

4.1 Learning Objectives

- ◆ To understand the reasons for testing;
- ◆ To have an idea about Audit Planning and Testing;
- ◆ To discuss testing critical control points;
- ◆ To learn tests of general controls at various levels;
- ◆ To have an idea about Continuous Audit and Embedded Audit Modules, and
- ◆ To discuss hardware testing and review of operating system and network.

4.2 Introduction to Basics of Testing (Reasons for Testing)

Testing is a scientific process performed to determine whether the controls ensure the system design effectiveness as well as the implemented system controls operational effectiveness. It involves, understanding a process and the expected results. 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.

4.3 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.

4.4 Audit Planning

- In planning the IS controls audit, the auditor uses the equivalent concepts of materiality (in financial audits) and significance (in performance audits) to plan both effective and efficient audit procedures.
- Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures.
- The underlying principle is that the auditor is not required to spend resources on items of little importance; that is, those that would not affect the judgment or conduct of a reasonable user of the audit report, in light of surrounding circumstances.
- On the basis of this principle, the auditor may determine that some areas of the IS controls audit (e.g. specific systems) are not material or significant, and therefore warrant little or no audit attention.
- Materiality and significance include both quantitative and qualitative factors in relation to the subject matter of the audit.
- Even though a system may process transactions that are quantitatively immaterial or insignificant, the system may contain sensitive information or provide an access path to other systems that contain information that is sensitive or otherwise material or significant.
- Planning occurs throughout the audit as an iterative process.

4.5 Audit Testing

- 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.
- For microcomputers, several manual and automated methods are available to test for erroneous data.
- An initial step is to browse the directories of the PCs in which the end-user-developed application resides. Any irregularities in files should be investigated.
- Depending on the nature of the audit, computer-assisted techniques could also be used to audit the application.

- 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 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.
- 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 & 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

4.6 IS Controls Audit Process

The IS control Audit process involves:

- ➔ Obtaining an understanding of an entity and its operations and key business processes,
- ➔ Obtaining a general understanding of the structure of the entity's networks,
- ➔ Identifying key areas of audit interest (files, applications, systems, locations),
- ➔ Assessing IS risk on a preliminary basis,
- ➔ Identifying critical control points (for example, external access points to networks),
- ➔ Obtaining a preliminary understanding of IS controls, and
- ➔ Performing other audit planning procedures.
- The auditor performs planning to determine an effective and efficient way to obtain the evidential matter necessary to support the objectives of the IS controls audit and the audit report.

- The nature and extent of audit planning procedures varies for each audit depending on several factors, including the entity's size and complexity, the auditor's experience with the entity, and the auditor's knowledge of the entity's operations.
- If the IS controls audit is performed as part of a financial audit, the auditor is to obtain an understanding of internal control over financial reporting sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures based on that assessment.
- If the IS controls audit is performed as part of a performance audit, when information systems controls are determined to be significant to the audit objectives, auditors should then evaluate the design and operating effectiveness of such controls.
- Auditors should obtain a sufficient understanding of information systems controls necessary to assess audit risk and plan the audit within the context of the audit objectives.
- **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 the following factors to assist the auditor in making this determination:**
 - (i) The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.
 - (ii) The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without assessing the effectiveness of relevant information systems controls.
 - (iii) The relationship of information systems controls to data reliability: 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.
 - (iv) Assessing the effectiveness of information systems controls as an audit objective: 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.

4.7 Identify Key Areas of Audit Interest

- The auditor should identify key areas of audit interest, which are those that are critical to
- achieving the audit objectives (e.g., general support and business process application)
- systems and files (or components thereof).
- For a financial audit, this would include key financial applications and data and related feeder systems.
- For a performance audit, this would include key systems that are likely to be significant to the audit objectives.
- For each key area of audit interest, the auditor should document relevant general support systems and major applications and files, including
 - (i) the operational locations of each key system or file,
 - (ii) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems),
 - (iii) other significant systems or system level resources that support the key areas of audit interest, and
 - (iv) prior audit problems reported.

The auditor should also identify all access paths into and out of the key areas of audit interest. By identifying the key systems, files, or locations, the auditor can concentrate efforts on them, and do little or no work associated with other areas.

A preliminary understanding of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. 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.
- Identification of business process level controls for key applications identified as key of audit interest, determination of where those controls are implemented (placed in operation) within the entity's systems.
- 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;
- A description of the entity's use of third-party IT services;
- Relevant laws and regulations and their relation 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.

4.8 Performing Information System Controls Audit Tests

To understand the Information Systems relevant to the Audit in the testing phase of the IS controls audit, the auditor uses information obtained in the planning phase to test the effectiveness of IS controls that are relevant to the audit objectives.

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

(i) Entity wide or Component Level: (General controls)

- 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.
- For example, the entity or component may have an entity-wide process for configuration management, including establishment of accountability and responsibility for configuration management, broad policies and procedures, development and implementation of monitoring programs, and possibly centralized configuration management tools.
- The absence of entity-wide processes may be a root cause of weak or inconsistent controls; by increasing the risk that IS controls are not applied consistently across the organization.

