200 Planning Phase

210 Overview of the Planning Phase

1. The overall objective of the planning phase is to determine an effective and efficient plan for obtaining sufficient, appropriate evidence for the design, implementation, and operating effectiveness of information system (IS) controls. **Sufficiency** is the measure of the quantity of evidence used to support the findings and conclusions related to the engagement objectives. **Appropriateness** is the measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the engagement objectives and supporting findings and conclusions.
2. The engagement team meets this overall objective for planning the IS controls assessment by performing the planning activities in figure 6.

Figure 6: Planning Phase Activities

Diagram

Description automatically generated

1. When performing the IS controls assessment, the nature and extent of planning activities varies depending on several factors, including the engagement objectives, the entity’s size and complexity, and the auditor’s experience with and knowledge of the entity and its operations.
2. The planning activities discussed in the following sections need not be performed as sequential, discrete steps. For example, the auditor may concurrently gather information, such as through interviews with entity personnel or the inspection of requested documents, related to multiple planning activities to obtain evidence effectively and efficiently.
3. Planning activities are intended to be iterative, in that, as information is obtained throughout the engagement, it is evaluated for its potential effect on IS control risk. Adjustments to the IS controls assessment scope and approach may be necessary to address additional risk factors identified, regardless of the phase in which the information is obtained. For example, the auditor could obtain new information about a business process application during the testing phase that may have an effect on the auditor’s risk assessment. The auditor considers and, as appropriate, adjusts the scope and approach of the IS controls assessment accordingly to obtain sufficient, appropriate evidence to support the engagement objectives.
4. During the planning phase, the concepts of significance and audit risk assist auditors in determining the scope (paragraph 110.08). **Significance** is the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Throughout this manual, the term significance is comparable to the term material as used in the context of federal financial audits. Such factors include the magnitude of the matter in relation to the subject matter of the engagement, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the matter’s effect on the audited program or activity. **Audit risk** is the possibility that the auditor’s findings, conclusions, recommendations, or assurance may be improper or incomplete. The underlying principle of these concepts is that the auditor is not required to spend resources on items of little importance, that is, those that would not affect the judgment or conduct of a reasonable user of the audit report, considering surrounding circumstances. Based on this principle, the auditor establishes the scope and approach of the IS controls assessment to exclude areas of the entity’s operations that are not significant to the engagement objectives and therefore warrant little or no audit attention.
5. Professional judgment assists auditors when evaluating significance and audit risk to the engagement objectives. **Professional judgment** is the use of the auditor’s professional knowledge, skills, and abilities, in good faith and with integrity, to diligently gather information and objectively evaluate the sufficiency and appropriateness of evidence. Professional judgment includes exercising reasonable care and professional skepticism.

220 Perform Preliminary Engagement Activities

1. For the IS controls assessment, preliminary engagement activities include assigning a combination of auditors and IT specialists to the engagement team who collectively possess the competence needed to address the engagement objectives and communicating the engagement terms with management, those charged with governance, and others. These activities are performed either at the beginning of or throughout an engagement and are distinct from audit procedures performed to address the engagement objectives.
2. See *Financial Audit Manual* (FAM) 215, Perform Preliminary Engagement Activities, for further discussion of preliminary engagement activities relevant to federal financial audits.

Assigning Auditors and IT Specialists

1. The audit organization must assign auditors to the engagement team who collectively possess the **competence**—knowledge, skills, and abilities obtained from education and experience—needed to address the engagement objectives and perform their work. For the IS controls assessment, a broad range of knowledge, skills, and abilities may be needed to perform effective and efficient audit procedures.
2. The engagement team may include a combination of financial, performance, and IS controls auditors and IT specialists. IT specialists possess special knowledge or skills in the IT field that extend beyond the knowledge and skills normally possessed by those working in specialized fields of auditing. A combination of IS controls auditors and IT specialists with technical skills in areas such as networks, operating systems, data management systems, infrastructure applications, access control software, and application-specific technical knowledge may be needed to identify and assess general controls at the business process, system, and entity levels.
3. The audit organization considers the levels of proficiency needed for each role on the engagement when assigning auditors to the engagement. The following are references to roles at GAO; however, descriptions of proficiency levels in relation to the audit are included so that corresponding roles can be identified in other audit organizations.

* Nonsupervisory auditors plan or perform audit procedures characterized by low levels of ambiguity, complexity, and uncertainty. Nonsupervisory auditors assigned to the IS controls assessment require a basic level of proficiency in auditing and information technology to perform assigned audit work. This includes fundamental knowledge of or limited experience with auditing tasks (e.g., interviewing, gathering and documenting evidence, and communicating both orally and in writing) and information technology (e.g., networks, operating systems, data management systems, infrastructure applications, and access control software).
* Supervisory auditors plan or direct engagements and perform audit procedures characterized by moderate levels of ambiguity, complexity, and uncertainty. Supervisory auditors assigned to the IS controls assessment have an intermediate level of proficiency in auditing and information technology to perform or direct assigned audit work. This includes practical application of auditing tasks and IT expertise to allow for proper review of audit documentation; assessment of the appropriateness and sufficiency of evidence; management of projects; and identification and assessment of general controls at the entity, system, and business process levels.
* Partners and directors plan, direct, or report on engagements and perform or review audit procedures characterized by high levels of ambiguity, complexity, and uncertainty. Partners and directors have an advanced level of proficiency in auditing and information technology to manage the quality of the engagement.

1. The auditor should determine whether IT specialists assisting the engagement team are competent in their areas of specialization. The competence of IT specialists significantly affects whether their work will be adequate for the engagement team’s purposes and will meet generally accepted government auditing standards (GAGAS) requirements. The auditor’s assessment of the competence of an IT specialist may be informed by the following:

* the professional certification, license, or other recognition of the competence of the specialist in the field, as appropriate;
* the reputation and standing of the specialist in the views of peers and others familiar with the specialist’s capability or performance;
* the specialist’s experience and previous work in the subject matter;
* the auditor’s assessment of the specialist’s knowledge and qualifications based on prior experience in using the specialist’s work;
* the specialist’s knowledge of any technical performance standards or other professional or industry requirements in the specialist’s field (for example, ethical standards and other membership requirements of a professional body or industry association, accreditation standards of a licensing body, or requirements imposed by law or regulation);
* the knowledge of the specialist with respect to relevant auditing standards; and
* the assessment of unexpected events, changes in conditions, or the evidence obtained from the results of audit procedures that indicate it may be necessary to reconsider the initial evaluation of the competence and qualifications of a specialist as the engagement progresses.

Using the Work of Others

1. The engagement team may use the work of auditors and IT specialists outside of the audit organization to support findings or conclusions for the IS controls assessment. These other auditors and IT specialists may be part of an independent public accounting firm contracted by the audit organization, part of the entity’s internal audit function, and IT specialists contracted by the audit organization. The work of others may provide useful information for planning and conducting the IS controls assessment.
2. The auditor should determine whether other auditors have completed or are completing IS controls work that is relevant to the engagement objectives. If such IS controls work is being performed, the auditor should determine whether the scope, quality, and timing of the work can be relied on within the context of the current engagement objectives.
3. The auditor may determine that the audit organization will contract with other auditors or IT specialists to perform all or a portion of the IS controls assessment. The auditor’s participation in the procurement process when the audit organization contracts for IT audit support services can be instrumental in determining the scope of such services, specifying minimum qualifications for the competence of contracted staff, and developing documentation requirements. The *Federal Information System Controls Audit Manual* (FISCAM) may be required to be used as a basis for the work to be performed.
4. If the auditor determines that the audit organization will use the work of other auditors, IT specialists, or both to perform all or a portion of the IS controls assessment, the auditor should, as applicable,

* obtain evidence concerning their qualifications and independence;
* perform procedures that provide a sufficient basis for using the work of other auditors (e.g., reviewing the other auditors’ report, audit plan, or audit documentation, or performing tests of the other auditors’ work); and
* evaluate the adequacy of the work of the IT specialist for the auditor’s purposes (e.g., evaluating the relevance and reasonableness of the specialist’s findings and conclusions and consistency with other audit evidence; understanding and evaluating the relevance and reasonableness of assumptions and methods used in the circumstances; and evaluating the relevance, completeness, and accuracy of source data that are significant to the work).

1. If the auditor determines that the work of the IT specialist is not adequate for the auditor’s purposes, the auditor should agree with the IT specialist on the nature and extent of further work that the IT specialist is to perform or perform additional audit procedures appropriate to the circumstances.
2. For federal financial audits, the auditor should comply with requirements for using the work of others discussed in FAM 600, Using the Work of Others, as applicable.

