

4. Testing – General and Automated Controls

Basics of 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 the controls design and the reliable results are done by one of the following methods

1. Substantive testing: This type of testing is used to substantiate the integrity of the actual processing.
2. Compliance testing: a Compliance test determines if controls are working as designed.

Audit Planning

In planning the IS controls audit, the auditor has uses the equivalent concepts of materiality and significance 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.

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 system that contains information that is sensitive or otherwise material or significant.

Planning occurs throughout the audit as an iterative process. However, planning activities are concentrated in planning phase, during which the objectives are to obtain an understanding of the entity and its operations, including its internal control, identify significant issues, assess risk, and design the nature, extent, and timing of audit procedures.

Audit Testing

The auditor must address many considerations that cover the nature, timing, and extent of testing. The auditor must devise an auditing plan and a testing methodology to determine whether the previously identified controls are effective. The auditor also tests whether the end-user application are producing valid and accurate information.

Secondly auditor may test the critical controls, process and apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.

IS Control 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 network,
- Identifying key areas of audit interests
- Assessing IS risk on a preliminary basis
- Identifying critical control points
- Obtaining a preliminary understanding of IS controls, and
- Performing other audit planning procedures.

The nature and extent of audit planning procedures varied 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 control 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 need to determine which audit procedures related to information system 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 these determinations.

- The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.
- The availability of evidence outside the information 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
- The relationship of information system 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 evidences about the reliability of data.
- Assessing the effectiveness of information systems controls as an audit objective: when assessing the effectiveness of information systems control is directly a part of audit objective, auditors should test information systems controls necessary to address the audit objectives.

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 areas of audit interest, the auditor should document relevant general support systems and major applications and files, including

- The operational locations of each key system or file
- Significant components of the associated hardware and software
- Other significant systems or system level resources that support the key areas of audit interest,
- Prior audit problems reported.

Documentation in Preliminary understanding of the design of IS control

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 if entity wide levels 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, including identification of control activities for which there are no or ineffective controls at the entity wide level and the related risks.

- Identification of business process level controls for key application identified as key areas of audit interest, determination of where those controls are implemented within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively
- Any internal or their-party information systems reviews, audits, or a specialized systems testing performed during the last years.
- Managements' plan of action and milestones, or their equivalent, that identify corrective actions planned to address known IS weakness and IS control weaknesses;
Status for 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 assessment for relevant systems
- System certification and accreditation documentation or equivalent for eleventh 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
- If IS controls are performed by service organization, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls.
- If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- Audit plan that adequately describes the objectives, scope, and methodology of the audit.
- Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

Performing information systems 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: control at this level consists of the entity-wide or component-wide processes designed to achieve the control activities. They are focused on how the entity or component manages IS related to each control activity.
- II. System Level: A control at the system level consists of processes for managing specific system resources related to either a general system or major application. These controls are more specific than those at the entity or component level and generally relate to a single type of technology. within the system level are the three further levels that auditor should assess which are as follows

- a. Network
- b. Operating System
- c. Infrastructure Application

III. Business process application level: control at this level consists of policies and procedures for controlling specific business processes. General control activities that are applicable to the entity wide and system levels, includes the general controls applied at the business process application level.

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 assessed. Generally, for each critical control point, this would include assessing controls related to the network, operating system, and infrastructure application components.

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 operations. 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 conducting with tests of business process application level.

Test of General Controls at the entity wide and System Levels

The auditor may test general controls through a combination of procedures, including observations, inquiry, inspection, and reperformance using appropriate test software. Although sampling is generally not used to test general controls, the auditor may use sampling to test certain controls such as those involving approvals.

However, if manual controls do not achieve the control objectives, the auditor should determine whether any specific IS controls are designed to achieve the objectives. If not, the auditor should develop appropriate findings principally to provide recommendations to improve internal control.

