

Testing – General and Automated Controls

BASIC CONCEPTS

1. **Testing:** This is a process to identify the correctness, completeness, and quality of developed computer software.
2. **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.
3. **IS Controls Audit Process:** It 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.
4. **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.
5. **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.
6. **Audit Reporting:** After completing the testing phase, the auditor summarizes the results of the audit, draws conclusions on the individual and aggregate effect of identified IS control weaknesses on audit risk and audit objectives and reports the results of the audit. The auditor evaluates the individual and aggregate effect of all identified IS control weaknesses on the auditor's conclusions and the audit objectives. The auditor evaluates the effect of any weaknesses on the entity's ability to achieve each of the critical elements and on the risk of unauthorized access to key systems or files. Also, the auditor evaluates potential control dependencies.
7. **Types of Audit Tools:** Snapshots, Integrated Test facility, System Control Audit Review File (SCARF), Continuous and Intermittent Simulation (CIS)

4.2 Information Systems Control and Audit

7.1 Advantages of Continuous Auditing: Timely, comprehensive and detailed auditing, Surprise test capability, Information to system staff on meeting of objectives, Training for new users.

8. 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). This technique is of following types: 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

Question 1

Explain software testing and state its objectives.

Answer

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.

One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. 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.

Question 2

Write a short note on Audit Testing.

Answer

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. In addition, 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 determines what 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.

Question 3

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.

4.4 Information Systems Control and Audit

Answer

These factors are given as follows:

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

Question 4

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.

Answer

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 entitywide 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 entitywide 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.

Question 5

Explain the test effectiveness of Information System Controls.

Answer

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 entitywide 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 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.

Question 6

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.

Answer

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. 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 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.
- The auditor may review documentation of control policies 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 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 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.
- 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. 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

4.8 Information Systems Control and Audit

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.

Question 7

Explain the information developed in the testing phase that the auditor should document.

Answer

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.

Question 8

Describe the advantages and disadvantages of Continuous Auditing techniques in brief.

Answer

Continuous Auditing Technique: Continuous auditing enables auditors to shift their focus from the traditional 'transaction' audit to the 'system and operations' audit.

Advantages: 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. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.

- **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.

Disadvantages: The following are some of the disadvantages and limitations 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 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.

Question 9

What is SCARF? Explain in brief.

Answer

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.

Question 10

Which types of information may be collected by the auditors by using SCARF?

4.10 Information Systems Control and Audit

Answer

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.

Question 11

Write a short note on Continuous and Intermittent Simulation (CIS).

Answer

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 a 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.

Exercise

Question 1

Describe various concurrent audit tools?

Question 2

What are the advantages and disadvantages of continuous auditing?

Question 3

Describe in short the review methodology for hardware?

Question 4

What are the various kinds of hardware testing?

Question 5

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