(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.
- 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:
 - **Network:** A network is an interconnected or intersecting configuration or system of components. For example, a computer network allows applications operating on various computers to communicate.
 - **Operating system:** An operating system is software that controls the execution of computer programs and may provide various services. For example, an operating system may provide services such as resource allocation, scheduling, input/output control, and data management.
 - **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.
- For example, the entity's configuration management should reasonably ensure that all changes to application systems are fully tested and authorized.
- General control activities that are applicable to the entitywide 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.
- The auditor should develop more detailed audit steps based on the entity's specific software and control techniques, after consulting with the financial or performance auditor about audit objectives and significant areas of audit interest.

4.9 Testing Critical Control Points

- The auditor should evaluate the effectiveness of IS controls including system and/or application level controls related to each critical control point.
- The auditor should evaluate all potential ways in which the critical control point could be accessed. Generally, for each critical control point, this would include assessing controls related to the network, operating system, and infrastructure application components.
- For example, if a particular router was deemed to be a critical control point, the auditor generally should test controls related to the router itself (a network component), its operating system, and the infrastructure application that is used to manage the router. Access to any of these could lead to access to the control point.
- The auditor determines the appropriate scope of the IS controls audit, including the organizational entities to be addressed (e.g., entitywide, selected component(s), etc.); the breadth of the audit (e.g., overall conclusion on IS control effectiveness, review of a specific application or technology area, such as wireless network etc.); the types of IS controls to be tested namely general and/or business process application level controls to be tested.

4.10 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.
- 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 entitywide 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 entitywide 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.

4.11 Tests of General Controls at the Entitywide & System levels

- The auditor may test general controls through a combination of procedures, including observation, inquiry, inspection (which includes a review of documentation on systems and procedures), and reperformance using appropriate test software.
- If general controls at the entitywide and system levels are not effectively designed and
- operating as intended, the auditor will generally be unable to obtain satisfaction that business

- process application-level controls are effective.
- In such instances, the auditor should
 - (i) determine and document the nature and extent of risks resulting from ineffective general controls and
 - (ii) identify and test any manual controls that achieve the control objectives that the IS controls were to achieve.

If specific IS controls are designed to achieve the objectives, but are in fact ineffective because of poor general controls, testing would typically not be necessary, except to support findings.

4.12 Tests of General Controls at the Business Process – Application Level

- These business process application level general controls are referred to as Application Security (AS) controls.
- If general controls are not operating effectively within the business process application, business process application controls and user controls generally will be ineffective.
- If the IS controls audit is part of a financial or performance audit, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls with the audit team.
- The auditor should determine whether to proceed with the evaluation of business process application controls and user controls.

4.13 Tests of Business Process Application Controls & User Controls

- The auditor generally should perform tests of those business process application controls (business process, interface, data management), and user controls necessary to achieve the control objectives.
- If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks arising from information systems to:
 - identify the impact on the audit objectives,
 - design audit procedures, and
 - develop appropriate findings.
- The auditor considers whether manual controls achieve the control objectives, including manual controls that may mitigate weaknesses in IS controls.
- If IS controls are not likely to be effective and if manual controls do not achieve the control objectives, the auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives to develop recommendations for improving internal controls.

4.14 Appropriateness of Control Tests

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 can enable the auditor to gather a wide variety of information about the operating effectiveness of control techniques.
- **Questionnaires** can be used to obtain information on controls and how they are designed.
- **Observation** of the operation of controls can be a reliable source of evidence. observation provides evidence about controls only when the auditor was present.
- The auditor may **review documentation** of control policies and procedures. Review of documents will allow the auditors to understand and assess the design of controls.
- **Inspection** of approvals/reviews provides the auditor with evidence that management is performing appropriate control checks.
- **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 may provide evidence about the accuracy of processing. Computer-assisted audit techniques (CAAT) may be used to test data files to determine whether invalid transactions were identified and corrected by programmed controls.
- **Reperformance of the control** 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.

4.15 Multityear Testing Plans

- In circumstances where the auditor regularly performs IS controls audits of the entity (as is done, for example, for annual financial audits), the auditor may determine that a multiyear plan for performing IS controls audits is appropriate.
- Such a plan will cover relevant key agency applications, systems, and processing centres.
- These strategic plans should cover not more than a three year period and include the schedule and scope of assessments to be performed .
- The auditor typically evaluates these plans annually and adjusts them for the results of prior and current audits and significant changes in the IT environment, such as implementation of new systems.
- This concept allows the auditor to test computer-related general and business process application controls on a risk basis rather than testing every control every year.
- Under a multiyear testing plan, different controls are comprehensively tested each year, so that each significant general and business process control is selected for testing at least once during the multiyear period, which should not be more than 3 years.
- For example, a multiyear testing plan for an entity with five significant business process applications might include comprehensive tests of two or three applications annually, covering all applications in a two or three year period. For systems with high IS risk, the auditor generally should perform annual testing.
- Such multiyear testing plans are not appropriate in all situations.
 - they are **not appropriate for first-time audits**,
 - for audits where some significant business process applications or general controls have not been tested within a sufficiently recent period (no more than 3 years),
 - for audits of entities that do not have strong entitywide controls.

