300 Testing Phase

310 Overview of the Testing Phase

1. The objective of the testing phase is to determine whether information system (IS) controls are designed, implemented, and operating effectively to achieve relevant control objectives based on sufficient, appropriate evidence. The engagement team meets this objective for the IS controls assessment by performing the testing activities in figure 7.

Figure 7: Testing Phase Activities

A picture containing diagram

Description automatically generated

1. During the testing phase, the auditor builds on the foundation established in the planning phase to test the design, implementation, and operating effectiveness of IS controls. The concepts of significance, audit risk, and professional judgment assist the auditor in identifying relevant IS controls; determining the nature, timing, and extent of IS control tests; and evaluating the results, including the significance of any IS control deficiencies identified. See section 210 for discussion of these and other relevant concepts.

320 Identify Relevant IS Controls

1. When performing the IS controls assessment, the auditor identifies relevant IS controls—those user, application, and general controls that are suitably designed and necessary to achieve relevant control objectives and that the auditor plans to test for implementation and operating effectiveness. The auditor uses the FISCAM Framework as part of the process for identifying relevant IS controls. The illustrative controls presented in the FISCAM Framework are consistent with management requirements for information security and privacy control requirements presented in the National Institute of Standards and Technology’s (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*.[[1]](#footnote-1) These illustrative controls are examples of IS controls that may achieve the control objectives and, as such, assist the auditor in identifying and obtaining an understanding of the IS controls that the entity designed to achieve the relevant control objectives for each area of audit interest.
2. The auditor should obtain a sufficient understanding of the design of the entity’s IS controls that are likely to achieve the relevant control objectives for each area of audit interest, if implemented and operating effectively. The auditor primarily obtains this understanding through inquiries of management and personnel with knowledge of the IS controls as applied to the areas of audit interest, and the inspection of relevant documentation describing the design of such controls. The auditor may also observe personnel performing the IS controls. In determining whether such controls are suitably designed, the auditor considers the nature of the IS controls (i.e., the way they are applied) and the documentary evidence available to demonstrate the existence or performance of the controls.
3. Of the IS controls that are likely to achieve the relevant control objectives for each area of audit interest, the auditor should identify those controls that achieve the relevant control objectives and improve the efficiency of the auditor’s IS control tests. Such IS controls are considered relevant IS controls in the context of an IS controls assessment and will be tested for implementation and operating effectiveness. When determining whether an IS control (or combination of IS controls) will achieve an control objective, the auditor considers the extent to which the IS control relates to the control objective. The more direct the relationship between the IS control and the control objective (as it pertains to the area of audit interest), the more effective the control may be in achieving the objective.
4. If there are several IS controls that are likely to be effective in achieving a control objective, the auditor considers

* the extent to which an IS control achieves several control objectives and thereby reduces the number of controls that would ordinarily need to be tested,
* the time that would be required to test the IS control, and
* the extent to which control dependencies exist among IS controls that are necessary to achieve the relevant control objectives for each area of audit interest.

1. A control dependency exists when the effectiveness of a control depends on the effectiveness of other controls. When the auditor determines that the effective operation of a control depends on the effective operation of other controls, the auditor considers specific risks to the dependent control’s effective operation and performs tests of the other controls to determine whether they are suitably designed, properly implemented, and operating effectively to address the specific risks identified. Determining if an IS control is effective often includes assessing the effectiveness of other controls upon which the effectiveness of the IS control depends. For example, the effectiveness of a configurable control within application software will depend on the design of the application control, as well as related logical access and configuration management general controls designed to prevent or detect unauthorized changes to the control. In this example, the auditor would test the application control, as well as the related logical access and configuration management controls, to arrive at a conclusion regarding the effectiveness of the application control.
2. Without effective general controls, user and application controls may be rendered ineffective depending on the extent of control dependencies. Consequently, if certain general controls upon which specific user and application controls depend are not likely to be effective, the auditor may forgo further testing of such controls. In such cases, the auditor develops appropriate findings and considers the effect of control risks arising from ineffective user, application, and general controls on the nature, timing, and extent of further audit procedures.
3. When selecting general controls for testing, the auditor considers the level (i.e., business process, system, and entity) at which such controls are applied and whether it is more efficient to test certain general controls at the system or entity levels rather than the business process level, assuming they are equally effective. For example, if an entity-level general control for user identification and authentication is likely to achieve a control objective for the appropriate restriction of logical access for multiple areas of audit interest (whether at the business process level or system level), it may be more efficient to test the entity-level general control.
4. The auditor may implement a tiered approach to evaluating the effectiveness of IS controls, beginning with entity-level and system-level general controls, followed by business process-level general controls, and finishing with user and application controls. Such an approach may be efficient if (1) the auditor determined in the planning phase that general controls are not likely to be effective in achieving the relevant general control objectives for the areas of audit interest and (2) the auditor plans to forgo testing of certain user and application controls if such general control objectives are not achieved. However, for such an approach to be both efficient and effective, the auditor needs to have an adequate understanding of IS control dependencies (e.g., the extent to which the effectiveness of specific user and application controls depend on the effectiveness of certain general controls).

