United States Government Accountability Office

July 2023

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)

2023 Exposure Draft

Accessible Version

GAO-23-104975

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 20, 2023

To Federal Officials and Others Interested in the *Federal Information System Controls Audit Manual*

GAO invites your comments on the proposed changes to the *Federal Information System Controls Audit Manual* (FISCAM). This letter identifies the major proposed changes and provides instructions for submitting comments on the proposed methodology.

GAO first issued FISCAM in 1999 and last issued a revision in February 2009. When issued in final form, this revision will supersede the February 2009 revision. The effective date for this revision will be included when it is issued in final form.

The proposed changes in the 2023 exposure draft update FISCAM to (1) address responses received through focus groups and interviews with internal and external officials, stakeholders, and users and (2) reflect changes in relevant auditing standards, guidance, control criteria, and technology since the last revision. Enclosure I to this letter contains a summary of the major proposed changes. In addition, GAO is developing a separate performance audit guide to focus on assessing controls designed, implemented, and operated to mitigate cybersecurity risks.

We are requesting comments on this draft from federal, state, and local government officials; managers and auditors at all levels of government; professional organizations; public interest groups; and other interested parties. To assist you in developing your comments, specific questions are presented in enclosure II to this letter along with a link for a fillable form. We encourage you to respond to these questions and comment on any additional issues that you note.

Please send your comment letters to our FISCAM inbox, FISCAM@gao.gov, no later than October 18, 2023. If you need additional information, please contact me at (202) 512-3406 or FISCAM@gao.gov.

Dawn Simpson

Dawn B. Simpson
Director, Financial Management and Assurance

Enclosures – 2

This exposure draft updates the *Federal Information System Controls Audit Manual* (FISCAM) to reflect changes in relevant auditing standards, guidance, control criteria, and technology since the last revision. The summary of major proposed changes below focuses on those changes that meaningfully affect the FISCAM methodology and does not include minor editorial changes.

Changes to the Format, Design, and Organization

Enhance the usability of the manual. The 2023 FISCAM exposure draft proposes to reformat, redesign, and reorganize FISCAM to enhance its usability. The major proposed changes to the format include the use of numbered sections, numbered paragraphs, and subheadings. Other major proposed changes to the design and organization of the manual are discussed below.

- The 2023 FISCAM exposure draft proposes four sections that include new and existing content from chapters 1 and 2 of extant FISCAM. Section 100, Introduction, provides an overview of the FISCAM methodology. Section 200, Planning Phase, includes auditor requirements, guidance, and procedures for planning an information system (IS) controls assessment, including identifying relevant IS control objectives. Section 300, Testing Phase, includes auditor requirements, guidance, and procedures for identifying IS controls for testing and determining the nature, extent, and timing of IS control tests. Section 400, Reporting Phase, includes auditor requirements and guidance for communicating the results of the IS controls assessment.
- The 2023 FISCAM exposure draft proposes the following three appendixes included as section 500:
    - Appendix 500A, FISCAM Glossary, updates extant FISCAM appendix XI, Glossary.
    - Appendix 500B, FISCAM Framework, updates the tables containing critical elements, control activities, control techniques, and suggested audit procedures from extant FISCAM chapters 3 and 4.
    - Appendix 500C, FISCAM Assessment Completion Checklist, provides new content that assists auditors with determining whether the FISCAM methodology was followed.
- Given the potential for revisions to address public comments, the 2023 FISCAM exposure draft does not include figures, such as those included in extant FISCAM. However, we anticipate the final product will include figures derived from the final product content. We are requesting feedback on the types of information that may be useful to provide in the form of figures.