4.16 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., entitywide, 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, including
- 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.

4.17 Audit Reporting

4.17.1 Audit Objectives

- Determine which IS Control Techniques are Relevant to the Audit Objectives.
- For each Relevant IS Control Technique Determine Whether it is Suitably Designed to Achieve the Critical Activity and has been implemented.
- Perform Tests to Determine whether such Control Techniques are Operating Effectively Identify Potential Weaknesses in IS Controls and Consider Compensating Controls.

4.17.2 Report Audit Results

For this,

- Evaluate the Effects of Identified IS Control Weaknesses
- Financial Audits, Attestation Engagements, and Performance Audits
- Consider Other Audit Reporting Requirements and Related Reporting Responsibilities

4.17.3 Substantive Testing

- Where controls are determined not to be effective, substantive testing may be required to
- determine whether there is a material issue with the resulting financial information.
- In an IT audit, substantive testing is used to determine the accuracy of information being generated by
- a process or application.
- Audit tests are designed and conducted to verify the functional accuracy, efficiency, and control of the audit subject.
- The auditor selects and uses computer-aided audit tools to gather information and conduct the planned audit tests.
- appropriate selection of audit tools and their effective and accurate uses are essential to adequate audit testing. For example, if the performance of an application requires analysis, a computer program analyzer or instrumentation package would be an appropriate choice for use as an audit tool.
- In addition, if the audit staff uses an electronic document management system to capture their audit work (e.g., interviews, electronic documents, and schedules), how well does the auditor use this support tool?

4.17.4 Documenting Results

The final step involves evaluating the results of the work and preparing a report on the findings. The audit results should include the audit finding, conclusions, and recommendations.

4.17.5 Audit Findings

- Audit findings should be formally documented and include the process area audited, the objective of the process, the control objective, the results of the test of that control, and a recommendation in the case of a control deficiency.
- An audit finding form serves the purpose of documenting both control strengths and weaknesses and can be used to review the control issue with the responsible IT manager to agree on corrective action.
- The information can then be used to prepare the formal audit report and corrective action follows up.

4.17.6 Analysis

- Analysis is the most important factor in converting raw data into a finished product ready for inclusion in an audit report.
- Complete analysis of test information should provide the auditor with all the necessary information to write an audit report.
- Thorough analysis includes a clear understanding of the standards the cause of the deviation the control weakness that led to the deviation the materiality and exposure involved.
- Timely analysis enables the auditor to determine the causes and exposures of findings early in the audit.
- This gives the auditor time to conduct further testing when necessary and allows everyone more time to create corrective actions. It also promotes the better use of audit time by determining findings and exposures with a minimum of testing.
- One of the purposes of the current work paper guidelines is to provide documentation of this analysis process. Four analysis steps may be needed:
 - 1) Reexamine the standards and the facts
 - 2) Determine the cause of the deviation
 - 3) Determine the materiality and exposure of the deviation
 - 4) Determine possible recommendations for corrective action

4.17.7 Reexamination

- This is the most essential step in performing analysis.
- From this step, the auditor has the requisite data to make a judgment and formulate an opinion.
- The two factors under consideration are a standard (for comparison to the facts) and the facts (to compare to the standard).
- Step one reviews the standard, the facts, and whether a discrepancy actually exists between the two.

4.17.8 Standards Compliance

- Standards are the procedures, operating guidelines, regulations, good business practices, or other predefined methodologies that define how an operation under audit should function.
- The standard establishes the viewpoint used by the auditor to evaluate test information.

- Standards should be identified and evaluated at the beginning of the audit, and decisions on the appropriateness of standards should be addressed at the time the audit tests are created.
- Performance of the audit may give the auditor additional data to use in developing more appropriate standards.
- The standard used must be clearly understood by the auditor and there must be sufficient confidence that the correct standard is used. Although the standard is a written, published procedure, it may be outdated, redundant, or not appropriate.
- Using the wrong standard can lead to incorrect or incomplete findings. Critical evaluation of a standard can also lead to the identification of inefficient practices.

Four situations may occur while evaluating standards:

- No standard exists either explicitly or implicitly (this may imply a high degree of risk since no standard is present to guide how a function should perform).
- standard exists but is not formal (i.e., good business practices).
- The standard is formal and published but is redundant, not cost effective, no longer necessary, or no longer appropriate in some other manner.
- The standard is formal & is appropriate for evaluating the work performed.

4.17.9 Facts

- After reviewing the standard, the auditor must evaluate the gathered facts.
- The auditor should re-verify that deviations found are representative of the current control environment, have
- adequate support (photocopies or other hard evidence if possible), and, whenever possible,
- have an agreement with the audit client that deviations exist.