Communication of Engagement Information

1. GAGAS (2018) requires certain communications with management, those charged with governance, and others. In satisfying the requirements for the communication of engagement information, the auditor may provide an overview of the IS controls assessment to management. Such an overview may include the following:

* Communicating the scope and approach of the IS controls assessment. This may include (1) an overview of the engagement objectives, including how the IS controls assessment will support achieving such objectives, and (2) high-level information about the approach, including who will be performing the IS controls tests, the tools that will be employed, and any precautions the engagement team plans to take to mitigate the risk of service degradation or interruption (for example, performing certain testing during nonpeak hours). However, it is important that the auditor not compromise the effectiveness of the IS controls assessment or the engagement. For example, communicating the nature and timing of detailed audit procedures may reduce the effectiveness of those procedures by making them too predictable.
* Identifying roles and responsibilities. This includes addressing the roles and responsibilities of key members of the engagement team, as well as management.
* Addressing logistical requirements. Logistical requirements may include on-site workspace arrangements and procedures for safeguarding sensitive information.

230 Understand the Entity’s Operations

1. Once preliminary engagement activities have been performed, the auditor begins planning the IS controls assessment to address the engagement objectives by obtaining an understanding of the entity’s operations. This understanding establishes a foundation for the auditor to assess IS control risk on a preliminary basis (section 260).
2. The auditor should obtain an understanding of the entity’s IT operations sufficient to plan the engagement. Elements of understanding the entity’s IT operations include

* IT strategic goals;
* size and locations of IT operations, including those of any service providers;
* IT organizational and management structure;
* use of external parties for IT operations, such as service organizations or contractors;
* complexity of IT operations;
* provisions of applicable laws and regulations establishing IS control requirements relevant to the engagement objectives; and
* information security management program, as discussed in section 240.

1. The auditor may gather information used in planning through different methods (inquiry, observation, and inspection) and from a variety of sources. Sources may include

* the results of previous audits, examinations, and other internal control assessments, including management reviews, relevant to the engagement objectives;
* entity policies and procedures;
* management officials;
* key personnel involved in IT operations;
* program managers (for programs significant to the engagement objectives);
* office of inspector general and internal audit managers;
* other members of the audit organization (concerning relevant completed, planned, or in-progress engagements involving the entity);
* personnel within the entity’s or the audit organization’s office of the general counsel;
* personnel within the entity’s or the audit organization’s special investigations unit; and
* other relevant reports and articles issued by or about the entity, including
  + GAO reports;
  + inspector general reports;
  + congressional hearings and reports;
  + consultant reports; and
  + material published about the entity in newspapers, magazines, internet sites, and other publications.

240 Understand the Entity’s Information Security Management Program

1. The auditor continues planning the IS controls assessment by obtaining an understanding of the entity’s information security management program. An information security management program is a program designed, implemented, and operated to reasonably assure that adequate information security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information systems. The entity’s information security management program is the foundation of its information security control structure and reflects senior management’s commitment to addressing information security risks. Information security management programs provide a framework and continuous cycle of activity for

* assigning and communicating responsibilities,
* identifying and responding to risks,
* developing and implementing effective information security policies,
* monitoring the adequacy of the entity’s IS controls, and
* holding individuals and external parties accountable for their internal control responsibilities.

1. GAO’s *Standards for Internal Control in the Federal Government* (Green Book) defines the principles for the five components of internal control related to the objectives that an entity strives to achieve.[[1]](#footnote-1) The five components follow.

* Control environment. The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives.
* Entity risk assessment. Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.
* Information and communication. The quality information management and personnel communicate and use to support the internal control system.
* Monitoring. Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.
* Control activities. The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity’s information system.[[2]](#footnote-2)

1. The FISCAM Framework for Security Management (section 530) aligns with the Green Book principles for the control environment, entity risk assessment, information and communication, and monitoring components of internal control associated with the IS controls assessment. The control activities component of internal control is the primary focus of the IS controls assessment. As such, the other control categories of the FISCAM Framework align with the Green Book principles for control activities.[[3]](#footnote-3)
2. Obtaining an understanding of the entity’s information security management program provides a preliminary understanding of how the entity identifies risks relevant to information technology and how it responds to them. This understanding provides the basis for the auditor’s preliminary assessment of IS control risk and determinations regarding the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest. See sections 260 and 270 for further discussion on assessing IS control risk on a preliminary basis, identifying relevant general control objectives, and determining the likelihood of effective general controls. See also section 250 for further discussion on identifying areas of audit interest as part of defining the scope of the IS controls assessment.
3. For federal financial audits, the auditor’s understanding of the entity’s information security management program may facilitate the auditor’s assessment of controls related to the five components of internal control to support the auditor’s overall assessment of internal control over financial reporting. For example, the auditor’s understanding of the entity’s information security management program may facilitate the auditor’s identification and testing of controls at the entity level that are important to the auditor’s conclusion about whether the entity has effective internal control over financial reporting. Further information on assessing the design, implementation, and operating effectiveness of the entity’s internal control in a federal financial audit is discussed in FAM 260, Understand the Entity’s Internal Control, and FAM 360, Perform Tests of Controls and Compliance with FFMIA.
4. The auditor should obtain an understanding of the entity’s information security management program sufficient to (1) assess the design and implementation of the control environment, entity risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment; (2) assess IS control risk on a preliminary basis; and (3) determine the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest.
5. In obtaining an understanding of the entity’s information security management program, the auditor considers whether management demonstrates a commitment to integrity and ethical values, including whether there is an appropriate tone at the top. The auditor also considers whether management uses quality information to achieve the entity’s information security and privacy objectives.
6. The auditor should use the FISCAM Framework for Security Management to obtain an understanding of the entity’s information security management program. The FISCAM Framework for Security Management presents critical elements, control objectives, illustrative controls, and audit procedures for security management general controls. Table 1 is an excerpt from the framework and presents the critical elements and control objectives relevant to an entity’s information security management program.

Table 1: Excerpt from the FISCAM Framework for Security Management (SM)

| Critical elements | Control objectives |
| --- | --- |
| SM.01 Management establishes organizational structures, assigns and communicates responsibilities, and develops plans and processes to implement an information security management program for achieving the entity’s information security and privacy objectives. | SM.01.01 Organizational structures are established to enable the entity to plan, execute, control, and assess the information security and privacy functions. |
| SM.01.02 Responsibilities are assigned to senior management positions within the information security and privacy functions. |
| SM.01.03 Planning documentation related to the entity’s information security management program is developed and maintained. |
| SM.01.04 System development life cycle processes that incorporate information security and privacy considerations are established. |
| SM.01.05 An incident response program is established. |
| SM.01.06 System-level and entity-level processes for implementing and operating the entity’s information security management program are developed and maintained. |
| SM.02 Management demonstrates a commitment to recruit, develop, and retain individuals who are competent and suitable for their information security and privacy positions. | SM.02.01 Expectations of competence and suitability for key information security and privacy roles are established and communicated. |
| SM.02.02 Screening activities are completed, and access agreements are signed prior to access authorization. |
| SM.02.03 Information security and privacy training programs and other mechanisms are established to communicate responsibilities and expected behavior for information and information system usage. |
| SM.02.04 Training activities are documented, monitored, retained, and evaluated. |
| SM.02.05 Transfer and termination activities are completed on a timely basis. |
| SM.03 Management holds individuals and external parties accountable for their internal control responsibilities related to the entity’s information security management program. | SM.03.01 Information security and privacy policies and procedures are enforced. |
| SM.03.02 External parties are held accountable for their assigned internal control responsibilities related to the entity’s information security and privacy objectives. |
| SM.03.03 Complementary user-entity controls related to external parties are identified, implemented, and operating effectively. |
| SM.04 Management identifies, analyzes, and responds to risks, including fraud risk, and significant changes related to the entity’s information security management program. | SM.04.01 Risk management strategies are developed, documented, and maintained. |
| SM.04.02 Risk identification, analysis, and response activities are conducted. |
| SM.05 Management designs and implements policies and procedures to achieve the entity’s information security and privacy objectives and respond to risks. | SM.05.01 Information security and privacy policies and procedures are developed and implemented. |
| SM.05.02 Information systems are authorized to operate. |
| SM.06 Management establishes and performs monitoring activities to evaluate the effectiveness of the entity’s information security management program. | SM.06.01 The effectiveness of information security and privacy controls is continually and periodically assessed. |
| SM.07 Management remediates identified internal control deficiencies related to the entity’s information security management program on a timely basis. | SM.07.01 Information security and privacy control deficiencies and vulnerabilities are reported, evaluated, and remediated on a timely basis. |

Source: GAO. | GAO-24-107026

1. To effectively use the FISCAM Framework for Security Management to obtain an understanding of the entity’s information security management program, the auditor considers the critical elements and control objectives in the context of the areas of audit interest. Specifically, the auditor considers the extent to which general controls that the entity designed and implemented to achieve specific security management general control objectives are likely to support the effective design, implementation, and operation of general controls relevant to logical and physical access, segregation of duties, configuration management, and contingency planning for the areas of audit interest. For example, security management general controls that the entity designed and implemented to continually and periodically assess the effectiveness of information security and privacy controls are likely to support the effectiveness of other general controls for the areas of audit interest. See section 250 for further discussion on defining the scope of the IS controls assessment, including identifying areas of audit interest. See also appendix 600C, FISCAM Security Management Questionnaire.
2. The auditor may use different audit procedures (inquiry, observation, and inspection) to obtain an understanding of the entity’s information security management program.