Changes to the Methodology and Framework

Simplify the FISCAM Framework. The extant FISCAM includes 14 control categories: five general control categories, five application security control categories aligning with the general control categories, and four business process application-level control categories. The 2023 FISCAM exposure draft proposes to combine the general and application security control categories in extant FISCAM into five general control categories: security management, access controls, segregation of duties, configuration management, and contingency planning. The 2023 FISCAM exposure draft also proposes to reorganize the business process, interface, and data management system control activities in extant FISCAM. Such control activities are collectively

renamed business process controls and consist of the user, application, and general control activities related to specific business processes (e.g., management of business process applications, interfaces, and data management systems).

Align the FISCAM Framework with relevant criteria. The extant FISCAM includes appendix IV, Mapping of FISCAM to NIST SP 800-53 and Other Related NIST Publications. This appendix maps each extant critical element to relevant controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*.[1] The 2023 FISCAM exposure draft includes appendix 500B, FISCAM Framework. This framework provides a more granular mapping of each illustrative control activity to relevant controls from NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.[2] Moreover, each control from NIST SP 800-53 is addressed by one or more illustrative control activities in the FISCAM Framework.

Clarify the use of the FISCAM Framework. The extant FISCAM generally requires auditors to determine whether IS controls are effective in achieving the FISCAM control categories. This generally involves assessing IS controls within each critical element of the control category. The 2023 FISCAM exposure draft does not require summary-level conclusions for each FISCAM control category but proposes to require auditors to (1) identify relevant IS control objectives and (2) test IS control activities sufficient to conclude on whether such control objectives are achieved. For federal financial audits, the auditor is required to identify relevant control objectives that support the auditor's overall assessment of internal control over financial reporting. The FISCAM Framework (app. 500B) presents an objectives-based control framework to assist the auditor in (1) identifying relevant IS control objectives and (2) selecting the IS control activities (or a combination of IS control activities) that are likely to achieve the relevant IS control objectives and are most efficient for testing. The *GAO and Council of the Inspectors General for Integrity and Efficiency Financial Audit Manual* (FAM) establishes a basis for determining relevant IS control objectives for financial audits.[3] The auditor is expected to use professional judgment to tailor the audit procedures as appropriate.

Changes Relevant to Professional Auditing Standards and Guidance

Incorporate changes to auditing standards since 2009. Changes to relevant auditing standards since FISCAM was last issued in 2009 are incorporated. The 2023 FISCAM exposure draft incorporates by reference generally accepted government auditing standards (GAGAS).[4]

[1]National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, rev. 2 (Gaithersburg, Md.: December 2007).
[2]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, rev. 5 (Gaithersburg, Md.: September 2020).
[3]GAO and Council of the Inspectors General for Integrity and Efficiency, *Financial Audit Manual*, vol. 1, GAO-22-105894 (Washington, D.C.: June 2022, updated May 2023); *Financial Audit Manual*, vol. 2, GAO-22-105895 (Washington, D.C.: June 2022, updated May 2023); and *Financial Audit Manual*, vol. 3, GAO-21-105127 (Washington, D.C.: September 2021, updated June 2023).
[4]GAO, *Government Auditing Standards: 2018 Revision*, GAO-21-368G (Washington, D.C.: July 2018, updated April 2021).

Clarify auditor requirements. The FISCAM exposure draft clarifies auditor requirements by removing "generally" and limiting the use of "must" and "should." "Must" indicates unconditional requirements that come directly from GAGAS. "Should" indicates requirements GAO has determined are mandatory when the circumstances exist to which the requirement is relevant, except in rare circumstances when the specific procedure to be performed would be ineffective in achieving the intent of the requirement.

Changes to Relevant Control Criteria

Incorporate changes to relevant control criteria since 2009. Changes to relevant control criteria since FISCAM was last issued in 2009 are incorporated where appropriate. The critical elements and control objectives included within the FISCAM Framework presented in appendix 500B are consistent with the principles and attributes included in *Standards for Internal Control in the Federal Government* (Green Book).[5] Additionally, the illustrative control activities included within the FISCAM Framework address information security and privacy control requirements presented in NIST Computer Security Resource Center publications—and specifically include all information security and privacy control requirements presented in NIST SP 800-53.[6]

[5]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).
[6]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, rev. 5 (Gaithersburg, Md.: September 2020).