To ensure that findings are accurate and descriptive of the population, samples should be:

- Large enough to reflect the behavior of the population from which they were drawn.
- Representative of all types of individual members in the population, and representative of the current control practices (timely)
- If the sample fails to meet these characteristics, the deviation might not be the basis for a useful finding. To remedy this, it may be necessary to add to the sample or select an entirely new sample.

4.18 Verification

Finally, the auditor must again compare the findings to the reexamined standards to determine if a valid discrepancy still exists. If not, there is no issue and nothing to report. If the discrepancy is still apparent, then the analysis of the finding continues.

4.18.1 Cause

- Once the auditor is sure of his or her understanding of the standard, the next step is to identify the cause of the deviation.
- This is based on the reexamination of the standards involved.
- Determining the cause of a deviation is answering the who, what, why, where, and when of a particular asset, transaction, or event.
- The answers provide the raw material to help make judgments about the control system currently in place. Determining the cause helps identify the exposures and aids in formulating recommendations.

4.18.2 Exposure and Materiality

- This step examines the potential consequences of deviations.
- It answers the question, “Why does this need correction?” To answer this, the auditor must understand exposure and materiality.
- Exposure results from subjecting an asset to potential loss, harm, damage, theft, improper or inefficient use, or neglect. Assets are tangible (money, buildings, computers) or intangible (an account, data, good will), human or nonhuman.
- The risk is posed by people (theft, neglect, misuse) or by the environment (fire or weather). The degree of exposure is related to the proximity and severity of the risk.
- Proximity of the risk refers to how available the asset is to the person or environmental factor posing the risk.
- Severity of the risk refers to the potential amount of loss for each deviation.
- The greater the value of the asset exposed to risk and the closer the proximity to risk, the higher the potential loss for each deviation.
- Materiality is a qualitative judgment about whether a deviation’s frequency of occurring and degree of exposure are significant enough for the deviation to be corrected and included in the final audit report.

- Frequency refers to how often an event will occur. It is the combination of the likelihood an individual transaction will deviate from the standard and the total number of transactions.
- With this understanding of exposure and materiality, answers to the following questions help identify why corrections should take place.
- What happened or can happen (exposure) because of the identified deviation? Remember the big picture. Start with the deviation found and expand outward to get to the big picture. Be specific regarding what assets, transactions, and business entities are affected. Name the risk(s) that the asset or transaction is exposed to.
- How serious (materiality) is this consequence in terms of some standard of value (money, time, personal injury, or ill will)? Identify which standard(s) of value apply to the deviation analyzed. Make measurements of the severity of the exposure. If extrapolating, use a statistically sound method of estimation.
- How often (frequency) has the deviation occurred or is it expected to occur?
- Upon completing this step of analysis, the auditor should have a complete understanding of the standard used to measure the deviation.
- Why the standard is an appropriate measure (or model) of how an asset/transaction should be handled or controlled the substantial, significant, compelling audit evidence (proof) that a deviation has occurred.
- What caused the deviation to occur in terms of the department/person responsible for controlling the asset/transaction, what controls were not in place or not followed that allowed the deviation to occur, and the effectiveness of management's review process and corrective action over the area under audit the degree of exposure and the materiality of the deviation.
- Based on this, the auditor will have sufficient data to make an informed judgment about the state of controls and the efficiency of operations in the area under audit.

4.18.3 Conclusions

Conclusions are auditor opinions, based on documented evidence, that determine whether an audit subject area meets the audit objective. All conclusions must be based on factual data obtained and documented by the auditor as a result of audit activity. The degree to which the conclusions are supported by the evidence is a function of the amount of evidence secured by the auditor.

4.19 Concurrent or Continuous Audit & Embedded Audit Modules

Today, organizations produce information on a real-time, online basis. Real-time recordings needs real-time auditing to provide continuous assurance about the quality of the data, thus, continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.

Continuous auditing techniques use two bases for collecting audit evidence.

- o One is the use of embedded modules in the system to collect, process, and print audit evidence
- o The other is special audit records used to store the audit evidence collected.

4.19.1 Types of audit tools: Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available which could be used for selecting and testing data. Many audit tools are also available some of which are described below:

(i) Snapshots:

- **Tracing a transaction in a computerized system can be performed with the** help of snapshots or extended records.
- The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application.
- These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

The main areas to dwell upon while involving such a system are

- 1) to locate the snapshot points based on materiality of transactions
- 2) when the snapshot will be captured
- 3) the reporting system design and implementation to present data in a meaningful way.

(ii) Integrated Test Facility (ITF):

- **The ITF technique involves the creation of a dummy** entity in the application system files and the processing of audit test data against the 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.
- In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

Methods of Entering Test Data:

- **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, one to the application system master file record and one to the ITF dummy entity.
- Tagging live transactions as ITF transactions has the advantages of ease of use.
- 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.
- The auditors may also use test data that is specially prepared.
- Test transactions would be entered along with the production input into the application system.
- In this approach the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way.