330 Determine the Nature, Timing, and Extent of IS Control Tests

1. When performing the IS controls assessment, the auditor establishes an efficient and effective approach for performing IS control tests to conclude on whether the entity’s IS controls are designed, implemented, and operating effectively to achieve the relevant control objectives for each area of audit interest. Once the auditor has identified relevant IS controls (section 320), the auditor determines the nature, timing, and extent of IS control tests. Control tests are a means of obtaining evidence on the implementation and operating effectiveness of relevant IS controls.
2. The nature, timing, and extent of IS control tests will vary by IS control.

* The nature of the IS control influences the type of evidence available to the auditor to demonstrate whether the control is implemented and operating effectively.
* The type of evidence available influences the nature of IS control tests that the auditor may perform, as well as the timing of such tests.
* The frequency at which the entity performs the IS control, along with the nature of the IS control test the auditor plans to perform, influences the timing and extent of IS control tests.

1. The auditor updates the detailed audit plans for each area of audit interest to document the nature, timing, and extent of IS control tests planned for the relevant IS controls. See section 350 for further discussion on documentation requirements for developing, updating, and completing detailed audit plans for each area of audit interest.

Determine the Nature, Timing, and Extent of IS Control Tests

1. The auditor should determine the nature, timing, and extent of IS control tests of relevant IS controls. Determinations regarding the nature, timing, and extent of IS control tests are interrelated, as the auditor’s determination of one will affect the auditor’s determination of the others. The nature, timing, and extent of IS control tests affect both the sufficiency and appropriateness of the evidence obtained through control testing.

Nature of IS Control Tests

1. The auditor should determine the nature of IS control tests—observation, inquiry, or inspection (including reperformance)—to be performed for each relevant IS control. This determination is based on the auditor’s understanding of the design of the IS control and the evidence available to demonstrate whether the control is properly implemented and operating effectively.
2. When determining the nature of IS control tests, the auditor considers the appropriateness—the measure of the quality of evidence that encompasses relevance, validity, and reliability—of the evidence available.

* Relevance refers to the extent to which evidence has a logical relationship with, and importance to, the issue being addressed.
* Validity refers to the extent to which evidence is a meaningful or reasonable basis for measuring what is being evaluated (i.e., the extent to which evidence represents what it is purported to represent).
* Reliability refers to the consistency of results when information is measured or tested and includes the concepts of being verifiable or supported (i.e., the extent to which records are present, sufficiently populated, and reflect the actual underlying information).

1. The source of the information to be used as evidence often affects the auditor’s consideration of its relevance and reliability. When using entity-produced information as evidence, the auditor should assess the appropriateness of the information prior to performing IS control tests. The auditor considers (1) steps taken by management or other auditors to obtain assurance over the reliability of the information and (2) testing management’s procedures to obtain assurance, performing direct testing of the information, or obtaining additional corroborating evidence. The nature, timing, and extent of the auditor’s procedures will depend on the nature of the information being used and the significance of the information to the auditor’s control tests. Using a risk-based approach, the auditor may determine the need to perform additional procedures if the auditor becomes aware of evidence that conflicts with that provided by management. In an overall assessment, the auditor documents how the auditor resolved situations involving conflicting evidence.
2. The following provides additional detail on the nature of IS control tests:

* Observation. The auditor conducts observation tests by observing entity personnel performing IS controls in the normal course of their duties. Observation generally provides highly reliable evidence that a control is properly applied when the auditor is there to observe it. However, it provides no evidence that the control was in operation at any other time. Consequently, the auditor generally supplements observation tests with corroborative evidence obtained from other tests (such as inquiry and inspection) about the operation of controls at other times.
* Inquiry. The auditor conducts inquiry tests by making either oral or written inquiries of entity personnel involved in the application of specific IS controls to determine what they do or how they perform a specific IS control. Such inquiries are typically open ended. Testimonial evidence obtained from inquiry alone is not sufficient; thus, the auditor supplements inquiry with other types of control tests—observation or inspection (which may include reperformance). Combining inquiry with inspection or reperformance typically provides more assurance than inquiry combined only with observation. The reliability of evidence obtained from inquiry depends on various factors, including the following:
  + The competence, experience, knowledge, independence, and integrity of the person of whom the inquiry was made. The reliability of evidence is enhanced when the person possesses these attributes.
  + Whether the evidence is general or specific. Evidence that is specific is usually more reliable than evidence that is general.
  + The extent of corroborative evidence obtained. Evidence obtained from several entity personnel is usually more reliable than evidence obtained from only one person.
  + Whether the evidence was provided orally or in writing. Generally, evidence provided in writing is more reliable than evidence provided orally.
* Inspection. The auditor conducts inspection tests by examining documents and records for evidence (such as implemented configuration settings, audit records for certain events that require logging, or the existence of initials or signatures on documents or records) that an IS control was performed. Business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals, as well as system design documentation may provide evidence of control design but do not provide evidence that controls are implemented and operating effectively. To use such documentation as part of the evidence of effective IS controls, the auditor obtains additional evidence to demonstrate that the IS controls have been implemented.