Test of General Control at the Business Process-Application level

If the auditor reaches a favorable conclusion on general controls at the entity wide and system levels, the auditor should evaluate and test the effectiveness of general controls for that application within which business process application controls or user controls are to be tested. These business process application level general controls are referred to as Application Security (AS) controls.

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 include the following

- Inquiries if 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.
- Questionnaire can be used to obtain information on control and how they are designed
- Observation of the operation of controls can be a reliable source of evidence
- The auditor may review documentation of control policies and procedures.
- 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 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.
- Reperformance of the control could be used to test the effectiveness of some programmed controls by reapplying the control through use of test data.

Documentation of control testing phase

- 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 and system sublevel, 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
- If a control is not achieved, any compensating control or other factors and the basis for determining whether they are effective;
- The auditor's conclusion about the effectiveness of the entity's IS control in achieving the control objective; and
- For each weakness, whether that 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.

Concurrent or continuous audit and embedded audit modules

Today, organization produces information on a real-time, online basis. Real time recordings need real-time auditing to provide continuous assurance about the quality of the data, thus, continuous auditing.

Errors in a computerized environment system are generated at high speed and the cost to correct and return programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least. Continuous auditing techniques use two bases for collecting audit evidence

1. Embedded Modules in the system to collect, process, and print audit evidence
2. Special audit records used to store the audit evidence collected.

Type of audit tools

Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidence may be built into the programs. Tools are discussed as below.

1. **Snapshots:** tracing a transaction in a computerized system can be performed with the help of snapshots or extended records.
2. **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.

Method for entering test data is also important. The transactions to be tested have to be tagged. The application system has to be programmed to recognize the tagged transaction and have them invoke two updates, one to the application master file record and one to the ITF dummy entity.

The auditor may also use test data that is specially prepared. Test transactions 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. The application system does not have to be modified to tag the ITF transaction.

Another important matter is dummy transaction may not show the output result in actual data so the application system may be programmed to recognize ITF transaction and to ignore them in terms of any processing that might affect user.

3. **System Control audit review File (SCARF):** the system control audit review file 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 in 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 type of information

- a. 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.
- b. Policy and Procedural Variance: Organization has to adhere to the policies, procedures and standard 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.
- c. System exception: SCARF can be used to monitor different types of application system exception. For example, salesperson might be given some leeway in the prices they charge to customers.
- d. 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.

- e. Snapshots and expended records: snapshots and extended records can be written into the SCARF file and printed when required.
 - f. Profiling Data: Auditors can use embedded audit routines to collect data to build profiles of system users.
 - g. Performance measurement: Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system
4. **Continuous and intermittent simulation (CIS):** this is a variation of the SCARF continuous audit techniques. This technique can be used to trap exception whenever the application system uses a database management system. During application system processing, CIS executed 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 DBMS.
 - 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 procedures
 - Exceptions identified by CIS are written to a exception log file.
 - The advantage of CIS is that it does not require notification to the application system and yet provides an online auditing capability.

Advantages and Disadvantage of Continuous Auditing

Benefits

1. Reducing the cost of the basic audit assignment by enabling auditors test a large sample of client's transaction and examine data faster and more efficiently than the manual testing required when auditing around the computer.
2. Reducing the amount of time and cost auditors traditionally spend on manual examination of transaction.
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 transaction and perform both tests of controls and substantive tests throughout the year on ongoing basis.

Advantages

1. Timely, Comprehensive and detailed auditing
2. Surprise test capacity
3. Information to system staff in meeting of objectives
4. Training for new users

Disadvantages

1. Auditor should be able to obtain resources required from the organization is support development, implementation, operation and maintenance of continuous audit techniques.
2. Continuous audit techniques more likely to be used if auditors are involved in the development work associated with a new application system
3. Auditors need the knowledge and experience of working with computer system to be able to use continuous audit techniques effectively and efficiency.

4. Continuous auditing techniques are more likely to be used where the audit trail is less visible and the cost of errors and irregularities are high.
5. Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.