Methods of Removing the Effects of ITF Transactions:

- 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 that might affect users.
- Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions.
- Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal.

(iii) System Control Audit Review File (SCARF): The system control audit review file (SCARF) technique 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 to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

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

- **Application system errors** - 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** - Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient 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.

(iv) Continuous and Intermittent 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:

- 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 enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit.

Continuous auditing has a number of potential benefits including:

- (1) 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;
- (2) reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;
- (3) 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
- (4) specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

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

- Timely, comprehensive and detailed auditing – Evidence would be available more timely and in a comprehensive manner.
- Surprise test capability – As evidences are collected from the system itself by using continuous audit techniques, 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.

The following are some of the disadvantages and limitations of the use of the continuous audit system:

- Auditors should be able to obtain resources required from the organisation 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 & 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.

4.20 Hardware Testing

Hardware testing may be done to the entire system against the Functional Requirement Specification(s) (FRS) and/or the System Requirement Specification (SRS). It is also intended to test up to and beyond the bounds defined in the software/hardware requirements specification(s).

4.20.1 Types of Hardware Testing

- 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

4.20.2 Review of Hardware

Review the capacity management procedures for hardware and performance evaluation procedures to determine:

- Whether they ensure continuous review of performance and capacity in terms of hardware, software, networks, user needs, business needs, management objectives and service levels.
- Whether historical data and analysis obtained from the Information System (IS) trouble logs, processing schedules, job accounting system reports, preventative maintenance schedules and reports are used in Information System (IS) management's hardware performance monitoring.
- Ensure that the technical management's decision to acquire or dispose off computing related hardware and software are indeed based on results of capacity planning models and workload forecasts tempered with good business judgment.

4.20.3 Review the hardware acquisition plan to determine:

- Whether the IS management has issued written policy statements regarding the acquisition of hardware.
- Whether the criteria for the acquisition of hardware are laid out & procedures and forms established to facilitate the acquisition approval process.
- Whether the hardware acquisition plan is in concurrence with the strategic business plan of management.
- Whether there is awareness of the budget constraints.
- Whether the requests for the acquisition of hardware are supported by cost benefit analysis.
- Whether all hardware are purchased through the IS purchasing department to take advantage of volume discounts or other quality benefits.
- Whether the environment is conducive and space is adequate to accommodate the current and new hardware.
- Whether IS management's hardware acquisition plan has taken into consideration technological obsolescence of the installed equipped, as well the new equipment in the acquisition plan.
- Whether there has been a consideration of lease expirations on current equipment.
- Whether documentation for hardware and software specifications, installation requirements, warranties, guarantees and likely lead-time associated with planned acquisitions is properly maintained.

4.20.4 Review the change in management controls for the following:

- Determine if changes to hardware configuration are planned and timely information is given to the individual responsible for scheduling.
- Determine whether the change schedules allow time for adequate installation and testing of new hardware.
- Verify that the operator documentation is appropriately updated to reflect changes in hardware.
- Select samples of hardware changes that have affected the scheduling of IS processing and determine if the plans for changes are being addressed in a timely manner.
- Ensure there is a cross-reference between the change and its cause, i.e. the problem.
- Ascertain whether the system programmers, application programmers and the IS staff have been informed of all hardware changes to ensure that changes are co-ordinated properly.

4.20.5 Review the preventive maintenance practices to evaluate the adequacy and the timeliness of preventive maintenance as under:

- Understand the frequency of scheduled preventive maintenance work performed by the hardware vendors and the in-house staff.
- Compare this frequency to hardware maintenance contract. Note any exceptions.
- Determine compliance with maintenance contractual agreements by examining maintenance log.
- Ascertain whether scheduled maintenance has had any adverse effect on the production schedule during peak season.
- Determine whether preventive maintenance logs are retained. Identify any abnormal hardware or software problems.
- Ensure that the hardware maintenance period commences on the same day as the warranty or guarantee expires. This prevents additional maintenance charges while in warranty period and also eliminates the time gap between the expiry of the warranty period and the commencement of maintenance.
- Verify whether the maintenance agreement has a maintenance call response time defined. It is the maximum time allowed between notification of a problem and the arrival of the maintenance staff.

4.21 Operating System Review

When testing operating software development, acquisition or maintenance, the following approach may be adopted:

4.21.1 Interview technical service manager, system programming manager, and other personnel regarding:

- Review and approval process of option selection
- Test procedures for software implementation
- Review and approval procedures for test results
- Implementation procedures
- Documentation requirements

4.21.2 Review cost/benefit analysis of system software procedures to determine they have addressed the following areas:

- Direct financial costs associated with the product
- Cost of product maintenance
- Hardware requirements and capacity of the product
- Training and technical support requirements
- Impact of the product on processing reliability
- Impact on data security
- Financial stability of the vendor's operations

4.21.3 Review controls over the installation of changed system software to determine the following:

- That all appropriate levels of software have been implemented and that predecessor updates have taken place
- System software changes are scheduled when they least impact IS processing.
- A written plan was established for testing changes to system software.
- Tests are being completed as planned.
- Problems encountered during testing were resolved and the changes were re-tested.
- Test procedures are adequate to provide reasonable assurance that changes applied to the system correct known problems and do not create new problems.
- Software will be identified before it is placed into the production environment.
- Fallback or restoration procedures are in place in case of production failure.