Inspection is generally a reliable source of audit evidence, and this type of test can be performed at any time since it involves the examination of documents and records. The auditor may also reperform the procedures or controls evidenced by the documents and records being inspected to determine if they were properly applied. Reperformance is the auditor’s independent execution of procedures or IS controls that were originally performed as part of the entity’s internal control. Reperformance tests can be performed manually or with computer-assisted audit techniques. These tests can be applied to user and application controls to determine whether such controls are designed, implemented, and operating effectively. The tests can also be applied to automated business processes that business process applications perform to verify the completeness, accuracy, and validity of the results these applications produce.

1. To test the implementation and operating effectiveness of relevant IS controls, the auditor uses professional judgment in determining and performing an appropriate mix of IS control tests to obtain sufficient, appropriate evidence to support their conclusions.
2. The auditor should perform other control tests in combination with inquiry to obtain sufficient, appropriate audit evidence regarding the implementation and operating effectiveness of relevant IS controls. Such other control tests allow the auditor to draw conclusions on how the IS control was applied at relevant times during the audit period; the consistency with which the IS control was applied; and by whom or by what means the IS control was applied, including, when applicable, whether the person performing the control possesses the necessary authority and competence to perform the control effectively.

Timing of IS Control Tests

1. The auditor should determine the timing of control tests to be performed for each relevant IS control. This determination is influenced by factors such as (1) the engagement type, (2) the audit period, (3) the overall timeline of the engagement, (4) the type of evidence available to the auditor to demonstrate whether the IS control is implemented and operating effectively, and (5) the nature of the test.

Extent of IS Control Tests

1. The auditor should determine the extent of IS control tests to be performed for each relevant IS control. The extent of IS control tests is the quantity of control testing to be performed for a specific IS control. This determination is influenced by the nature of the IS control test, as well as the frequency at which the entity performs the IS control. Additionally, this determination will influence whether the auditor will use statistical sampling or nonstatistical selection methods to determine whether the IS control is operating effectively.
2. The frequency at which the entity performs an IS control will inform the auditor’s determination regarding the sufficiency of audit evidence obtained from a given IS control test. Generally, IS controls that are performed more frequently will require a greater extent of testing than those that are performed infrequently. For IS controls that do not operate frequently, such as those that operate only once or twice a year (e.g., periodic access recertification), the auditor may determine that it is necessary to test all the items in the population (i.e., all instances in which the IS control was performed during the audit period).
3. For IS controls that do not leave documentary evidence of existence or performance, the auditor may test their effectiveness through inquiry and observation. However, the appropriate extent of inquiry and observation is a matter of professional judgment. For application controls, the auditor may observe one or a few instances in which the IS control is performed. The auditor may also verify the completeness, accuracy, and validity of the results the applications produced. However, the auditor’s determination regarding the implementation and operating effectiveness of application controls will partially depend on the auditor’s conclusions on the effectiveness of the general controls upon which the application controls depend.
4. The auditor also considers whether circumstances that warrant the performance of an IS control occurred during the audit period. For example, certain IS controls for managing changes to entity information systems need not be tested for operating effectiveness if no relevant changes were made during the audit period. When such circumstances arise, the auditor corroborates the information obtained to confirm that the IS control was not applicable for the audit period.
5. When planning additional IS control tests to obtain sufficient, appropriate evidence regarding the operating effectiveness of IS controls, the auditor may test all instances (the population of items) or some instances in which the IS control was performed during the audit period. If the auditor does not plan to test all the items within the population, the auditor should use statistical sampling (items intended to be representative of and statistically projected to the population of items) or nonstatistical selection (items not intended to be representative of or statistically projectable to the population of items) to identify items for control testing.

Statistical Sampling for IS Control Tests

1. The auditor should use attribute sampling and select items either through simple random selection (SRS) or through systematic random selection (SYS), when using statistical sampling to identify items within a population for control testing. SRS is a selection technique in which every combination of sampling units has the same probability of being selected as every other combination of the same number of sampling units—resulting in every member of the population having an equal probability of selection.[[2]](#footnote-2) SYS is a selection technique in which a starting point within the first uniform interval—determined by dividing the number of units in the population by the sample size—is randomly selected and then an item is selected at each uniform interval from the starting point throughout the population. Attribute sampling achieves the objective of selecting items for the sample in such a way that the auditor may reasonably expect the sample to be representative of the relevant population and likely to provide the auditor with a reasonable basis for conclusions about the population.
2. When planning IS control tests involving statistical sampling, the auditor should determine a sample size sufficient to reduce sampling risk to an acceptably low level. Sampling risk is the risk that the auditor’s conclusions based on a sample may be different from the conclusion if the entire population were subjected to the same audit procedure. For tests of controls, sampling risk is the risk of assessing control risk either too low or too high. For sampling control tests, the auditor should determine

* the objectives of the control test (including what constitutes a deviation),
* the population (including sampling unit and time frame),
* the method of selecting the statistical sample (SRS or SYS), and
* the sample design and resulting sample size (paragraph 330.24).