We encourage you to comment on the following discussion items and any additional items that you note when reviewing the 2023 *Federal Information System Controls Audit Manual* (FISCAM) exposure draft. Please use the fillable form to associate your comments with specific questions and section and paragraph numbers. We request that you provide your rationale for any proposed changes along with suggested revised language.

1. The 2023 FISCAM exposure draft proposes to simplify the FISCAM Framework by consolidating and reorganizing certain control categories, objectives, and activities. The 2023 FISCAM exposure draft also proposes to clarify the use of the FISCAM Framework through enhanced auditor requirements and application guidance.

   Please comment on how these updates to the FISCAM Framework are likely to affect the auditor's ability to evaluate IS controls to the extent necessary to support the achievement of the engagement objectives. Specifically, please comment on the clarity and appropriateness of the auditor requirements and application guidance for:

   a. identifying relevant information system (IS) control objectives for each area of audit interest in section 240 and section 270;[1]

   b. selecting IS control activities (or a combination of IS control activities) that are likely to achieve the relevant IS control objectives and are most efficient for testing in section 320; and

   c. determining whether sufficient, appropriate evidence for the design, implementation, and operating effectiveness of IS controls has been obtained to the extent necessary to support the achievement of the engagement objectives in section 340.

2. The 2023 FISCAM exposure draft includes a FISCAM Assessment Completion Checklist to help auditors determine whether they have followed FISCAM requirements.

   Please comment on

   a. the usefulness of this checklist in helping auditors determine whether they have followed FISCAM requirements and

   b. any enhancements to improve it.

3. The 2023 FISCAM exposure draft presents expanded guidance for assessing IS controls that external entities, including service organizations, perform on behalf of the entity.

[1]Areas of audit interest are a subset of the entity's information systems, information system components, and information system resources that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. At the business process level, areas of audit interest may include business process applications, 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.

This guidance was removed from extant FISCAM appendix VII, Entity's Use of Service Organizations, and incorporated throughout sections 200, 300, and 400.

Please comment on how these changes are likely to affect the auditor's ability to assess IS controls that external entities perform.

4. The 2023 FISCAM exposure draft does not include graphics, tools, or templates.

   Please comment on where graphics, tools, or templates may provide clarity.

GAO Project Team

Financial Management and Assurance

Dawn B. Simpson, Director
Nicole Burkart, Assistant Director
Rebecca L. Perkins, Auditor in Charge
Christopher J. Pfau, Senior Auditor
Beryl H. Davis, Managing Director

Applied Research and Methods

Robert F. Dacey, Chief Accountant

Information Technology and Cybersecurity

Vijay A. D'Souza, Director
Mark J. Canter, Assistant Director
Daniel M. Swartz, Assistant Director

CONTENTS

Contents

Abbreviations

ACL	access control list
AICPA	American Institute of Certified Public Accountants
AT-C	AICPA Codification of *Statements on Standards for Attestation Engagements*
AU-C	AICPA Codification of *Statements on Auditing Standards*
CAAT	computer-assisted audit technique
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CNSS	Committee on National Security Systems
CONOPS	concept of operations
DISA	Defense Information Systems Agency
DHS	Department of Homeland Security
DOD	Department of Defense
FAM	GAO/CIGIE Financial Audit Manual
FFMIA	Federal Financial Management Improvement Act of 1996
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014 and/or the Federal Information Security Management Act of 2002
FMFIA	Federal Managers' Financial Integrity Act
GAGAS	generally accepted government auditing standards
IS	information system
ISACA	Information Systems Audit and Control Association
IT	information technology
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
NSS	national security system
OMB	Office of Management and Budget
PKI	public key infrastructure
SDLC	software development life cycle
SP	Special Publication
STIG	Security Technical Implementation Guide
SRS	simple random selection
SYS	systematic random selection

