any transaction as it moves through the application.
   - The images are then used to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.
   - Important Consideration
     - To locate the snapshot points based on materiality of transactions
     - When the snapshot will be captured and
     - The reporting system design and implementation.

2. INTEGRATED TEST FACILITY (ITF):
   - The ITF technique involves the creation of a **DUMMY ENTITY** in the application system files.
     - The processing of audit **TEST DATA AGAINST THE DUMMY ENTITY** as a means of verifying processing authenticity, accuracy, and completeness.
     - This test data would be included with the **NORMAL PRODUCTION DATA USED** as input to the application system. Auditor has to decide on method to enter test data and the methodology for removal of the effects of the ITF transactions.
   - Methods of Entering Test Data:
     - Tagging:
       - The transactions to be tested have to be **TAGGED.**
       - The application system has to be **PROGRAMMED TO RECOGNIZE** the tagged

transactions and have them invoke two updates,

1. To the application system master file record and
2. To the ITF dummy entity.

- Auditors can also **EMBED AUDIT SOFTWARE** modules **TO RECOGNIZE** transactions having characteristics as ITF transactions.
- Advantage: **EASE OF USE** and testing with transactions representative of **NORMAL SYSTEM PROCESSING**.
- Disadvantage: use of live data could mean that the **LIMITING CONDITIONS** within the system are not tested and embedded modules may **INTERFERE WITH THE PRODUCTION PROCESSING.**

✳ Special Prepared Test Data:

- The auditors may also use test data that is specially prepared.
- Test transactions would be entered along with the **PRODUCTION INPUT**.
- Advantage:
  - ✓ Test data is likely to achieve **MORE COMPLETE COVERAGE** of the execution paths in the application system to be tested than selected production data.
  - ✓ The application system does not have to be **MODIFIED** to tag the ITF transactions.
- Disadvantage: Preparation of the test data could be **TIME CONSUMING AND COSTLY**.

☞ Methods of Removing the Effects of ITF Transactions:

The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed.

✳ The application system may be **PROGRAMMED TO RECOGNIZE** ITF transactions and **TO IGNORE** them in terms of any processing.

✳ Submitting additional inputs that **REVERSE THE EFFECTS** of the ITF transactions.

✳ Submit **TRIVIAL ENTRIES** so that the effects of the ITF transactions on the output are minimal. The effects of the transactions are not really removed.

3. SYSTEM CONTROL AUDIT REVIEW FILE (SCARF)

☞ It involves embedding audit software modules within a host application system to provide **CONTINUOUS MONITORING** of the system's transactions.

☞ The information collected is written onto a special audit file- the **SCARF MASTER FILES**.

☞ Auditors then examine the information contained on this file.

☞ Auditors might use SCARF to collect the following types of information:

✳ **Application system error**: SCARF audit routines provide an independent check on the **QUALITY OF SYSTEM PROCESSING**, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.

✳ **Policy and procedural variances**:

- Organizations have to **ADHERE TO THE POLICIES, PROCEDURES AND**

STANDARDS of the organization and the industry to which they belong.

- SCARF audit routines can be used to check when **VARIATIONS** from these policies, procedures and standards have occurred.

- **System exception**:
  - SCARF can be used to monitor **DIFFERENT TYPES OF APPLICATION SYSTEM EXCEPTIONS**.
  - For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical sample:** SCARF provides an **EASY WAY OF COLLECTING ALL THE SAMPLE INFORMATION** together on one file and use analytical review tools thereon.
- **Snapshots and extended records:** Snapshots and extended records can be written into the SCARF file and **PRINTED** when required.
- **Profiling data:**
  - Auditors can use embedded audit routines to collect data to **BUILD PROFILES** of system users.
  - Deviations from these profiles indicate that there may be **SOME ERRORS OR IRREGULARITIES**.
- **Performance measurement:** Auditors can use embedded routines to collect data that is useful for **MEASURING OR IMPROVING** the performance of an application system.