1. The auditor should define the objectives of each IS control test, including what constitutes a deviation, when using statistical sampling for IS control testing. Generally, the primary objective of a control test involving statistical sampling is to determine whether a specific control is operating effectively. When control tests involving statistical sampling are used, the auditor evaluates operating effectiveness in terms of the rate of deviations in units or dollars from prescribed controls. To perform such an evaluation, the auditor first defines (1) the controls to be tested and (2) what constitutes an error, exception, or control failure for each control. Control deviations are defined in terms of controls not followed.
2. The auditor should define the population by identifying the whole set of items on which the auditor needs to reach a conclusion and from which the statistical sample will be drawn. This includes

* describing the population and its source;
* conducting data reliability tests, such as verifying extraction parameters to determine whether the population that management officials provided is complete, accurate, and valid;
* identifying the evidence (e.g., source documents or transaction documents demonstrating whether the control is operating effectively) to be tested; and
* determining the period covered by the test.

1. The auditor should determine whether the population needs to be stratified prior to sampling if multiple organizational units or locations are involved in performing the same IS controls. Stratification is the process of dividing a population into subpopulations, each of which is a group of individual items, or sampling units, that have similar characteristics. In making this determination, the auditor considers such factors as

* the extent of uniformity of the controls and their performance across organizational units or locations,
* whether the organizational units or locations have the authority to make significant changes to the controls or how they are performed at the local level,
* the amount and nature of centralized oversight or control over the organizational units or locations with respect to the controls and their performance, and
* whether there could be a need for separate conclusions for each organizational unit or location.

1. The auditor may use statistical sampling to test the operating effectiveness of certain general controls, such as those involving approvals. For example, the auditor may use statistical sampling to test management approvals related to the entity’s change management process. When multiple business process applications and information systems have been identified as areas of audit interest, the auditor may use (1) one population of changes for all or several business process applications or information systems or (2) separate populations of changes for each business process application or information system. However, the auditor will only be able to use one population of changes for multiple business process applications and information systems if the change management process and corresponding approvals are consistent across such applications and systems. In making this decision, the auditor may evaluate such factors as

* the extent of uniformity of the controls and how such is evidenced for each business process application or information system,
* whether the business process application or information system owners (or those responsible for performing the controls) can make significant changes to the controls or their evidence,
* the amount and nature of centralized oversight of the change management process, and
* whether there could be a need for separate conclusions for each business process application or information system.

1. If the auditor concludes that the separate populations of changes will be used for each business process application or information system, the auditor selects separate samples for each population and evaluates the results of each sample separately.
2. When planning sampling control tests, the auditor should determine a sample size to obtain sufficient, appropriate audit evidence about the operating effectiveness of relevant IS controls. The auditor uses professional judgment in determining the number of items to select and the method used to select them. To determine sample size, the auditor uses professional judgment to determine four factors:

* confidence level,
* tolerable rate of deviation of the population to be tested (maximum rate of deviations from the prescribed control that the auditor is willing to accept without altering the preliminary assessment of control risk),
* expected rate of deviation of the population to be tested (expected error rate), and
* the desired level of assurance (complement of risk overreliance) that the tolerable rate of deviation is not exceeded by the actual rate of deviation in the population—the auditor may decide the desired level of assurance based on the extent to which the auditor’s risk assessment considers relevant controls.

1. Once the auditor determines these factors, the auditor may use automated audit tools to determine sample size and to select samples for testing.

Nonstatistical Selection for IS Control Tests

1. Performing IS control tests that involve nonstatistical selection may provide sufficient evidence, along with other sources of evidence, that an IS control is operating effectively during the audit period. It may also be the most efficient way to test the control. For example, some IS controls may operate biweekly or weekly. For these controls, statistical sampling may not be efficient or even feasible given the small number of items in the population from which the auditor will select the sample. For these controls that operate less frequently, the effect of other sources of evidence is often greater than the effect for more frequent operating controls.
2. Table 7 provides guidance on the number of items to select when testing small populations associated with less frequently performed IS controls. For larger populations, such as IS controls that operate daily, the auditor performs statistical sampling to obtain evidence of control effectiveness.