SECTION 100

INTRODUCTION

Contents of the Introduction

110 Purpose and Applicability

.01 The *Federal Information System Controls Audit Manual* (FISCAM) presents a methodology for assessing the design, implementation, and operating effectiveness of information system (IS) controls. Generally accepted government auditing standards (GAGAS) define IS controls as internal controls that depend on information system processing.[8] IS controls include user, application, and general controls. This manual uses the term "IS controls assessment" to refer to the auditor's assessment of IS controls using FISCAM.

.02 The purpose of the IS controls assessment is to evaluate the design, implementation, and operating effectiveness of IS controls to the extent necessary to support the achievement of the engagement objectives. IS controls assessments can also be performed to support the engagement team's conclusions regarding the reliability of information that information systems produce that is intended to materially support findings, conclusions, or recommendations. IS controls assessments conducted in accordance with FISCAM are performed as part of a financial audit, attestation engagement, or performance audit.

.03 The FISCAM methodology is designed to be applied to a wide variety of IS controls assessments, and is to be used in connection with federal financial statement audits and attestation engagements. FISCAM may be used for performance audits when the engagement objectives include assessing the effectiveness of business process application controls, similar to an assessment performed for financial audits.

.04 A wide range of auditors and audit organizations that conduct IS controls assessments of federal entities and programs, as well as audits of nonfederal entities that collect, process, or maintain information on behalf of federal entities, may use this manual.[9] IS controls assessments are generally performed by IS controls auditors—auditors with technical expertise and experience in IS controls auditing. However, other auditors with appropriate training, expertise, and supervision may undertake specific tasks performed as part of the IS controls assessment. Throughout this manual, the term "auditor" means either an (1) IS controls auditor or (2) other auditor working in consultation with or under the supervision of an IS controls auditor.

[8]GAO, *Government Auditing Standards: 2018 Revision*, GAO-21-368G (Washington, D.C.: July 2018, updated April 2021) para. 8.63.
[9]For FISCAM purposes, nonfederal entities include state, local, territorial, and tribal governments; nonprofits; and for-profit organizations.

120 IS Control Concepts

.01 This section describes IS control concepts used throughout FISCAM. It defines IS controls, describes the types of IS controls, and defines control objectives for each type. The section also contains information about the levels at which these controls may be implemented.

Types of IS Controls and Control Objectives

.02 IS controls are those internal controls that depend on information system processing.[10] IS controls include the following:

- User controls – Portions of controls that are performed by people interacting with information systems. A user control is an IS control if its effectiveness depends on information system processing.
- Application controls – Controls that are incorporated directly into application software, including controls over the input, processing, and output of data.
- General controls – The policies and procedures that apply to all or a large segment of an entity's information systems.[11]

FISCAM organizes IS controls as business process controls or general controls based on whether they have a direct or indirect effect on information processing objectives (completeness, accuracy, and validity).

.03 Business process controls consist of those user, application, and general controls that are designed to achieve one or more of the following information processing objectives:

- Completeness – All transactions and events that should have been recorded have been properly recorded at each stage of processing.
- Accuracy – Data relating to transactions and events are properly and timely recorded at each stage of processing.
- Validity – All recorded transactions and events that actually occurred are related to the entity and were executed according to prescribed procedures.

When designed, implemented, and operating effectively, business process controls reasonably assure the completeness, accuracy, and validity of transactions, events, and data. General controls included as business process controls in FISCAM are those that directly support the effective operation of user and application controls, which are designed to achieve information processing objectives.