4. CONTINUOUS AND INTERMITTED SIMULATION (CIS):

- This is a variation of the SCARF continuous audit technique.
- This technique can be used to **TRAP EXCEPTIONS** whenever the application system uses a database management system.
- During application system processing, CIS executes in the following way:
  - DBMS:
    - The database management system reads an **APPLICATION SYSTEM TRANSACTION**.
    - It is passed to **CIS**.
    - CIS then determines whether it wants to examine the transaction further.
    - If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
  - CIS replicates or **SIMULATES** the application system processing.
  - Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether **DISCREPANCIES EXIST** between
    - The results it produces and
    - Those the application system produces.
  - Exceptions identified by CIS are written to an **EXCEPTION LOG FILE**.
  - The advantage of CIS is that it **DOES NOT REQUIRE MODIFICATIONS** to the application system and yet **PROVIDES AN ONLINE AUDITING CAPABILITY**.

- Advantages and Disadvantages of Continuous Auditing: Continuous auditing has a

number of potential benefits including:

- ✳ reducing the cost of the basic audit assignment by enabling auditors to test a larger sample (up to 100 percent) of client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;
- ✳ reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;
- ✳ increasing the quality of audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structure; and
- ✳ specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis

☞ Advantages of continuous audit techniques (M'10- 5 Marks):

- ✳ Timely, comprehensive and detailed auditing:
  - 🖋 Evidence would be available more timely and in a comprehensive manner.
  - 🖋 The entire processing can be evaluated and analyzed rather than examining the 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.
- ✳ Information to system staff on meeting of objectives:
  Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- ✳ Training for new users:
  - 🖋 Using the ITFs new users can submit data to the application system, and
  - 🖋 Obtain feedback on any mistakes they make via the system's error reports.

☞ Disadvantages and limitations of the use of the continuous audit system:

- ✳ Auditors should be able **TO OBTAIN RESOURCES REQUIRED** from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- ✳ Continuous audit techniques are more likely to be **USED IF AUDITORS ARE INVOLVED IN THE DEVELOPMENT** work associated with a new application system.
- ✳ Auditors need the **KNOWLEDGE AND EXPERIENCE OF WORKING WITH COMPUTER SYSTEMS** to be able to use continuous audit techniques effectively and efficiently.
- ✳ 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**.
- ✳ Continuous audit techniques are unlikely to be effective unless they are implemented in an **APPLICATION SYSTEM THAT IS RELATIVELY STABLE**