250 Define the Scope of the IS Controls Assessment

1. The process for defining the scope of the IS controls assessment is iterative and continues throughout the planning phase. Identifying and obtaining an understanding of the significant business processes, business process controls, and areas of audit interest enable the auditor to begin defining the scope of the IS controls assessment. This allows the auditor to focus efforts on those areas that are necessary to achieving the engagement objectives, thereby reducing or eliminating work associated with other areas.
2. Business processes are the primary means through which the entity accomplishes its mission. Business processes transform inputs into outputs through a series of transactions, activities, and events to achieve the entity’s operations, reporting, and compliance objectives.[[4]](#footnote-4) Examples of business processes include mission-related processes (e.g., education, public health, or income security), financial management processes (e.g., collections, disbursements, or payroll), and other support processes (e.g., human resources, acquisitions and procurement, property management, or security). Significant business processes are those that are significant to the engagement objectives. For example, when evaluating the condition of contracting activities performed under an acquisition and procurement program, the engagement team may identify several supporting business processes—acquisition planning, contract development, contract award, contract execution, contract modifications, and contract closeout—that contribute to the condition of the program. Throughout this manual, references to significant business processes may include those the entity performs and those that external parties, including service organizations, contractors, and others, perform on behalf of the entity.
3. Business process controls include the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions; activities across business processes; and events between business process applications, their components, and other systems. See section 120 for additional discussion.
4. Areas of audit interest are a subset of the entity’s information systems that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. For example, at the business process level, areas of audit interest may include business process applications, process automation software, system interfaces, data management systems, specific data files, and system-generated reports. At the system level, areas of audit interest may include operating systems, access control software, and hardware devices used for information processing, data storage, and network communications.
5. For federal financial audits, FAM 235, Identify Material Line Items, Accounts, Note Disclosures, and Classes of Transactions; Applicable Assertions; and Significant Financial Management Systems, requires the auditor to identify material line items, accounts, and classes of transactions, as well as significant financial management systems. In the context of an IS controls assessment performed in connection with a federal financial audit, material classes of transactions are referred to as significant business processes, and significant financial management systems are referred to as areas of audit interest at the business process level. Additionally, FAM 330, Identify Control Objectives, requires the auditor to prepare a specific control evaluation (SCE) worksheet that documents (among other things) the control activities the auditor plans to test related to material line items, accounts, note disclosures, and classes of transactions. The control activities included on an SCE worksheet comprise the manual and IS controls intended to achieve the financial statement control objectives, which include the information processing objectives of completeness, accuracy, and validity.[[5]](#footnote-5) The control activities included on the SCE worksheet that are identified as IS controls are generally considered business process controls in the context of an IS controls assessment. The auditor may use the FISCAM Framework for Business Process Controls to identify control objectives for the financial management systems involved in the material classes of transactions. The auditor may also use the framework to identify controls intended to achieve such control objectives. Further information on identifying control activities is discussed in FAM 340, Identify and Understand Control Activities. Additionally, instructions for completing the SCE worksheet are included in FAM 395G, Specific Control Evaluation Worksheet.

Identify and Understand Significant Business Processes

1. The auditor should identify business processes that are significant to the engagement objectives. The auditor uses professional judgment in determining which business processes are significant.
2. The auditor should obtain an understanding of the significant business processes by performing walk-throughs or alternative audit procedures. **A walk-through** is a combination of audit procedures (i.e., observation, inspection, and inquiry) that enable the auditor to understand the steps and resources involved in a significant business process from beginning to end, including the information systems used and the design and implementation of the IS controls involved.
3. Walk-throughs may be performed during the planning and testing phases of an engagement. During the planning phase, walk-throughs are primarily performed to obtain an understanding of the significant business processes by tracing one or more transactions, activities, or events through all processing. During the testing phase, walk-throughs are often performed as control tests involving a combination of observation, inquiry, and inspection (which may include reperformance) using nonstatistical selection. Alternative audit procedures generally include inspecting relevant documentation and inquiring of appropriate personnel without directly observing the process and controls.
4. When performing walk-throughs of the significant business processes during the planning phase, the auditor may

* observe appropriate personnel performing their assigned duties;
* inquire of appropriate personnel to obtain an understanding of information system processing that cannot be observed directly; and
* inspect business process documentation, such as process narratives, flowcharts, standard operation procedures, desktop guides, and user manuals.

1. If it is not feasible to perform walk-throughs, the auditor performs alternative audit procedures to obtain an understanding of the significant business processes, including the information systems used and the design and implementation of the IS controls involved. For example, it may not be feasible to perform walk-throughs of significant business processes that external parties perform. In such instances, alternative procedures may include

* inspecting service organization reports, if available;
* inspecting other audit or examination reports, as applicable;
* inquiring of management and personnel with knowledge of the significant business processes that external parties perform; and
* inspecting relevant documentation that the external parties provided to management.

1. In obtaining an understanding of the significant business processes, the auditor considers

* how transactions or other inputs are initiated;
* the format and content of the inputs and outputs, including source documents, data files, and system-generated reports;
* the manual and automated processing steps performed, including how inputs and outputs are accessed, updated, and deleted;
* the information technology that enables automated processing (e.g., robotic process automation and artificial intelligence);
* the business or organizational units involved;
* how the entity uses the services performed by external parties on behalf of the entity, including service organizations, contractors, and others;
* the points in the business process at which conditions or events related to the information technology could significantly affect the entity’s ability to achieve its information processing objectives (completeness, accuracy, validity); and
* the points in the business process at which conditions or events related to the information systems used could significantly affect the completeness, accuracy, or validity of a recorded transaction (e.g., when data are entered, transferred, changed, or deleted).

1. For example, the auditor may determine that the procurement of goods and services is significant to the engagement objectives. The auditor may identify the business activities—processing purchase orders, receiving goods and services, recording accounts payable, and disbursing payments—related to the procurement process. The auditor obtains an understanding of each of the business units and activities involved in the procurement process in sufficient detail to document how purchase transactions are initiated; transaction data flows between business units; information systems are used for information processing; data are input, processed, and output; system-generated reports are used; and services performed by external parties are incorporated into the procurement process.
2. The auditor should inspect available system documentation that explains the processing and flow of data within the business process application, as well as system interfaces to other information systems and the design of the underlying data management systems. Examples include end user guides, system administration guides, system interface documentation, data flow diagrams, and workflow diagrams.
3. The auditor should prepare a written description of each significant business process, including the information systems used. See section 280 for further discussion of documenting an understanding of significant business processes.

Identify and Understand Business Process Controls Using the FISCAM Framework

1. The auditor should identify and obtain an understanding of the business process controls designed to achieve information processing objectives—completeness, accuracy, and validity—based on the auditor’s understanding of the significant business processes. This understanding is primarily obtained through walk-throughs of the significant business processes and the inspection of system documentation for the business process applications, system interfaces, and data management systems used within such processes (paragraphs 250.06 through 250.14).
2. The auditor should use the FISCAM Framework for Business Process Controls (section 520) to identify relevant business process control objectives and to facilitate identifying controls that the entity designed to achieve those objectives. Relevant control objectives, as used in FISCAM, are those that are necessary to achieve the engagement objectives. For each business process, the auditor identifies

* user and application controls that are designed to achieve completeness, accuracy, and validity and
* direct general controls that support the effective operation of user and application controls.

1. The FISCAM Framework for Business Process Controls presents critical elements, control objectives, illustrative controls, and illustrative audit procedures for business process controls. Table 2 is an excerpt from the framework that presents the critical elements and control objectives. Critical elements BP.01 through BP.03 address user and application control objectives, and critical elements BP.04 through BP.06 address general control objectives that directly support the effective operation of user and application controls.