4.21.4 Review system software change controls to determine the following:

- Access to the libraries containing the system software is limited to individual(s) needing to have such access.
- Changes to the software must be adequately documented and tested prior to implementation.
- Software must be properly authorized prior to moving from the test environment to the production environment.

4.21.5 Review systems documentation specifically in the areas of:

- Installation control statements
- Parameter tables
- Exit definitions
- Activity logs/reports

4.21.6 Review and test systems software implementation to determine adequacy of controls in:

- Change procedures
- Authorization procedures
- Access security features
- Documentation requirements
- Documentation of system testing
- Audit trails
- Access controls over the software in production.

4.21.7 Review system software security for the following:

- Procedures have been established to restrict the ability to circumvent logical security access controls.
- Procedures have been established to limit access to the system interrupt capability.
- Existing physical and logical security provisions are adequate to restrict access to the master consoles.
- System software vendor-supplied installation passwords were changed at the time of installation.

4.21.8 Review database supported information system controls to determine the following:

- Access to shared data is appropriate.
- Data organization is appropriate.
- Adequate change procedures are utilized to ensure the integrity of the database management software.
- Integrity of the database management system's data dictionary is maintained.
- Data redundancy is minimized by the database management system where redundant data exists, appropriate cross-referencing is maintained within the system's data dictionary or other documentation.

4.22 Reviewing the Network

The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. The reviewer should identify the following:

- LAN topology and network design
- Significant LAN components (such as servers and modems)
- Network topology (including internal LAN configuration as well as interconnections to other LANs, WANs or public networks).
- LAN uses, including significant traffic types and main applications used over the network.
- LAN administrator
- Significant groups of LAN users

In addition, the reviewer should gain an understanding of the following:

- Functions performed by the LAN Administrator
- The company's division or department procedures and standards relating to network design support, naming conventions and data security.
- LAN transmission media and techniques, including bridges, routers and gateways.

To test physical security, a reviewer should perform the following:

- Inspect the LAN wiring closet and transmission wiring and verify they are physically secured.
- Observe the LAN file server computer and verify it is secured in a manner to reduce the risk of removal of components and the computer itself.

- Obtain a copy of the key logs for the file server room and the wiring closet, match the key logs to actual keys that have been issued and determine that all keys held are assigned to the appropriate people, for example, the LAN Administrator and support staff.
- Select a sample of keys held by people without authorised access to the LAN file server facility and wiring closet and determine that these keys do not permit access to these facilities.
- Look for LAN operating manuals and documentation not properly secured.

Environmental controls for LANs are similar to those considered in the mainframe environment. However, the equipment may not require as extensive atmospheric controls as a mainframe. The following should be considered:

- LAN file server equipment should be protected from the effects of static electricity (anti-static rug) and electrical surges (surge protector)
- Air conditioning and humidity control systems should be adequate to maintain temperatures within manufacturers' specifications.
- The LAN should be equipped with an uninterruptible power supply (UPS) that will allow the LAN to operate in case of minor power fluctuations or in case of a prolonged power outage.
- The LAN file server facility should be kept free of dust, smoke and other matter particularly food.
- Backup diskettes and tapes should be protected from environmental damage and the effects of magnetic fields.

To test environmental controls, a reviewer should visit the LAN file server facility and verify:

- Temperature and humidity are adequate.
- Static electricity guards are in place.
- Electric surge protectors are in place.
- Fire extinguishers are nearby.
- Observe the LAN file server facility, looking for food and beverage containers and tobacco products in the area and in the garbage cans.
- Observe the storage methods and media for backup and verify they are protected from environmental damage.

LAN logical security controls should be in place to restrict, identify and report authorized and unauthorized users of the LAN.

- Users should be required to have unique passwords and be required to change them periodically. Passwords should be encrypted and not displayed on the computer screen when entered.
- LAN user access should be based on written authorization, on a need to know/need to do basis. This should include documenting requests for adds, changes and detection of LAN logical access.
- A LAN workstation should be disabled automatically after a short period of inactivity.
- Remote access to the system supervisor should be prohibited. For maximum security an individual should only be able to logon to the supervisor account on the console terminal.
- This combination of physical security over consoles and logical security over the supervisor account provides for maximum protection against unauthorized access.
- All logon attempts to the supervisor account should be logged on in the computer system.
- The LAN supervisor should maintain up-to-date information about all communication lines connected to the outside.