Table 7: Testing Small Populations

|  |  |  |
| --- | --- | --- |
| Control frequency and population size | | Number of items to test |
| Quarterly | (4) | 2 |
| Monthly | (12) | 2-4 |
| Semimonthly | (24) | 3-8 |
| Weekly | (52) | 5-9 |

Source: GAO. |  GAO-24-107278

1. In nonstatistical selection, the auditor selects items for control testing based on the auditor’s judgment. The auditor tests the selected items using any type of test or combination of tests (i.e., observation, inquiry, inspection, or a combination of these—although inquiry alone is not sufficient). For example, the auditor may determine that inquiries of entity personnel regarding the specific procedures performed in a control and inspection of documents evidencing performance of those procedures together provide sufficient evidence of the control’s operating effectiveness.

Automated Audit Tools

1. Automated audit tools (sometimes referred to as computer-assisted audit techniques, or CAATs) can be used to gather, or assist in gathering, audit evidence and to test the effectiveness of controls. For example, auditors can leverage data analytics tools, such as various programming languages and specialized audit software, in testing IS controls where discrete data are available. The advantage of using automated audit tools in control testing is that it is possible to test every item in a population to determine whether there were any control deviations.
2. To use automated audit tools, the entity needs to provide access to all required resources, including data. Additionally, obtaining such access may require significant collaboration between the auditor and the entity to reach agreement on the data the entity will provide and the resources the auditor will use.
3. If the auditor plans to use automated audit tools, the auditor should understand the following for each:

* what are the associated risks,
* when to use the tool,
* how to operate the tool,
* how to analyze the data, and
* how to interpret the results.

1. Through a technical review, the auditor should verify that

* the use and operation of the automated audit tool is appropriate,
* the results the tool produces are complete and accurate, and
* any conclusions are supported.

1. There are many different types of automated audit tools. The auditor may decide to use multiple tools depending on the circumstances, including

* commercial software, such as Microsoft Excel, CaseWare IDEA Data Analysis Software, and SAS Viya, for performing data analytics, statistical modeling, and so forth on data imported from entity files;
* programming languages, such as Python and R, for writing programs for performing data mining, data analytics, statistical modeling, and so forth;
* generalized audit software, such as data extraction tools and reporting facilities, for querying and extracting information from the entity’s information system;
* specialized audit software for performing specific tasks in specific circumstances, such as comparing source and object code, analyzing unexecuted code, and generating test data;
* an embedded audit module within the client’s software for replicating a specific aspect of a control procedure or for recording details of certain transactions in a file accessible only to the auditor;
* a test facility integrated into the client’s software for processing the auditor’s test data in the same way that the client’s live data are processed and for verifying the results are correct;
* parallel simulation for processing the client’s live data using an identical copy of the client’s software for which the auditor has separate control and performs program code analysis to ensure that the processing is identical to that of the client’s operational software;
* program code analysis for validating that the instructions given to the computer are the same instructions that the auditor has previously identified when reviewing the systems documentation; and
* a tool for processing test data that the auditor prepared using the current production version of the client’s software but separate from the client’s normal input data.

Considerations for Testing IS Controls That Service Organizations Perform

1. When the auditor identifies relevant IS controls that service organizations perform, the auditor obtains evidence about the implementation and operating effectiveness of such controls through one or more of the following procedures:

* obtaining and inspecting a service organization report covering the appropriate period of time, if available;
* performing appropriate tests of controls at the service organization; and
* using another auditor to perform tests of controls at the service organization on behalf of the auditor.

1. The service organization may use an independent auditor to prepare a service organization report. User entities of service organizations and their auditors may use this report to understand and obtain evidence about the service organization’s controls. There are a variety of service organization reports prepared to provide assurance on the design, implementation, and operating effectiveness of various controls. In the context of an IS controls assessment performed using FISCAM, the auditor will generally use service organization reports that focus on controls relevant to the entity’s internal control over financial reporting.[[3]](#footnote-3) These reports provide assurance over the design of internal controls at a point in time (type 1 report) or the design and operating effectiveness of internal controls over a period of time (type 2 report), including IS controls, based on the service organization’s description of controls relevant to the service being provided.[[4]](#footnote-4) A service organization report may be intended to satisfy the needs of multiple auditors conducting engagements with varying objectives. As a result, the service auditor’s report may or may not address the relevant control objectives identified by the auditor. It is the auditor’s responsibility to identify and evaluate the results of relevant tests of controls to determine whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of the relevant IS controls the service organization performs.
2. If the auditor plans to use a service organization report as evidence that IS controls that a service organization performs are designed, implemented, and operating effectively, the auditor should obtain a report on management’s description of the service organization’s system and the suitability of the design and operating effectiveness of internal controls over a period (type 2 report). The auditor should determine whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of IS controls to support the auditor’s conclusions by

* assessing the adequacy of the standards under which the service auditor’s report was issued;
* evaluating whether the report is for a period that is appropriate for the auditor’s purpose;
* evaluating the adequacy of the relevant IS controls that the service organization performed, as described in the service auditor’s report, to achieve relevant control objectives and the relevance and adequacy of the service auditor’s tests of such controls;
* evaluating the adequacy of the period covered by the service auditor’s tests of the IS controls the service organization performed and the time elapsed since performance of such tests;
* evaluating whether the results of the service auditor’s tests of the IS controls the service organization performed, as described in the service auditor’s report, provide sufficient, appropriate evidence to support the auditor’s conclusions;
* determining whether complementary user-entity controls that the service organization identified as necessary to support the effectiveness of relevant IS controls the service organization performed are designed, implemented, and operating effectively;[[5]](#footnote-5) and
* if applicable, evaluating the adequacy of any IS controls a subservice organization performed that are necessary to support the effectiveness of relevant IS controls the service organization performed.