.04 General controls are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls in FISCAM exclude those that directly support the effective operation of user and application controls,

[10]GAO-21-368G, para. 8.63.
[11]GAO-21-368G, para. 8.63(a),(b),(c).

which are included in FISCAM as business process controls. General controls create a suitable environment to support the effective operation of business process controls. General controls may be designed to achieve one or more of the following information security objectives:

- Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- Integrity – Guarding against improper information modification or destruction, which includes ensuring information's nonrepudiation and authenticity.[12] A loss of integrity is the unauthorized modification or destruction of information.
- Availability – Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

.05 General controls include security management, logical and physical access controls (access controls), segregation of duties, configuration management, and contingency planning.[13]

.06 Security management is the foundation of a security-control structure and reflects senior management's commitment to addressing security risks. Information security management programs provide a framework and continuous cycle of activity for managing risk, developing and implementing effective security policies, assigning responsibilities, and monitoring the adequacy of the entity's IS controls. Without a well-designed information security management program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

.07 Access controls limit access or detect inappropriate access to information system resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Logical access controls require users to authenticate themselves and limit the files and other resources that authenticated users can access and the actions that they can execute. Physical access controls involve restricting physical access to information system resources and protecting them from intentional or unintentional loss or impairment.

.08 Segregation of duties controls include having policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations and thereby prevent unauthorized actions or unauthorized access to assets or records. Segregation of duties involves segregating work responsibilities so that one individual does not control all critical stages of a

[12]Nonrepudiation is protection against an individual falsely denying having performed a particular action. It provides the capability to determine whether a given individual took a particular action, such as creating information, sending a message, approving information, and receiving a message.
[13]GAO-21-368G, para. 8.63(a).

process. Effective segregation of duties is achieved by splitting responsibilities between two or more individuals or organizational units. In addition, dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

.09 Configuration management controls involve identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically control changes to that configuration during the system's life cycle. Configuration management controls that are designed and implemented effectively prevent unauthorized or untested changes to information system resources and provide reasonable assurance that systems are securely configured and operated as intended.

.10 In addition, configuration management controls that are designed and implemented effectively provide reasonable assurance that software programs and changes to software programs go through a formal, documented systems development process that identifies all changes to the baseline configuration.[14] To reasonably assure that changes to information systems are necessary, work as intended, and do not result in the loss of data or program integrity, such changes are authorized, documented, tested, and independently reviewed.

.11 Contingency planning controls provide for the continuation of critical or essential mission and business functions in the event of a system disruption, compromise, or failure and the restoration of the information system following a system disruption. Contingency planning involves protecting against losing the capability to process, retrieve, and protect electronically maintained information. Effective contingency planning is achieved by having procedures for protecting information system resources and minimizing the risk of unplanned interruptions. It also involves having a plan to recover and reconstitute information systems should system disruptions occur.

Implementation Levels for IS Controls

.12 IS controls may be applied at the business process, system, and entity levels. Each level is described below.

- Business process level refers to user, application, and general controls applied to a specific business process. These controls are specific to a business process and often correspond to information system components applied to the business process—business process applications, interfaces, and data management systems.
- System level refers to IS general controls applied to an information system. These controls are more specific than those applied at the entity level and often correspond to one of three sublevels inherent in all information systems: infrastructure, platform, and software:

[14]A documented set of specifications for an information system or a configuration item within a system that has been formally reviewed and agreed on at a given point in time and can be changed only through change control procedures.

  - Infrastructure comprises the physical information system resources necessary to run software and includes the hardware devices used for information processing, data storage, and network communication. Infrastructure also includes the logical information system resources necessary to run multiple virtual machines on shared physical information system resources.
  - Platform comprises the logical information system resources necessary to run application software, including the operating system and related computer programs, tools, and utilities.
  - Software comprises application software, access control software, and other software.
- Entity level refers to IS general controls applied to the entity or component as a whole.

130 Overview of the FISCAM Methodology

.01 This section describes the organization, content, and other general information about FISCAM. It contains summary information about each of the manual's sections. This section also contains information about technology neutrality and future revisions.