To test logical security, a reviewer should interview the person responsible for maintaining

LAN security to ensure that person is:

- Aware of the risks associated with physical and logical access that must be minimized.
- Aware of the need to actively monitor logons and to account for employee changes.
- Knowledgeable in how to maintain and monitor access.

The reviewer should also perform the following interview users to access their awareness of management policies regarding LAN security and confidentiality.

- Evaluate a sample of LAN users' access /security profiles to ensure access is appropriate and authorized based on the individual's responsibilities.
- Review a sample of the security reports to:
- Ensure only authorized access is occurring.

- Verify timely and effective review of these reports is occurring and that there is evidence of the review.
- Look for unauthorized users. If found, determine the adequacy and timeliness of follow-up procedures
- Attempt to gain access using variety of unauthorized logon-IDs/passwords. Verify that access is denied and logged. Logon to and briefly use the LAN. Then, verify that access and use are properly recorded on the automated activity report.
- If the LAN logon session automatically logs off after a short period of inactivity, logon to the terminal and visually verify the automatic logoff feature.
- Visually search for written passwords in the general areas of the computer that utilize the LAN.
- If the LAN is connected to an outside source through a modem or dial-up network, attempt to gain access to the LAN through these telecommunications mediums using authorized and unauthorized management.
- Review a sample of LAN access change requests and determine if the appropriate management authorizes them and that the standard form has been utilized.

SELF EXAMINATION QUESTIONS

1. Describe various phases of IS Control Audit.
2. “An Auditor identifies control techniques and determines the effectiveness of controls at various levels”. Explain those levels in brief.
3. Briefly discuss components that an auditor should document in the testing phase.
4. Write a short note on ‘Audit Tools’.
5. Discuss advantages and disadvantages of Continuous Auditing.
6. What are the various types of hardware testing?
7. How would an operating system test be performed?
8. “Testing the LAN and its environment is a vital part of IS Audit”. Give an overview of the procedures to do so?
9. Describe the review methodology for hardware, in brief.

INTRODUCTION TO BASICS OF TESTING (REASONS FOR TESTING): It is a process used to identify the correctness, completeness and quality of developed computer software. Testing is a scientific process performed to determine whether the controls ensure the system design effectiveness as well as the implemented system controls operational effectiveness. Testing of Controls involves obtaining the population and conducting the compliance tests: 1. Substantive Testing 2. Compliance Testing	THE INFORMATION SYSTEM (IS) CONTROLS AUDIT INVOLVES THE FOLLOWING THREE PHASES: • Planning • Testing • Reporting	AUDIT PLANNING: • The auditor uses the concepts of materiality and significance to plan both effective and efficient audit procedures. • The auditor is not required to spend resources on items of little importance. • Some areas of the IS controls audit are not material or significant, and therefore warrant no audit attention. • Planning occurs throughout the audit as an iterative process.
AUDIT TESTING: • If the end-user applications are producing valid and accurate information. • Computer-assisted techniques could be used. • The auditor should test the ability and extent of error detection, correction and prevention. • The auditor should look for controls such as input balancing and record or hash totals. • The intensity/extent of the testing should be related to the sensitivity/importance of the application. • Testing should reveal any type of exposure of sensitive data.		MORE ON AUDIT TESTING: • The auditor must test the critical controls, processes, and apparent exposures. It calls for validation in several ways as follows: • Asking different personnel the same question. • Asking the same question in different ways. • Comparing checklist answers to work papers, programs, documentation and tests. • Comparing checklist answers to observations. • Conducting mini-studies of critical phases of the operation.

IS CONTROLS AUDIT PROCESS: The IS Control Audit process involves: • Understanding of an entity and its operations • Understanding of the structure of the entity's networks • Identifying key areas of audit interest • Assessing IS risk • Identifying critical control points • Understanding of IS controls	If the IS Controls Audit is performed as part of a Financial Audit: The auditor is to obtain an understanding of internal control over financial reporting sufficient to assessee the risk of material misstatement of the financial statements.	If the IS Controls Audit is performed as part of a Performance Audit: • The availability of evidence outside the information system to support the findings and conclusions. • The relationship of information systems controls to data reliability. • Assessing the effectiveness of information systems controls as an audit objective.
IDENTIFY KEY AREAS OF AUDIT INTEREST: The auditor should identify key areas of audit interest, which are those that are critical to achieving the audit objectives. For each key area of audit interest, the auditor should document: • The operational locations of each key system or file • Significant components of the associated hardware and software • Prior audit problems reported	The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls: • Identification of entitywide level controls • Identification of business process level controls for key applications • Management's plans and actions and milestones • Documented security plans • Documented risk assessments for relevant systems • Documented business continuity of operations plans and disaster recovery plans • Audit plan	PERFORMING INFORMATION SYSTEM CONTROLS AUDIT TESTS: • As audit evidence is obtained through performing control testing. • The auditor should periodically assess the audit evidence obtained to identify any revisions needed to the audit plan. • The auditor determines whether to perform tests of the operating effectiveness of such controls. • The auditor should determine whether it is possible and practicable to obtain sufficient, appropriate audit evidence.