1. For federal financial audits, the auditor should refer to *Financial Audit Manual* (FAM) 640, Entities Using a Service Organization, when inspecting a service organization report to obtain evidence about the design, implementation, and operating effectiveness of IS controls that a service organization performs. In such cases, the auditor uses FAM 640A, Service Organization Type 2 Assessment Tool, when determining whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of relevant IS controls.
2. For performance audits, the auditor may adapt and apply the FAM Service Organization Type 2 Assessment Tool (FAM 640A) when determining whether a service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of relevant IS controls.
3. There may be instances in which a service organization uses another service organization (subservice organization) to perform services that are likely to be relevant to the user entity’s internal control and the auditor’s assessment of IS controls. The service organization report will describe either of the following:

* Inclusive method: Method of addressing the services a subservice organization provides whereby management’s description of the service organization’s system includes a description of the nature of the services that the subservice organization provided as well as the subservice organization’s relevant control objectives and related controls.
* Carve-out method: Method of addressing the services a subservice organization provides whereby management’s description of the service organization’s system identifies the nature of the services that the subservice organization performed and excludes from the descriptions, and from the scope of the service auditor’s engagement, the subservice organization’s relevant control objectives and related controls.

1. If the auditor plans to use a type 2 report that excludes the services a subservice organization performs and those services are relevant to the auditor’s assessment of IS controls, the auditor should apply the same testing procedures noted in this section to the services that the subservice organization provides.
2. If the auditor determines that additional evidence about the operating effectiveness of IS controls that service organization (or subservice organization) performs is required, the auditor may obtain additional evidence by

* contacting the service organization, through management, to obtain specific information;
* evaluating procedures, including the results of such procedures, that management performed to (1) hold the service organization accountable for its assigned internal control responsibilities and (2) authorize the operation (or use) of the information systems the service organization operates on behalf of the entity;
* requesting that a service auditor be engaged to perform procedures that will supply the necessary information about IS controls that the service organization performs; and
* visiting the service organization and performing the IS control tests necessary to obtain sufficient, appropriate evidence to determine the effectiveness of IS controls the service organization performs.

340 Perform IS Control Tests and Evaluate the Results, Including the Significance of IS Control Deficiencies

1. Once the auditor has determined the nature, timing, and extent of IS control tests and has updated the detailed audit plans for each area of audit interest to document such tests planned for the relevant IS controls, the auditor performs the tests. The auditor performs IS control tests using suitable criteria and evaluates the results, including the significance of any IS control deficiencies identified.
2. In evaluating the results, the auditor performs an overall assessment of the evidence obtained and determines whether the audit procedures performed are adequate to reduce audit risk to an acceptably low level. In determining whether relevant IS controls are designed, implemented, and operating effectively to achieve the relevant control objectives for an area of audit interest, the auditor considers whether the evidence obtained supports the final assessment of IS control risk for the area of audit interest. The auditor communicates the results to the overall engagement auditor, if appropriate. The auditor prepares a written results memo (sometimes referred to as a summary memo) for the IS controls assessment to document the overall assessment of the collective evidence obtained and the auditor’s final determinations regarding IS control risk and audit risk (section 350).
3. For federal financial audits, the auditor identifies control objectives that, if achieved, would address the risks of material misstatement on the SCE worksheet for which IS controls are identified. Additionally, the auditor is required to perform sufficient tests of IS controls that have been suitably designed and properly implemented to achieve the relevant control objectives and support a low assessed level of control risk for the financial audit.

Perform IS Control Testing

1. The auditor should perform control tests of the relevant IS controls using suitable criteria. Criteria may include the statutes, regulations, executive orders, implementing guidance, directives, policies, contracts, grant agreements, standards, measures, expected performance, defined business practices, and defined benchmarks against which performance of the selected control is compared or evaluated. See section 140 for further discussion on criteria. The evidence obtained through the auditor’s IS control tests is included in the auditor’s overall assessment of the collective evidence obtained throughout the IS controls assessment.
2. For federal financial audits, the auditor should comply with requirements for documenting IS controls that are included on the specific control evaluation worksheet as discussed in FAM 390, Documentation (Internal Control Phase).