Organization and Content

.02 FISCAM is organized into the following five sections:

- Section 100 – Introduction
- Section 200 – Planning Phase
- Section 300 – Testing Phase
- Section 400 – Reporting Phase
- Section 500 – Appendixes

.03 Section 100 introduces FISCAM. In addition to describing the purpose and applicability of FISCAM, section 100 identifies applicable audit and attestation standards, identifies applicable criteria, explains IS control concepts, and describes the objectives-based control framework. Section 100 does not include auditor requirements.

.04 Sections 200, 300, and 400 comprise the FISCAM methodology and specific auditor requirements and guidance for conducting the planning, testing, and reporting phases of the IS controls assessment. The overall objective and approach for each phase are discussed below.

.05 Section 500 includes three appendixes that contain supplementary information to assist the auditor in applying the FISCAM methodology.

- Appendix 500A, FISCAM Glossary, defines the terms used throughout FISCAM.
- Appendix 500B, FISCAM Framework, presents an objectives-based control framework to assist the auditor in identifying relevant IS control objectives and selecting IS control activities (or a combination of IS control activities) that are likely to achieve the relevant IS control objectives and are most efficient for testing. The FISCAM Framework presents control categories, critical elements, control objectives, and illustrative control activities in a hierarchical structure to facilitate the auditor's planning, testing, and reporting procedures. The FISCAM Framework links each illustrative control activity to relevant criteria and provides illustrative audit procedures for each control activity.
- Appendix 500C, FISCAM Assessment Completion Checklist, is designed to help auditors determine whether they have complied with FISCAM requirements.

Planning Phase

.06 The overall objective of the planning phase is to determine an effective and efficient approach for obtaining sufficient, appropriate evidence for design, implementation, and operating effectiveness of IS controls to the extent

necessary to support the achievement of the engagement objectives and report on the results.

.07 During the planning phase, the auditor

- assigns a combination of auditors and specialists to the engagement team who collectively possess the competence needed to address the engagement objectives;
- communicates the engagement information with management, those contracting for or requesting audit services, oversight committees, and those charged with governance;
- obtains an understanding of the entity's operations sufficient to identify the business processes that are significant to the engagement objectives; and
- obtains an understanding of the significant business processes by performing walk-throughs and through other methods. As part of this, the auditor
  - gathers information on the design and implementation of business process controls relevant to the significant business processes and
  - begins to identify areas of audit interest.

.08 Identifying areas of audit interest at the business process and system levels enables the auditor to establish an appropriate basis for defining the scope of the IS controls assessment. Areas of audit interest are a subset of the entity's information systems, information system components, and information system resources that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. At the business process level, areas of audit interest may include business process applications, interfaces, and 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.

.09 By identifying areas of audit interest, the auditor may concentrate efforts on them and reduce work associated with other areas. The process for identifying areas of audit interest begins with the auditor's understanding of the significant business processes and continues throughout the planning phase as the auditor gathers additional information on the business process applications, interfaces, and data management systems involved in the significant business processes.

.10 With the understanding obtained, the auditor uses the FISCAM Framework to (1) identify relevant IS control objectives for each area of audit interest, (2) obtain an understanding of the entity's information security management program, and (3) determine the likelihood that IS control activities will effectively achieve the relevant IS control objectives. Relevant IS control objectives, as used in FISCAM, are those that are necessary to support the achievement of the engagement objectives. FAM establishes a basis for determining relevant control objectives for financial audits. The auditor uses the

- FISCAM Framework for Business Process Controls (app. 500B, table 8) to identify (1) relevant user and application control objectives and (2)

relevant general control objectives for key areas of audit interest at the business process level;