Table 2: Excerpt from the FISCAM Framework for Business Process (BP) Controls

| Critical elements | Control objectives |
| --- | --- |
| BP.01 Management designs and implements user and application controls to reasonably assure that data input into the information system are complete, accurate, and valid. | BP.01.01 Data are properly prepared and approved for input into the information system on a timely basis. |
| BP.01.02 Data input rules detect erroneous data values before information system processing. |
| BP.01.03 Data input errors are researched and resolved on a timely basis. |
| BP.02 Management designs and implements user and application controls to reasonably assure that data processing by the information system is complete, accurate, and valid. | BP.02.01 Data processing errors are identified on a timely basis. |
| BP.02.02 Data processing errors are researched and resolved on a timely basis. |
| BP.03 Management designs and implements user and application controls to reasonably assure that output data are complete, accurate, and valid. | BP.03.01 Data are approved for output. |
| BP.03.02 Output data errors are identified on a timely basis. |
| BP.03.03 Output data errors are researched and resolved on a timely basis. |
| BP.04 Management designs and implements general controls to reasonably assure that business process applications are properly managed to achieve information processing objectives. | BP.04.01 Business process application roles and responsibilities are defined and assigned to appropriate personnel. |
| BP.04.02 Policies and procedures for administering and using business process applications are developed and implemented. |
| BP.04.03 Business process applications are designed to facilitate the performance of business processes and reasonably assure the completeness, accuracy, and validity of transactions and data. |
| BP.04.04 Business process applications are designed to facilitate the protection of personally identifiable information. |
| BP.04.05 The effectiveness of application controls and the adequacy of automated business processes that business process applications perform are periodically assessed. |
| BP.04.06 Access to business process applications is appropriately controlled. |
| BP.04.07 Modifications to business process applications and changes to configurable controls within application software are appropriately controlled. |
| BP.05 Management designs and implements general controls to reasonably assure that system interfaces are properly managed to achieve information processing objectives. | BP.05.01 System interface roles and responsibilities are defined and assigned to appropriate personnel. |
| BP.05.02 Policies and procedures for managing system interfaces are developed and implemented. |
| BP.05.03 System interfaces are designed to exchange information between systems and reasonably assure the completeness, accuracy, and validity of the exchange. |
| BP.05.04 System interface errors are identified on a timely basis. |
| BP.05.05 System interface errors are researched and resolved on a timely basis. |
| BP.05.06 Access to system interface data and user-defined processing of data are appropriately controlled. |
| BP.05.07 Modifications to system interfaces are appropriately controlled. |
| BP.06 Management designs and implements general controls to reasonably assure that data management systems are properly managed to achieve information processing objectives. | BP.06.01 Data management system roles and responsibilities are defined and assigned to appropriate personnel. |
| BP.06.02 Policies and procedures for managing data management systems are developed and implemented. |
| BP.06.03 Data management systems are designed to organize, maintain, and control access to application data to reasonably assure the completeness, accuracy, and validity of transactions and data. |
| BP.06.04 The completeness, accuracy, and validity of data maintained in data management systems are periodically assessed. |
| BP.06.05 Access to data management systems is appropriately controlled. |
| BP.06.06 Modifications to data management systems and data maintained in those systems are appropriately controlled. |

Source: GAO. | GAO-24-107026

1. The following examples illustrate the use of the FISCAM Framework for Business Process Controls in identifying relevant control objectives and the controls designed by the entity to achieve those objectives.

* If the auditor has identified a data file, which is a collection of records stored in computerized form, as a potential area of audit interest, the auditor would use the framework and
  + the auditor’s understanding of the entity’s significant business processes to identify the (1) user and application control objectives that, if achieved, would provide reasonable assurance of the completeness, accuracy, and validity of the data file and (2) user and application controls designed by the entity to achieve those objectives and
  + the auditor’s understanding of the relevant business process applications, system interfaces, and data management systems to identify the (1) general control objectives that, if achieved, would directly support the effective operation of user and application controls and (2) direct general controls that the entity designed to achieve those objectives.
* If the auditor has identified a business process application as a potential area of audit interest, the auditor would use the framework and
  + the auditor’s understanding of the entity’s significant business processes to identify the (1) user and application control objectives supported by the business process application and (2) user and application controls designed by the entity to achieve those objectives and
  + the auditor’s understanding of the business process application to identify the (1) general control objectives that, if achieved, would directly support the effective operation of user and application controls and (2) direct general controls that the entity designed to achieve those objectives.

1. The auditor should determine whether any business process controls that external parties perform on behalf of the entity, including those that service organizations and contractors perform, are intended to achieve the relevant business process control objectives. The auditor uses professional judgment when determining the significance of such controls to the entity’s internal control and the engagement objectives. Factors that may affect the significance of business process controls that external parties perform include the following:

* the nature and significance of the transactions that the external party processes and
* the degree of interaction between the entity’s internal control and the external party controls.[[6]](#footnote-6)

1. If significant business process controls are performed by external parties on behalf of the entity, the auditor should obtain a sufficient understanding of such controls to assess IS control risk on a preliminary basis and design further audit procedures in response to risk. This understanding includes knowledge of the extent to which management understands and has documented the relationship between such controls and their system of internal control. The auditor may obtain a preliminary understanding of controls external parties perform through the audit procedures performed in connection with general control objective SM.03.02. External parties are held accountable for their assigned internal control responsibilities related to the entity’s information security and privacy objectives (section 240, table 1). For federal financial audits, see FAM 640, Entities Using a Service Organization, for further guidance on the nature and extent of work the auditor is to perform when the entity uses services that a service organization or subservice organization provides.
2. See section 320 for further discussion on identifying relevant IS controls for testing.

Identify and Understand Areas of Audit Interest

1. The auditor should identify areas of audit interest at the business process and system levels. Identifying areas of audit interest is an iterative process that primarily occurs during the planning phase.
2. The auditor identifies potential areas of audit interest at the business process level based on the auditor’s understanding of the information resources used in the significant businesses processes (e.g., business process applications). This understanding is primarily obtained through walk-throughs of the significant business processes (see paragraphs 250.07 through 250.10). For example, during a walk-through of a significant business process, the auditor may observe personnel using reports from an inventory management application to validate inventory counts. Upon inquiry of personnel, the auditor may determine that the volume of transactions processed by the inventory management application is significant. The auditor identifies the inventory management application and its database component as areas of audit interest because the volume of transactions the inventory management application processes and the database component stores is significant to the engagement objectives.
3. The auditor identifies potential areas of audit interest at the system level based on the auditor’s understanding of each of the potential areas of audit interest at the business process level. This understanding is primarily obtained through the inspection of system documentation for the business process applications. In obtaining an understanding, the auditor considers the

* individuals who fulfill system roles and responsibilities,
* authorization boundary,
* information system components,
* security categorization,
* impact level,
* control dependencies,
* system interconnections,
* security and privacy requirements,
* controls selected to satisfy those requirements, and
* operational environment. [[7]](#footnote-7)

1. The auditor uses professional judgment when evaluating the significance of potential areas of audit interest to the engagement objectives. The auditor may characterize the significance of potential areas of audit interest by

* the presence or number of application controls incorporated directly into the business process application,
* the dollar value of the transactions processed,
* the volume of transactions processed,
* the sensitivity or significance of the information processed, or
* the existence of an access path to another system that contains sensitive or significant information.

1. The following examples illustrate how the auditor may identify potential areas of audit interest at the business process and system levels.

* The auditor’s understanding of an information system’s authorization boundary may assist the auditor in identifying areas of audit interest at the business process level that are excluded from but connected to an information system used in the significant businesses process. For example, after inspecting system documentation for a payroll system identified within a significant business process, the auditor may determine that the payroll system relies on data from a timekeeping system that is not within the same authorization boundary. Because the timekeeping system is a separate information system that may have different security and privacy requirements and controls that have a direct effect on information processing objectives relevant to the significant business process, the auditor may identify the timekeeping system as an area of audit interest at the business process level.
* The auditor’s understanding of an information system’s components and system interconnections may assist the auditor in identifying areas of audit interest at the business process level that may not be evident when observing a significant businesses process. For example, the auditor may not be able to observe the use of system interface software that transfers data between system components during a walk-through of a significant business process.
* The auditor’s understanding of the controls that management selected for the information system used in a significant business process may assist the auditor in identifying areas of audit interest at the system level from which the information system inherited certain controls. **Control inheritance** occurs when an information system or information system component receives protection from security or privacy controls that are developed, implemented, assessed, authorized, and monitored by personnel other than those responsible for the information system or information system component. For example, the mechanisms for enforcing logical access control for a business process application may be developed, implemented, assessed, authorized, and monitored as part of a separate information system.
* The auditor’s understanding of the operational environment may assist the auditor in identifying areas of audit interest at the system level from which various information systems inherited certain controls used in the significant business processes. For example, in identifying related access paths through the inspection of network and information system diagrams, the auditor may identify areas of audit interest that provide inherited controls the entity employs (or external parties employ on behalf of the entity) to protect the access paths and control the flow of information. In obtaining an understanding of related access paths, the auditor considers
  + internet presence and any outward-facing, publicly accessible servers, such as web and email services;
  + network segmentation and the location of firewalls, routers, and switches;
  + intrusion detection and prevention systems;
  + file transfer systems and connections to external parties, as well as inter- and intra-entity connections;
  + network management systems;
  + wireless connections;
  + remote access; and
  + whether the use of mobile devices or personally owned systems, components, and devices is permitted.