The auditor identifies control techniques and determines the effectiveness of controls at each of the following levels: • Entity Wide or Component Level (General controls) • System Level (General controls) • Business Process Application Level (General Controls + Business) • Process Application Control	TESTS OF GENERAL CONTROLS AT THE ENTITYWIDE AND SYSTEM LEVELS: • Test general controls through a combination of procedures. • If general controls at the entitywide and system levels are not effectively designed and operating (i) determine extent of risks (ii) identify and test any manual controls • If manual controls do not achieve the control objectives, determine whether IS controls are designed to achieve the objectives. • If not, then the auditor should develop appropriate findings to improve internal control.	TESTS OF GENERAL CONTROLS AT THE BUSINESS PROCESS APPLICATION LEVEL: • Evaluate and test the effectiveness of general controls for those applications within which business process application controls are to be tested. • They are referred to as Application Security (AS) controls. • If general controls are not operating effectively, business process application controls will be ineffective. • If financial or performance audit, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls.
TESTS OF BUSINESS PROCESS APPLICATION CONTROLS AND USER CONTROLS: • If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks to: - identify the impact on the audit objectives - design audit procedures - develop appropriate findings. • Whether manual controls achieve the control objectives • The auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives.	TEST EFFECTIVENESS OF INFORMATION SYSTEM CONTROLS: • Conduct tests of relevant control techniques that are effective in design to determine their effectiveness. • To test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, then general controls at the business process application level, and concluding with tests at the business process application level. • Ineffective IS controls at each tier generally preclude effective controls at the subsequent tier. • Determine whether entitywide and system level general controls are effectively designed, implemented and operating effectively. • The auditor should conclude whether such controls are effectively designed and placed in operation.	

TESTING CRITICAL CONTROL POINTS: • The auditor should evaluate the effectiveness of IS controls. • The auditor should evaluate all potential ways in which the critical point could be accessed. • This would include assessing controls related to the network, operating system, and infrastructure application components. • Determine the appropriate scope of audit: (a) the organisational entities to be addressed (b) the breadth of the audit (c) the types of IS controls to be tested.	APPROPRIATENESS OF CONTROL TESTS: • Inquiries of IT and management personnel • Questionnaires can be used • Observation of the operation of controls • Review documentation of control policies and procedures • Inspection of approval • Analysis of system information obtained through system or specialized software • Data review and analysis of the output of the application processing • Reperformance of the control	Based on the results of controls tests, the auditor should determine whether the control techniques are operating effectively: • Controls that are not operating effectively are potential IS control weaknesses. • For each potential weakness, there are specific compensating controls to mitigate the potential weakness. • If the auditor could adequately mitigate the potential weakness, he should obtain evidence. • If it effectively mitigates the potential weakness, conclude that the control activity is achieved. • If the potential weakness is not effectively mitigated, the potential weakness is an actual weakness.
DOCUMENTATION OF CONTROL TESTING PHASE: • An understanding of the information systems • IS Control objectives and activities • By level and system sublevel, a description of control techniques used by the entity • By level and sublevel, specific tests performed • Documentation that describes the nature, timing, and extent of the tests • Evidence of the effective operation of the control techniques • Conclusions about the effectiveness of the entity's IS controls	AUDIT REPORTING: • Audit Objectives • Report Audit Results • Substantive Testing • Documenting Results • Audit Finding • Analysis • RE-examination • Standards Compliance • Facts • Verification • Cause • Exposure and Materiality	

CONCURRENT/CONTINUOUS AUDIT - Types of Audit Tools: (She Is Smart and Cool) • Snapshots • Integrated Test Facility (ITF) • System Control Audit Review File (SCARF): - Application system errors - Policy and procedural variances - System exception - Statistical sample - Snapshots and extended records - Performance measurement • Continuous and Intermittent Simulation (CIS)	Advantages • Timely, comprehensive and detailed auditing • Surprise test capability • Information to system staff on meeting of objectives • Training for new users	Disadvantages • Auditors should be able to obtain resources required from the organisation to support it. • More likely to be used if auditors are involved in the development work of a new application system. • Auditors need the knowledge and experience of working with computer systems to be able to use it effectively and efficiently. • It is more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high. • It won't be effective if the application system is not relatively stable.
REVIEW OF HARDWARE: • The capacity management procedures for hardware • The hardware acquisition plan • The change in management controls • The preventive maintenance practices	OPERATING SYSTEM REVIEW: • Interview technical and system programming manager • Review the feasibility study and selection process • Review cost/benefit analysis • Review controls over the installation • Review system software maintenance activities • Review system software change controls • Review systems documentation • Review software implementation	REVIEWING THE NETWORK: • LAN topology and network design • Significant LAN components • Network topology • LAN uses • LAN administrator • Significant groups of LAN users • Functions performed by the LAN Administrator • LAN transmission media and techniques, including bridges, routers and gateways

---***---