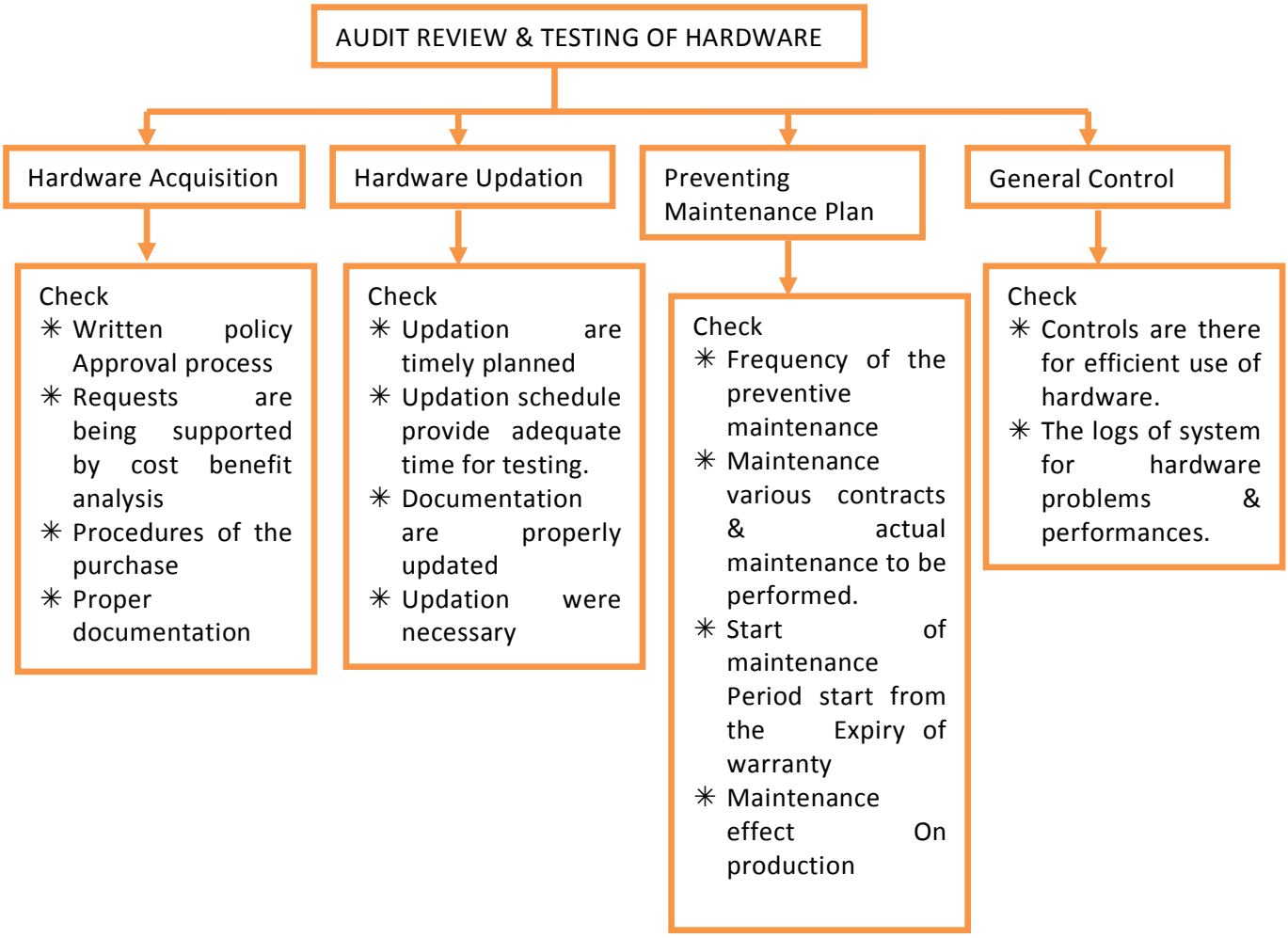
☞ HARDWARE TESTING AND REVIEW:

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

- ✳ Functional testing
- ✳ User Interface testing
- ✳ Usability testing
- ✳ Compatibility testing
- ✳ Model Based testing
- ✳ Error exit testing
- ✳ User help testing
- ✳ Security testing
- ✳ Capacity testing
- ✳ Performance testing
- ✳ Reliability testing
- ✳ Recovery testing
- ✳ Installation testing
- ✳ Maintenance testing
- ✳ Accessibility testing

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

- ✳ Hardware Acquisition
- ✳ Hardware Updation
- ✳ Preventing Maintenance Plan
- ✳ General Control used for efficient and reliable working of hardware.



- OPERATING SYSTEM REVIEW:

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

  - Review and approval process of option selection
  - Review cost/benefit analysis of system software procedures
  - Review controls over the installation of changed system software
  - Review systems documentation specifically in the areas of:
    - Installation control statements
    - Parameter tables
    - Exit definitions
    - Activity logs/reports
  - Review and test systems software implement
    - Change procedures
    - Authorization procedures
    - Access security features
    - Documentation requirements
    - Documentation of system testing
    - Audit trails:
- REVIEWING OF 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:
    - UPS working
    - Server:
      - Server Access.
      - Server room access (restricted to administrator).
      - Server room remains properly locked & keys are used in controlled manner
      - Server protection from electric surge.
    - LAN:
      - LAN documentation access.
      - LAN components Access.
      - LAN wiring/ cabling/ telecommunication links.
    - Access: Workstation Access.
    - Back up: Backup diskettes ad tapes access.

- TEST OF LOGICAL CONTROLS:
  - Firewall
  - Data encryption
  - Password (Login ID)
  - Access controls (access of applications & programs)
  - Network Monitoring
- TEST OF ENVIRONMENTAL CONTROLS:
  - 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.
  - Electric surge protectors are in place.
  - LAN:
    - LAN file server facilities are protected from water damage/flood.
    - LAN workstation should be disabled automatically after a short period of inactivity.
  - Temperature and humidity are adequate.