260 Assess IS Control Risk on a Preliminary Basis

1. When performing the IS controls assessment, the auditor assesses IS control risk to determine the nature, timing, and extent of control tests. The auditor obtains an understanding of the risks related to information processing objectives (i.e., completeness, accuracy, and validity) before consideration of related IS controls. This understanding helps the auditor assess IS control risk. While the auditor assesses IS control risk throughout the engagement, risk assessment activities are concentrated in the planning phase.
2. FISCAM defines **IS control risk** as the likelihood that conditions or events, related to the areas of audit interest, that could significantly affect the entity’s ability to achieve its information processing objectives, will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls. IS control risk is a function of the design, implementation, and operating effectiveness of the entity’s IS controls relevant to the engagement objectives. Some IS control risk will always exist because of the inherent limitations of internal control.
3. The auditor’s preliminary assessment of IS control risk for each area of audit interest enables the auditor to establish an appropriate basis for planning the IS controls assessment to reduce audit risk to an acceptably low level, as required by GAGAS (2018).
4. In assessing IS control risk, the auditor considers the extent to which IS controls mitigate inherent and IS risk factors. These risk factors can result in an increase or decrease the auditor’s assessed level of IS control risk for the area of audit interest. The auditor uses professional judgment in determining (1) the extent of audit procedures necessary to identify inherent and IS risk factors and (2) the effect of such risk factors on the auditor’s preliminary assessment of IS control risk.
5. The auditor should involve senior members of the engagement team in the assessment of IS control risk. The auditor may use the results of management’s risk assessments, along with other information collected during the planning phase, to arrive at a preliminary assessment of IS control risk. However, the auditor is not required or expected to reperform management’s risk assessments when using the results of such to inform the auditor’s assessment of IS control risk. The auditor may also consult with an IT specialist when assessing IS control risk.
6. The auditor should prepare a written risk assessment that identifies the inherent risk factors, IS risk factors, fraud risk factors, and results of previous engagements that significantly increase or decrease the auditor’s assessed level of IS control risk for each area of audit interest. See section 280 for further discussion of documenting the preliminary assessment IS control risk.
7. For federal financial audits, further information on the assessment of inherent and control risk—including risk factors related to information technology—is discussed in FAM 265, Identify Risks of Material Misstatement and Assess Inherent Risk. Risk of material misstatement is the risk that, prior to the financial audit, the financial statements are materially misstated due to fraud or error. In the context of a federal financial audit, the auditor’s assessment of IS control risk is incorporated into the financial auditor’s assessment of the risk of material misstatement to determine the nature, timing, and extent of further audit procedures.

Identify Inherent and IS Risk Factors

Inherent Risk Factors

1. The auditor should obtain an understanding of the inherent risk factors, before consideration of related IS controls, related to information processing objectives (i.e., completeness, accuracy, and validity) relevant to the engagement objectives. For federal financial audits, the auditor obtains an understanding of the inherent risk assessments identified on the SCE worksheet. For performance audits, the auditor obtains an understanding of inherent risks that the data significant to the engagement objectives are not reliable (i.e., incomplete, inaccurate, or invalid), through discussions with the overall engagement auditor.

IS Risk Factors

1. The auditor should identify IS risk factors related to information processing objectives relevant to the engagement objectives. The auditor identifies IS risk factors related to information processing objectives based on information obtained during the planning phase to develop an understanding of the entity’s operations; information security management program; significant business processes; and business process controls, including any operations, processes, or controls external entities perform on behalf of the entity. The auditor may also identify IS risk factors through inquiries of appropriate personnel and the inspection of relevant reports on the entity’s control activities, including IS controls. For each area of audit interest, the auditor considers the identified IS risk factors and assesses the level of control risk.
2. The auditor identifies IS risk factors relevant to the area of audit interest based on the auditor's understanding of the area of audit interest, including the information technology the entity employs in connection with the area of audit interest. **IS risk factors** are conditions or events that affect the susceptibility of the area of audit interest to information system processing errors before consideration of any mitigating IS controls. The information technology the entity employs can introduce IS risk factors, such as the following:

* Certain types of hardware and software in use may be more susceptible to threats than others. For example, hardware or software that is not updated or patched, as well as unsupported information system components, present greater inherent risk than those that are updated, patched, and supported by the developer, vendor, or manufacturer.
* The entity’s use of new or emerging technology can increase the risk that secure configurations of corresponding information system components may not be well-developed or tested, or that IT personnel may not have the knowledge, skills, and abilities necessary to properly select and implement security controls over such technology.
* The consistency of the system-level security and privacy architectures with the entity’s enterprise architecture, as well as the entity’s mission and business strategies, can affect the design of information systems and related security controls.
* The complexity of the entity’s IT operations, including the extent to which external parties perform IT operations, including information security and privacy functions, on behalf of the entity, can result in higher inherent risk.
* Software programs developed in-house may have higher inherent risk than vendor-supplied software that has been thoroughly tested and is in general commercial use. On the other hand, vendor-supplied software new to commercial use may not have been thoroughly tested or undergone client processing to a degree that would reveal existing flaws.
* The structure of the entity’s networks and the configuration of network components affect the access paths into and out of the information systems relevant to the significant business processes. For example, factors increasing inherent risk include a significant number of internet access points that are not centrally controlled; networks that are not segmented to protect sensitive information and information systems; and a lack of tools and software that enhance network security, such as intrusion detection and prevention systems.
* Highly decentralized information systems, particularly web applications, add complexity and increase potential vulnerabilities.
* In certain information systems, the audit trails and supporting information that the systems produce may be limited in their usefulness (1) as a basis for applying certain types of controls or (2) as audit evidence.

1. An understanding of the entity’s information security management program enables the auditor to identify IS risk factors related to the entity’s control environment, risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment. Inspecting the documented results of information security management program activities that management performs may also assist the auditor in identifying IS risk factors. For example, the auditor’s inspection of information security and privacy control assessments, results of continuous monitoring activities, and any relevant plans of action and milestones for the areas of audit interest assists the auditor in determining the likelihood that IS controls applied to the areas of audit interest will be effective. The auditor may consider the following IS risk factors, which are organized by the security management critical elements from table 10 (section 530):

* SM.01 Management establishes organizational structures; assigns and communicates responsibilities; and develops plans and processes to implement an information security management program for achieving the entity’s information security and privacy objectives. IS risk factors include conditions or events related to
  + the placement of the chief information officer, chief risk officer, information security officer, and privacy officer positions within the organizational structure;
  + the nature of the IT organizational structure (i.e., a centralized or decentralized structure);
  + the extent to which the IT organizational structure is designed to support the segregation of incompatible duties;
  + the extent to which management demonstrates an appropriate level of interest in and awareness of information security and privacy functions, including those functions that external parties perform;
  + the quality of the entity-level information security management program and privacy management program plans and whether such plans align with the entity’s strategic plan;
  + the extent to which the entity’s system development life cycle processes adequately address information security and privacy considerations;
  + the extent to which the entity has established an adequate incident response program;
  + the quality of the entity’s system security and privacy plans for the areas of audit interest;
  + the quality of the entity’s information system contingency plans for the areas of audit interest; and
  + the extent to which information security and privacy responsibilities—particularly those pertaining to the areas of audit interest—are clearly defined and appropriately assigned to personnel with the authority and expertise needed to fulfill them.
* SM.02 Management demonstrates a commitment to recruit, develop, and retain individuals who are competent and suitable for their information security and privacy positions. IS risk factors include conditions or events related to
  + turnover of key personnel involved in IT operations, including turnover that could affect the areas of audit interest (i.e., high or low turnover);
  + the number of personnel with appropriate knowledge, skills, and abilities relative to the size and complexity of the entity’s IT operations (i.e., adequate or inadequate number);
  + the adequacy of the security and privacy workforce development and improvement program; and
  + the appropriateness of the information security and privacy training programs.
* SM.03 Management holds individuals and external parties accountable for their internal control responsibilities related to the entity’s information security management program. IS risk factors include conditions or events related to
  + the extent to which information security and privacy policies are enforced;
  + the extent to which the terms and conditions for the protection of controlled unclassified information processed, stored, or transmitted on external systems are clearly documented (e.g., in a memorandum of understanding or service agreement) and understood by entity personnel responsible for enforcement;[[8]](#footnote-8)
  + the extent to which external parties performing IT operations, including information security and privacy functions, on behalf of the entity are held accountable for their assigned internal control responsibilities; and
  + the adequacy of the entity’s processes for assessing the effectiveness of information security and privacy controls that external parties designed, implemented, and operated—particularly those pertaining to the areas of audit interest.
* SM.04 Management identifies, analyzes, and responds to risks, including fraud risk, and significant changes related to the entity’s information security management program. IS risk factors include conditions or events related to
  + the quality of the entity-level risk management strategy for information security and privacy risks;
  + the quality of the entity-level continuous monitoring strategy;
  + the extent to which the entity appropriately considers inherent and control risks, including fraud risk, related to information systems—particularly those information systems identified as areas of audit interest;
  + the extent to which the entity properly identifies, analyzes, and responds to risks arising from (1) internal sources, such as the ability to retain key personnel involved in IT operations or the adequacy of system backups to facilitate the recovery and reconstitution of information systems following a system disruption, and (2) external sources, such as vulnerabilities, flaws, and threats;
  + the extent to which the entity incorporates audit recommendations or identified internal control deficiencies into its risk management processes;
  + the extent to which the entity appropriately modifies information systems—particularly those identified as areas of audit interest—in response to changing conditions on a timely basis; and
  + the extent to which management is involved in major system development or modification decisions.
* SM.05 Management designs and implements policies and procedures to achieve the entity’s information security and privacy objectives and respond to risks. IS risk factors include conditions or events related to
  + the quality of the entity’s policies and procedures for managing and using business process applications, system interfaces, and data management systems, as well as information security and privacy policies and procedures implemented at the system and entity levels;
  + the extent to which the entity’s policies and procedures are clearly documented and understood by entity personnel responsible for enforcement;
  + the extent to which the entity’s policies and procedures address appropriate segregation of duties for the entity’s IT operations;
  + the complexity of the entity’s processes for authorizing information systems and common controls for inheritance by information systems, including the extent to which the entity’s authorization processes rely on information from external parties, such as third-party assessors; and
  + the quality of the entity’s authorization packages—particularly for those information systems identified as areas of audit interest.
* SM.06 Management establishes and performs monitoring activities to evaluate the effectiveness of the entity’s information security management program. IS risk factors include conditions or events related to
  + the quality of the entity’s system-level continuous monitoring strategies and the extent to which the entity’s system-level continuous monitoring activities are implemented in accordance with such strategies;
  + the quality of the entity’s information security and privacy control assessments for the areas of audit interest;
  + the quality of the entity’s information system contingency plan test results for the areas of audit interest;
  + the extent to which the entity appropriately considers whether reliable system-generated information is used for key operating decisions;
  + the extent to which the entity monitors the effectiveness of segregation of duties controls, including alternative IS controls implemented to mitigate risks resulting from incompatible duties that cannot be segregated; and
  + the extent to which the entity adequately identifies and responds to unusual or exceptional conditions.
* SM.07 Management remediates identified internal control deficiencies related to the entity’s information security management program on a timely basis. IS risk factors include conditions or events related to
  + the extent to which the entity timely and appropriately responds to findings, recommendations, or concerns related to its information system controls;
  + the adequacy of the entity’s processes for developing, documenting, and periodically reviewing and updating plans of actions and milestones;
  + the extent to which identified control deficiencies and vulnerabilities are analyzed in relation to the entire entity and appropriate corrective actions are applied entity-wide; and
  + the extent to which remediation tasks and milestones are accomplished by scheduled completion dates.