- FISCAM Framework for Security Management (app. 500B, table 9) to (1) obtain an understanding of the entity's information security management program, (2) identify relevant security management control objectives for key areas of audit interest at the system level (i.e., infrastructure, platform, and software), and (3) determine the likelihood that security management control activities will effectively achieve the relevant IS control objectives;
- FISCAM Framework for Access Controls (app. 500B, table 10) to (1) identify relevant access control objectives for key areas of audit interest at the system level and (2) determine the likelihood that access control activities will effectively achieve the relevant IS control objectives;
- FISCAM Framework for Segregation of Duties (app. 500B, table 11) to (1) identify relevant segregation of duties control objectives for key areas of audit interest at the system level and (2) determine the likelihood that segregation of duties control activities will effectively achieve the relevant IS control objectives;
- FISCAM Framework for Configuration Management (app. 500B, table 12) to (1) identify relevant configuration management control objectives for key areas of audit interest at the system level and (2) determine the likelihood that configuration management control activities will effectively achieve the relevant IS control objectives; and
- FISCAM Framework for Contingency Planning (app. 500B, table 13) to (1) identify relevant contingency planning control objectives for key areas of audit interest at the system level and (2) determine the likelihood that contingency planning control activities will effectively achieve the relevant IS control objectives.

.11 The auditor then preliminarily assesses IS risk, which is the auditor's combined assessment of inherent risk and control risk related to the areas of audit interest. See section 260 for further discussion of the auditor's preliminary assessment of IS risk. The auditor's preliminary assessment of IS risk enables the auditor to establish an appropriate basis for planning the engagement to reduce audit risk to an acceptably low level. The auditor's preliminary assessment of IS risk informs the auditor's decisions regarding the nature, extent, and timing of IS control tests.

.12 The auditor also determines the likelihood of effective general controls relevant to the areas of audit interest. This determination informs the nature, extent, and timing of (1) general control tests and (2) user and application control tests. Additionally, for federal financial audits, the likelihood of effective general control activities relevant to the areas of audit interest also informs the nature, extent, and timing of non-IS control tests.

Testing Phase

.13 The overall objective of the testing phase is to obtain sufficient, appropriate evidence for the design, implementation, and operating effectiveness of IS controls to the extent necessary to support the achievement of the engagement objectives.

.14 During the testing phase, the auditor develops test plans to assist the auditor in obtaining sufficient, appropriate evidence to conclude on whether the entity's IS controls are designed, implemented, and operating effectively to achieve the relevant IS control objectives for each of the areas of audit interest. When developing test plans, the auditor uses the FISCAM Framework to identify and select IS controls for testing. When selecting user, application, and general control activities for testing, the auditor considers the extent to which control dependencies exist between such controls and the potential affect they may have on achieving the related IS control objectives. A control dependency exists when the effectiveness of a control activity depends on the effectiveness of other control activities. For example, the effectiveness of a configurable control within application software will depend on the design of the application control, as well as related access and configuration management general controls designed to prevent or detect unauthorized changes to the control. The auditor also considers the likelihood that such IS control activities will be designed, implemented, and operating effectively. Once the auditor has selected the IS control activities that are likely to achieve the relevant IS control objectives and are most efficient for testing, the auditor determines the nature, extent, and timing of IS control tests.

.15 The auditor then performs control tests of the selected IS control activities using suitable criteria, determines whether the control activities tested are effective in achieving the relevant IS control objectives for the areas of audit interest, and performs an overall assessment of the evidence obtained. In performing an overall assessment of the collective evidence obtained throughout the IS controls assessment, the auditor reassesses IS risk and determines whether the audit procedures performed are adequate to reduce audit risk to an acceptably low level.

Reporting Phase

.16 The overall objective of the reporting phase is to determine the auditor's compliance with FISCAM requirements and to communicate the results of an engagement.

Other Information

Technology

.17 The FISCAM methodology is technology neutral so that it can be applied without modification to a wide variety of IS controls assessments.

Auditor Responsibility for Interim Changes

.18 IS control-related criteria change periodically. The auditor is responsible for monitoring any changes to IS control-related criteria and considering the effect of such changes on FISCAM methodology.