Determine Whether Relevant Control Objectives Are Achieved

1. The auditor should evaluate the results of control tests to determine whether relevant IS controls are implemented and operating effectively to achieve the relevant control objectives for each area of audit interest. Identified control deviations related to the design, implementation, or operating effectiveness of relevant IS controls may prevent achieving relevant control objectives and may result in IS control deficiencies. A **control deviation** is an instance in which a control differs, or deviates, from the auditor’s expectations regarding design, implementation, or operating effectiveness. A **control deficiency** is a condition when the design, implementation, or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, errors in information processing on a timely basis.

* A deficiency in design exists when (1) a control necessary to meet the control objective is missing or (2) an existing control is not suitably designed so that even if the control operates as designed the control objective would not be met.
* A deficiency in implementation exists when a suitably designed control has not been implemented or has not been implemented as designed.
* A deficiency in operation exists when a suitably designed and properly implemented control does not consistently operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

1. With assistance from the entity, the auditor investigates and obtains an understanding of the reasons for any IS control deviations. For those IS control deviations that are not resolved through entity-provided additional evidence, the auditor should communicate to management, in writing and on a timely basis, the details of the potential IS control deficiency identified. The auditor should communicate potential IS control deficiencies to the entity in sufficient detail for management to consider whether there are additional factors or compensating controls that are relevant to the auditor’s determination of whether (1) a control deficiency exists and (2) the related control objective is achieved.
2. The auditor should determine whether there are specific compensating controls that could mitigate a potential IS control deficiency. If the auditor believes that compensating controls could adequately mitigate a potential IS control deficiency and achieve the related control objective, the auditor should obtain evidence that the compensating controls are designed, implemented, and operating effectively. If the compensating controls effectively mitigate the potential IS control deficiency, the auditor can conclude that the control objective is achieved. Nonetheless, the auditor communicates any control deviations identified to the entity. If the potential IS control deficiency is not effectively mitigated, the auditor will generally conclude that it is an IS control deficiency and document the elements of a finding—criteria, condition, cause, and effect. The auditor may also conclude and document the elements of a finding for certain potential IS control deficiencies that, despite being effectively mitigated, represent IS deficiencies. For example, the auditor may determine that a specific IS control selected for testing is not operating effectively. Although compensating controls mitigate the effect of this control failure, the auditor may elect to develop the elements of a finding to facilitate communication with management and to enable management to develop appropriate corrective actions.
3. The auditor should communicate to management the criteria, condition, cause, and effect of the IS control deficiencies identified through the IS controls assessment. These items may serve as the basis for recommendations for corrective actions, which are discussed in further detail in paragraphs 430.11 through 430.16.

Evaluate the Significance of IS Control Deficiencies and Their Effect on IS Control Risk

1. The auditor should evaluate and document the significance of identified IS control deficiencies. In determining whether, individually or in combination, IS control deficiencies are significant in the context of the engagement objectives, the auditor considers their effect on IS control risk for each area of audit interest, as well as their impact on the effectiveness of relevant business process controls.
2. The auditor should reassess, based on the audit procedures performed and the collective evidence obtained, the level of IS control risk for each area of audit interest. For each area of audit interest, the auditor assesses final IS control risk at one of three levels:

* Low. The auditor concludes that IS controls adequately mitigate risk factors to achieve relevant control objectives.
* Moderate. The auditor concludes that IS controls more likely than not adequately mitigate risk factors to achieve relevant control objectives.
* High. The auditor concludes that IS controls do not adequately mitigate risk factors and do not achieve relevant control objectives.

If IS control risk is assessed at moderate or high for one or more of the areas of audit interest, the auditor should determine the impact of the underlying control deficiencies on the effectiveness of relevant business process controls.

1. For federal financial audits, if IS control risk is assessed at moderate or high for one or more of the areas of audit interest, the auditor determines the impact of the underlying control deficiencies on the effectiveness of IS controls identified on the SCE worksheet. In determining whether the IS controls identified on the SCE worksheet are operating effectively to address the identified risks of material misstatement, the auditor considers the operating effectiveness of business process controls and indirect general controls. The auditor communicates these determinations to the financial auditor to assist them in completing the SCE worksheet. See section 430 for further discussion on reporting deficiencies.
2. For examination-level attestation engagements, the reassessment of IS control risk for each area of audit interest and determination of the impact of the underlying control deficiencies on the effectiveness of relevant business process controls forms the basis of the auditor’s determination whether, individually or in combination, the IS control deficiencies are material weaknesses or significant deficiencies.[[6]](#footnote-6) See section 430 for further discussion on reporting deficiencies.
3. For performance audits, this reassessment of IS control risk for each area of audit interest and determination of the impact of the underlying control deficiencies on the effectiveness of relevant business process controls forms the basis of the auditor’s determination whether, individually or in combination, the IS control deficiencies are significant in the context of the control objectives. In addition, as part of this determination, the auditor considers whether management had previously detected or was otherwise aware of auditor-identified IS control deficiencies. See section 430 for further discussion on reporting deficiencies.