Identify Fraud Risk Factors

1. The engagement team members should discuss fraud risk factors and assess the risk of fraud occurring that is significant to the engagement objectives. It is important that all members of the engagement team are aware of the fraud risk factors identified, including any specific fraud risks or suspected fraud associated with the information technology that the entity employs.
2. Fraud risk factors affect the auditor’s assessment of IS control risk. The auditor uses professional judgment in determining (1) the extent of audit procedures necessary to identify fraud risk factors and (2) the effect of such risk factors on the auditor’s preliminary assessment of IS control risk.
3. The following control risk factors related to the information technology that the entity employs may increase the risk of fraud:

* failure to fully implement an effective information security management program, including monitoring activities to evaluate the effectiveness of the program;
* weaknesses in access controls or other IS controls that could allow overrides of internal controls or unauthorized access to information systems susceptible to fraud (e.g., payment systems);
* lack of adequate segregation of duties controls; and
* pervasive or long-standing IS control deficiencies.

1. Assessing the risk of fraud is an ongoing process throughout the engagement and relates not only to planning the engagement but also to evaluating evidence obtained during the engagement. If information comes to the auditor’s attention indicating that fraud significant to the engagement objectives may have occurred, the auditor addresses the specific GAGAS-established requirements.
2. A specific area of concern for fraud is management override of controls. The IS controls assessment may include procedures to identify system-based overrides. These procedures may include testing for instances of users performing inappropriate combinations of transactions (i.e., transactions that are required to be segregated) and other similar procedures. Some examples of antifraud controls to consider include workflow approvals, restricting access to sensitive files, segregation of duties, review of audit trails, and review of key management reports.
3. The auditor’s training, experience, and understanding of the entity or program being audited may provide a basis for recognizing that some acts coming to the auditor’s attention may indicate fraud. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond the auditor’s professional expertise and responsibility.

Evaluate Results of Previous Engagements

1. The auditor should evaluate whether the audited entity has taken appropriate corrective action to address previously reported findings and recommendations that are significant to the engagement objectives. When planning the audit, the auditor should ask management to identify previous engagements or other studies that directly relate to the engagement objectives, including whether the entity has implemented related recommendations. This would include weaknesses management identified through its monitoring controls (e.g., for federal entities, plans of action and milestones) that are relevant to the areas of audit interest. The auditor uses this information in assessing IS control risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current engagement objectives.
2. The auditor may obtain information from relevant reports and other documents concerning IS controls that are issued by or about the entity, including

* the entity’s prior Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. § 3554(c)) or equivalent reports on IS controls;
* the entity’s annual performance and accountability report or equivalent reports on performance, including reports filed to comply with the Federal Financial Management Improvement Act of 1996 (FFMIA)[[9]](#footnote-9) and Federal Managers’ Financial Integrity Act of 1982 (FMFIA);[[10]](#footnote-10)
* other reports by management, the auditor, or others that contain information concerning IS controls that are relevant to the engagement objectives;
* service organization reports, if available, for any operations, processes, or controls that service organizations perform on behalf of the entity;
* GAO reports;
* inspector general and internal audit reports (including those for performance audits and other reviews); and
* consultant reports.

Assess IS Control Risk on a Preliminary Basis

1. The auditor should preliminarily assess the level of IS control risk for each area of audit interest based on the auditor’s understanding of inherent risk factors, IS risk factors, fraud risk factors, and results of previous engagements. Such risk factors can increase or decrease the auditor’s assessed level of IS control risk for the area of audit interest. For each area of audit interest, the auditor assesses preliminary IS control risk at one of three levels:

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

1. The auditor should determine (1) the likelihood that conditions or events related to the area of audit interest could affect the entity’s ability to achieve the relevant control objectives and (2) the impact that such conditions or events (e.g., significance) would have on the entity’s achievement of those objectives.
2. To assess likelihood and impact, the auditor also considers other factors or compensating controls that may mitigate the effects of identified inherent and control risk factors. If other factors or compensating controls are present, the auditor documents such factors or controls, determines whether they are effective in mitigating the effects of the identified inherent and control risk factors, and draws conclusions about likelihood and impact.
3. The auditor’s assessed level of IS control risk for each area of audit interest differs from management’s security categorizations of information systems and information processed through, stored on, and transmitted by such systems. Security categorization of federal information systems and information, as required by Federal Information Processing Standard (FIPS) 199, is an important first step in the entity’s information security and privacy risk management process.[[11]](#footnote-11) Though considered in the context of the same information security objectives of confidentiality, integrity, and availability, the auditor’s assessment of IS control risk for each area of audit interest need not match management’s security categorizations for the corresponding information systems.
4. The auditor should involve senior members of the engagement team in determining the nature, timing, and extent of IS control tests in response to assessed risks. As IS control risk increases, audit risk increases. However, audit risk can be reduced by taking actions such as adding specialists, additional reviewers, and other resources to conduct the engagement, as well as changing the approach to obtain additional evidence, higher-quality evidence, or alternative forms of corroborating evidence. Consequently, the auditor’s assessment of IS control risk affects the nature, timing, and extent of IS controls testing. As IS control risk increases, the auditor may expand the nature, timing, and extent of audit procedures to conclude on the effectiveness of such controls.

270 Identify Relevant General Control Objectives and Determine Likelihood of Effective General Controls

1. When planning the IS controls assessment, the auditor identifies general control objectives for each area of audit interest. Such control objectives are a subset of those necessary to achieve the engagement objectives (i.e., relevant control objectives). Achieving relevant general control objectives for areas of audit interest at the system and entity levels creates a suitable environment to support the effective operation of user, application, and direct general controls (section 250). The engagement objectives and the auditor’s understanding of the entity’s operations, information security management program, significant business processes, business process controls, and areas of audit interest provide the basis for identifying such control objectives.
2. The auditor also determines the likelihood that general controls the entity designed will achieve (or support achieving) relevant control objectives for each area of audit interest. The auditor’s understanding of the entity’s information security management program (including the results of the program’s activities that management performs) provides the basis for determining the likelihood that general controls will achieve (or support achieving) relevant control objectives for each area of audit interest. The likelihood of effective general controls informs the nature, timing, and extent of (1) general control tests and (2) user and application control tests.
3. For federal financial audits, further information on determining the likelihood of effective general controls is discussed in FAM 270, Determine Likelihood of Effective IS Controls, and FAM 290, Documentation (Planning Phase). The auditor communicates the likelihood of effective general controls to the financial auditor to assist them in completing their assessment under FAM 270.
4. The auditor should identify relevant general control objectives for each area of audit interest at the system and entity levels. When identifying such relevant general control objectives, the auditor considers the general control objectives related to the five general control categories: security management, logical and physical access, segregation of duties, configuration management, and contingency planning. Depending on the engagement’s objectives, the auditor may determine that it is not necessary to identify relevant general control objectives from all five general control categories.
5. The auditor should determine the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest. In determining the likelihood that general controls will be effective and relevant general control objectives will be achieved, the auditor exercises professional judgment based on the auditor’s understanding of the entity’s information security management program (including the results of information security management program activities that management performs), as well as the auditor’s understanding of business process controls and preliminary assessment of IS control risk for each area of audit interest. The auditor considers whether such determinations affect the preliminary assessment of IS control risk for each area of audit interest. See section 240 for further discussion on obtaining an understanding of the entity’s information security management program; section 250 for further discussion on obtaining an understanding of user, application, and direct general controls; and section 260 for further discussion on assessing IS control risk on a preliminary basis.

Security Management

1. The auditor should use the FISCAM Framework for Security Management (section 530) to (1) identify security management general control objectives relevant to each area of audit interest and (2) determine the likelihood that security management general controls applied to the areas of audit interest will achieve the relevant control objectives. When identifying relevant security management control objectives and determining the likelihood that security management general controls applied to the areas of audit interest will achieve the relevant control objectives, the auditor considers the preliminary level of IS control risk for each area of audit interest.
2. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that security management general controls will be effective. Regardless of whether the auditor identifies security management general control objectives as being relevant to the areas of audit interest, the auditor is required to obtain an understanding of the entity’s information security management program sufficient to (1) assess the design and implementation of the entity’s control environment, risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment and (2) plan the IS controls work necessary to achieve the engagement objectives. The auditor’s understanding of the entity’s information security management program provides the basis for determining the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest. For example, the auditor’s inspection of information security and privacy control assessments, results of continuous monitoring activities, and any relevant plans of action and milestones for the areas of audit interest assists the auditor in determining the likelihood that IS controls applied to the areas of audit interest will be effective.
3. See section 240 for further discussion on obtaining an understanding of the entity’s information security management program. Section 240, table 1, is an excerpt from the FISCAM Framework for Security Management and presents the critical elements and associated control objectives.

Access Controls (Logical and Physical Access)

1. The auditor should use the FISCAM Framework for Access Controls (section 540) to (1) identify logical and physical access general control objectives relevant to each area of audit interest and (2) determine the likelihood that logical and physical access general controls applied to the areas of audit interest will achieve the relevant control objectives.
2. When identifying relevant logical and physical access general control objectives and determining the likelihood that logical and physical access general controls applied to the areas of audit interest will achieve the relevant control objectives, the auditor considers the preliminary level of IS control risk for each area of audit interest. For example, when inspecting information security and privacy control assessments, results of continuous monitoring activities, and any relevant plans of action and milestones for the areas of audit interest, the auditor considers the extent to which logical and physical access general controls are addressed and whether management determined such controls to be effective.
3. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that logical and physical access general controls will be effective.
4. Table 3 is an excerpt from the FISCAM Framework for Access Controls and presents the critical elements and associated control objectives.

Table 3: Excerpt from the FISCAM Framework for Access Controls (AC)

| Critical elements | Control objectives |
| --- | --- |
| AC.01 Management designs and implements general controls to appropriately protect information system boundaries in response to risks. | AC.01.01 Connectivity to the information system is appropriately controlled. |
| AC.01.02 Network sessions are appropriately controlled. |
| AC.02 Management designs and implements general controls to appropriately restrict logical access to information systems to authorized individuals for authorized purposes. | AC.02.01 Identification and authentication requirements are established. |
| AC.02.02 Information system users, processes, and services are appropriately identified and authenticated before accessing information systems. |
| AC.02.03. Information system users, processes, and services are appropriately authorized before accessing information systems. |
| AC.02.04 Access privileges restrict access to information resources to authorized individuals for authorized purposes. |
| AC.03 Management designs and implements general controls to appropriately protect data in response to risks. | AC.03.01 Media controls are appropriately selected and employed based on risk. |
| AC.03.02 Cryptographic controls are appropriately selected and employed based on risk. |
| AC.04 Management designs and implements general controls to appropriately restrict physical access to information resources to authorized individuals for authorized purposes. | AC.04.01 Physical access controls are appropriately selected and employed based on risk. |
| AC.05 Management designs and implements detective general controls to appropriately monitor logical and physical access in response to risks. | AC.05.01 Incidents are properly identified and logged. |
| AC.05.02 Incidents are properly analyzed, and appropriate actions are taken. |

Source: GAO. | GAO-24-107026

Segregation of Duties

1. The auditor should use the FISCAM Framework for Segregation of Duties (section 550) to (1) identify segregation of duties general control objectives relevant to each area of audit interest and (2) determine the likelihood that segregation of duties general controls applied to the areas of audit interest will achieve the relevant control objectives.
2. When identifying relevant segregation of duties general control objectives and determining the likelihood that segregation of duties general controls applied to the areas of audit interest will achieve the relevant control objectives, the auditor considers the preliminary level of IS control risk for each area of audit interest. For example, when obtaining an understanding of the entity’s information security management program and assessing preliminary IS control risk relevant to the areas of audit interest, the auditor considers the extent to which the IT organizational structure is designed to support the segregation of incompatible duties.
3. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that segregation of duties general controls will be effective.
4. Table 4 is an excerpt from the FISCAM Framework for Segregation of Duties and presents the critical elements and associated control objectives.

Table 4: Excerpt from the FISCAM Framework for Segregation of Duties (SD)

| Critical element | Control objectives |
| --- | --- |
| SD.01 Management designs and implements general controls to appropriately segregate incompatible duties and mitigate risks resulting from incompatible duties that cannot be segregated. | SD.01.01 Incompatible duties are identified based on risk. |
| SD.01.02 Incompatible duties are appropriately segregated when possible. |
| SD.01.03 Alternative general controls are implemented to mitigate risks resulting from incompatible duties that cannot be segregated. |

Source: GAO. | GAO-24-107026

Configuration Management

1. The auditor should use the FISCAM Framework for Configuration Management (section 560) to (1) identify configuration management general control objectives relevant to each area of audit interest and (2) determine the likelihood that configuration management general controls applied to the areas of audit interest will achieve the relevant control objectives.
2. When identifying relevant configuration management general control objectives and determining the likelihood that configuration management general controls applied to the areas of audit interest will achieve the relevant control objectives, the auditor considers the preliminary level of IS control risk for each area of audit interest. For example, when inspecting information security and privacy control assessments, results of continuous monitoring activities, and any relevant plans of action and milestones for the areas of audit interest, the auditor considers the extent to which configuration management general controls are addressed and whether management determined such controls to be effective.
3. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that configuration management general controls will be effective.
4. Table 5 is an excerpt from the FISCAM Framework for Configuration Management and presents the critical elements and associated control objectives.

Table 5: Excerpt from the FISCAM Framework for Configuration Management (CM)

| Critical elements | Control objectives |
| --- | --- |
| CM.01 Management designs and implements general controls to develop and maintain secure baseline configurations for information systems. | CM.01.01 Baseline configurations for information systems and system documentation for administrators and users are developed and maintained. |
| CM.01.02 An inventory of information system components is developed and maintained. |
| CM.01.03 Configuration items for information systems are identified and placed under configuration management. |
| CM.01.04 Configuration settings are established and documented for configuration items. |
| CM.02 Management designs and implements general controls to manage changes to entity information systems and information system components. | CM.02.01 Planned changes to configuration items are formally authorized, analyzed, tested, and approved prior to implementation. |
| CM.02.02 Emergency changes to configuration items are documented, analyzed, and reviewed. |
| CM.02.03 Information systems and information system components are routinely monitored for deviations from established configuration settings and unauthorized changes. |
| CM.02.04 Logical access controls relevant to configuration management are selected and employed based on risk. |
| CM.03 Management designs and implements general controls to protect information systems and information system components from vulnerabilities, flaws, and threats. | CM.03.01 Vulnerability monitoring is routinely conducted. |
| CM.03.02 Critical updates and patches for information systems are implemented, and unsupported information system components are replaced on a timely basis. |
| CM.03.03 Information systems and information system components are protected from spam and malicious code. |

Source: GAO. | GAO-24-107026

Contingency Planning

1. The auditor should use the FISCAM Framework for Contingency Planning (section 570) to (1) identify contingency planning general control objectives relevant to each area of audit interest and (2) determine the likelihood that contingency planning general controls applied to the areas of audit interest will achieve the relevant control objectives.
2. When identifying relevant contingency planning general control objectives and determining the likelihood that contingency planning general controls applied to the areas of audit interest will achieve the relevant control objectives, the auditor considers the preliminary level of IS control risk for each area of audit interest. For example, when obtaining an understanding of the entity’s information security management program and assessing IS control risk relevant to the areas of audit interest, the auditor may consider the quality of the entity’s information system contingency plans and related test results.
3. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that contingency planning general controls will be effective.
4. Table 6 is an excerpt from the FISCAM Framework for Contingency Planning and presents the critical elements and associated control objectives for contingency planning.