Assess Sufficiency and Appropriateness of Evidence and Level of Audit Risk

1. The auditor should perform an overall assessment of the collective evidence obtained throughout the IS controls assessment to support the auditor’s findings and conclusions. The auditor considers whether sufficient, appropriate evidence has been obtained to achieve the engagement objectives and report on the results. Sufficiency and appropriateness of evidence are relative concepts, which may be thought of as a continuum rather than as absolutes. Sufficiency and appropriateness are evaluated in the context of the related findings and conclusions. For example, even though the auditor may identify some limitations or uncertainties about the sufficiency or appropriateness of some of the evidence, the auditor may nonetheless determine that in total there is sufficient, appropriate evidence to support the findings and conclusions.
2. The auditor should determine whether the audit procedures performed throughout the IS controls assessment are adequate to reduce audit risk to an acceptably low level. The auditor’s overall assessment of the collective evidence obtained and final assessment of IS control risk inform the auditor’s conclusion regarding audit risk.

350 Prepare Testing Phase Documentation

1. The auditor should prepare testing phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand from the audit documentation the nature, timing, and extent of audit procedures performed and the results of the IS controls assessment, including the significance of any IS control deficiencies identified.
2. The auditor should prepare audit documentation containing sufficient, appropriate evidence for the auditor’s findings, conclusions, and recommendations before the report is issued.

Completed Audit Plan, Results Memo, and Detailed Audit Plans

1. The auditor should complete the written audit plan for the IS controls assessment to reflect the results of the audit procedures performed.
2. The auditor should prepare a written results memo (sometimes referred to as a summary memo) for the IS controls assessment that includes a description of the overall assessment of the collective evidence obtained and the auditor’s final determinations regarding IS control risk and audit risk.
3. The auditor should update and complete detailed audit plans to document the approach for testing controls for the relevant control objectives for each area of audit interest.
4. Detailed audit plans for each area of audit interest

* identify the area of audit interest;
* explain the relationship of the area of audit interest to the significant business processes and any other areas of audit interest, as applicable;
* identify the relevant control objectives;
* identify the relevant IS controls selected for testing that are likely to achieve the relevant control objectives;
* describe the nature, timing, and extent of IS control tests for each relevant IS control;
* document the results of completed IS control tests; and
* provide links to supporting documentation.

1. In such cases where certain IS controls support the achievement of multiple control objectives for more than one area of audit interest, the auditor may include references to separate detailed audit plans for such controls. Including such references minimizes redundancy in the audit documentation. Control tests for such controls need only be performed once and linked to the detailed audit plans developed for each applicable area of audit interest.

Sampling Plans

1. When performing IS control tests involving statistical sampling, the auditor should prepare written sampling plans that include

* the objectives of each test (including what constitutes a deviation),
* the population (including sampling unit and time frame),
* the method of selecting the sample (SRS or SYS), and
* the sample design and resulting sample size.

Technical Reviews

1. When IS control tests involving automated audit tools are performed, the auditor should prepare relevant audit documentation in sufficient detail to enable a technical review by audit staff independent of the preparer to determine that

* the use and operation of the automated audit tool is appropriate,
* the automated audit tool’s results are complete and accurate, and
* any conclusions are supported.

FISCAM Assessment Completion Checklist

1. The auditor should complete the testing phase portion of the FISCAM assessment completion checklist. See appendix 600B.

1. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and* *Organizations*, Special Publication 800-53, rev. 5 (Gaithersburg, Md.: September 2020). [↑](#footnote-ref-1)
2. American Institute of Certified Public Accountants, *Audit Guide: Audit Sampling*, ed. 2 (Hoboken, N.J.: Wiley 2019). [↑](#footnote-ref-2)
3. These reports are issued under the American Institute of Certified Public Accountants’ (AICPA) Standards for Attestation Engagements [Clarified] (AT-C) 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting. There are other types of reports on service organizations that may be available, including reports on controls at a service organization other than those likely to be relevant to user entities’ internal control over financial reporting (for example, controls that are relevant to cybersecurity; supply chain; or user entities’ compliance with specified requirements of laws, regulations, contracts, or grant agreements). [↑](#footnote-ref-3)
4. Type 1 and type 2 reports focus on controls likely to be relevant to entities’ internal control over financial reporting, issued under the AICPA’s AT-C 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting. There are other types of reports on service organizations that may be available, including reports on controls at a service organization other than those likely to be relevant to entities’ internal control over financial reporting (for example, controls that are relevant to entities’ compliance with specified requirements of laws, regulations, contracts, or grant agreements). [↑](#footnote-ref-4)
5. A service that the service organization provides may be designed with the assumption that the user entity will implement certain controls. In such circumstances, the description of the service organization’s system may include a description of the complementary user-entity controls that the user entity is expected to perform. [↑](#footnote-ref-5)
6. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected, on a timely basis. [↑](#footnote-ref-6)