Table 6: Excerpt from the FISCAM Framework for Contingency Planning (CP)

| Critical elements | Control objectives |
| --- | --- |
| CP.01 Management designs and implements general controls to achieve continuity of operations and prioritize the recovery and reconstitution of information systems that support critical or essential mission and business functions in the event of a system disruption, compromise, or failure. | CP.01.01 Criticality analyses are performed to prioritize mission and business functions and determine the criticality of information systems, information system components, and information system services. |
| CP.01.02 Information system contingency plans and other organizational plans are established and implemented to continue critical or essential mission and business functions in the event of a system disruption, compromise, or failure, and to eventually restore the information system following a system disruption. |
| CP.01.03 Information system users and other personnel are trained to fulfill their roles and responsibilities associated with the information system contingency plan in the event of a system disruption. |
| CP.01.04 Information system contingency plans are periodically tested to determine their effectiveness and the entity’s readiness to execute them. |
| CP.02 Management designs and implements general controls to prevent or minimize system disruption and potential damage to information resources and facilities due to natural disasters, structural failures, hostile attacks, or errors. | CP.02.01 Environmental controls are appropriately selected and employed based on risk. |
| CP.02.02 Management has established alternate sites, services, and information security mechanisms to permit the timely resumption of operations supporting critical or essential mission and business functions in the event of a system disruption. |
| CP.02.03 System backups are regularly conducted, and system media containing backup data and software are properly maintained to facilitate the recovery and reconstitution of information systems following a system disruption. |
| CP.02.04 Maintenance of information system components is properly performed on a timely basis to prevent or minimize system disruption. |

Source: GAO. | GAO-24-107026

Business Process Controls

1. The auditor should determine the likelihood that business process general controls applied to the areas of audit interest will achieve the relevant business process general control objectives for each area of audit interest. See section 250 for further discussion on identifying the relevant business process general control objectives.

280 Prepare Planning Phase Documentation

1. The auditor should prepare planning phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand the engagement objectives, scope, and approach of the IS controls assessment.

Auditor’s Understanding of Significant Business Processes

1. The auditor should prepare a written description of each significant business process sufficient to clearly identify the areas of audit interest involved at the business process level, as well as business process controls applied to the significant business processes. At the business process level, areas of audit interest may include business process applications, process automation software, system interfaces, data management systems, specific data files, and system-generated reports. The auditor may prepare complementary diagrams to document the auditor’s understanding of the flow of information through the significant business processes, as well as the related user, application, and direct general controls. These diagrams may be based on the auditor’s inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals, as well as the auditor’s inspection of available business process application documentation explaining the processing and flow of data within the applications involved. Diagrams may summarize the flow of information and data in terms of

* input and output reports or documents,
* processing steps,
* files used during processing,
* organizational units involved,
* business process applications and information systems involved, and
* system interfaces.

For federal financial audits, the auditor documents the understanding of significant business processes, the information system processing, and IS controls in cycle memorandums, or other equivalent narratives, and may prepare or obtain related flowcharts (FAM 320.01). FAM 390, Documentation (Internal Control Phase), provides details on preparing a cycle memorandum to clearly describe significant business processes.

Auditor’s Preliminary Assessment of IS Control Risk

1. The auditor should prepare a written preliminary assessment of IS control risk for each area of audit interest. As part of the auditor’s preliminary assessment of IS control risk, the auditor documents determinations regarding preliminary IS control risk and the reasons for such determinations (i.e., the significant factors that increase or decrease such assessments). Such significant factors include inherent risk factors, IS risk factors, fraud risk factors, and results of previous engagements. The auditor also documents other factors or compensating controls that may mitigate the effects of identified IS risk factors.

Planning Memo and Audit Plan

1. The auditor should prepare a written planning memo for the IS controls assessment that includes a description of key decisions about the scope of the IS controls assessment, including

* the identification of significant business processes;
* the identification of areas of audit interest at the business process and system levels;
* key decisions related to the areas of audit interest;
* the identification of relevant user, application, and general control objectives for each area of audit interest, as applicable; and
* the auditor’s basis for such scoping decisions, such as the auditor’s understanding of the entity’s information security management program, the auditor’s preliminary assessment of IS control risk, and the auditor’s determinations regarding the likelihood that general controls applied to the areas of audit interest will be effective.

1. The auditor should prepare a written audit plan for the IS controls assessment and should update the document, as necessary, to reflect any significant changes to the plan during the engagement. The written audit plan describes

* the nature and extent of planned audit procedures for the planning phase;
* the nature, timing, and extent of planned audit procedures for the testing phase (see detailed audit plan in paragraph 280.06); and
* other planned audit procedures that are required to be carried out so that the engagement complies with GAGAS.

The auditor should complete the planned audit procedures for the planning phase.

1. During the planning phase, the auditor should begin to develop a detailed audit plan that describes the nature, timing, and extent of planned audit procedures for relevant control objectives for each area of audit interest. This planned approach generally includes the audit procedures necessary for obtaining an understanding of the controls that the entity designed and implemented to achieve the relevant control objectives. However, the auditor may elect to defer decisions regarding the nature, timing, and extent of further audit procedures to assess the operating effectiveness of controls until the auditor has assessed design and implementation. See section 350 for further discussion on documentation requirements for developing, updating, and completing detailed audit plans for each area of audit interest.

FISCAM Assessment Completion Checklist

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

1. The Green Book broadly classifies these objectives into three categories: operations, reporting, and compliance. Operations addresses the effectiveness and efficiency of operations. Reporting addresses the reliability of reporting for internal and external use. Compliance addresses compliance with applicable laws and regulations. [↑](#footnote-ref-1)
2. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](https://www.gao.gov/products/GAO-14-704G) (Washington, D.C.: September 2014). [↑](#footnote-ref-2)
3. In the context of FISCAM, the term IS controls (user, application, and general controls) refers to both the policies and procedures established by management to effect relevant principles within each component of internal control and the techniques and mechanisms established by management through policies and procedures to achieve objectives and respond to risks in the internal control system as part of the control activities component. [↑](#footnote-ref-3)
4. The term transaction tends to be associated with business processes addressing reporting objectives (e.g., financial reporting of accounts payable transactions), while the term activity is more often associated with operations or compliance objectives. For the purposes of this manual, “transactions” covers both definitions. [↑](#footnote-ref-4)
5. The financial statement control objectives relate to each identified risk of material misstatement at the assertion level for which inherent risk is more than remote. [↑](#footnote-ref-5)
6. The degree of interaction refers to the extent to which an entity can and elects to implement effective controls over transactions that the external party processes. [↑](#footnote-ref-6)
7. An information system authorization boundary comprises all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems connected to the information system. Business process applications may be separately authorized or included within a larger information system authorization boundary. [↑](#footnote-ref-7)
8. Executive Order No.13556, *Controlled Unclassified Information* (Nov. 4, 2010) (reprinted in 75 Fed. Reg. 68,675 (Nov. 9, 2010), establishes an open and uniform program for managing unclassified information requiring safeguarding or dissemination controls. The National Archives and Records Administration (NARA), which the order directed to implement and oversee the controlled unclassified information (CUI) program, issued a final rule on September 14, 2016, that became effective on November 14, 2016. See 81 Fed. Reg. 63,324 (Sept. 14, 2016), which is codified at 32 C.F.R. part 2002. NARA’s CUI regulations define CUI as information the that the federal government creates or possesses, or that an entity creates or possesses for or on behalf of the federal government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. According to NARA’s regulations, CUI information may be designated as basic or specified depending on whether specific handling or dissemination controls are required by specific authorizing law, regulation, or government-wide policy. See 2 C.F.R. § 2002.4. [↑](#footnote-ref-8)
9. FFMIA, *reprinted in* 31 U.S.C. § 3512 note. FFMIA only applies to the 15 executive departments and additional nine large executive agencies listed in 31 U.S.C. § 901(b). [↑](#footnote-ref-9)
10. 31 U.S.C. § 3512 (c), (d), commonly known as the Federal Managers’ Financial Integrity Act or FMFIA. [↑](#footnote-ref-10)
11. National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems, FIPS 199 (Gaithersburg, Md.: March 2004). [↑](#footnote-ref-11)