140 Applicable Auditing and Attestation Standards and Requirements

.01 In conducting the IS controls assessment in accordance with GAGAS, GAGAS requirements and guidance apply based on the type of engagement the auditor performs.

- For financial audits, the requirements and guidance in GAGAS chapters 1 through 6 and American Institute of Certified Public Accountants (AICPA) Statements on Auditing Standards apply. GAGAS incorporates by reference AICPA Statements on Auditing Standards for financial audits. However, FISCAM does not incorporate, directly or by reference, any specific auditor requirements presented in the statements. It is incumbent upon the auditor and audit organization to ensure that AICPA professional auditing standards are met when conducting financial audits in accordance with GAGAS.
- For attestation-level examination, review, and agreed-upon procedures engagements, the requirements and guidance in GAGAS chapters 1 through 5 and 7 and AICPA Statements on Standards for Attestation Engagements apply. GAGAS incorporates by reference AICPA Statements on Standards for Attestation Engagements for attestation engagements. However, FISCAM does not incorporate, directly or by reference, any specific auditor requirements presented in the statements. It is incumbent upon the auditor and audit organization to ensure that AICPA professional auditing standards are met when conducting attestation engagements in accordance with GAGAS.
- For performance audits, the requirements and guidance in GAGAS chapters 1 through 5, 8, and 9 apply. GAGAS does not incorporate other standards by reference, but recognizes that auditors may use or may be required to use other professional standards in conjunction with GAGAS.

.02 FISCAM incorporates by reference the GAGAS requirements presented in chapters 1 through 9. Where appropriate, FISCAM expands on certain GAGAS requirements to provide additional guidance for the IS controls assessment. FISCAM does not specifically cite applicable GAGAS requirements. However, the auditor and audit organization are responsible for meeting all applicable requirements when conducting an engagement in accordance with GAGAS.

.03 For federal financial audits, FISCAM is to be used in conjunction with the *GAO and Council of the Inspectors General for Integrity and Efficiency Financial Audit Manual* (FAM).[15] FAM includes references to the AICPA's Clarified Statements on Auditing Standards (AU-C) and Clarified Statements on Standards for

[15]GAO and Council of the Inspectors General for Integrity and Efficiency, *Financial Audit Manual*, vol. 1, GAO-22-105894 (Washington, D.C.: June 2022, updated May 2023); *Financial Audit Manual*, vol. 2, GAO-22-105895 (Washington, D.C.: June 2022, updated May 2023); and *Financial Audit Manual*, vol. 3, GAO-21-105127 (Washington, D.C.: September 2021, updated June 2023).

Attestation Engagements (AT-C). FISCAM refers to FAM for additional requirements and guidance, as appropriate.

.04 FISCAM does not incorporate directly or by reference any specific auditor requirements from other professional auditing standards, but recognizes that auditors may use or may be required to use other professional auditing standards in conjunction with FISCAM, such as the *IT Audit Framework* published by ISACA (formerly the Information Systems Audit and Control Association).[16]

.05 The following terms are used in FISCAM to describe the degree of responsibility the corresponding statements impose on auditors and audit organizations:

- **Must**. Compliance is mandatory when the circumstances exist to which the requirement is relevant. “Musts” indicate unconditional requirements that come directly from professional auditing standards.
- **Should**. Compliance is mandatory when the circumstances exist to which the requirement is relevant, except in rare circumstances when the specific procedure to be performed would be ineffective in achieving the intent of the requirement. The auditor documents (1) the justification for any departure and (2) how the alternative audit procedures performed were sufficient to achieve the intent of the requirement or policy.
- **May**. Compliance is optional. “May” is used in FISCAM to provide further explanation of and guidance for implementing auditor requirements.

.06 When these or similar terms are used to describe management or entity actions (rather than actions of the auditor or audit organization), the general meaning of the terms is intended.

[16]ISACA, *IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit*, 4th ed. (Schaumburg, Ill.: 2020).

150 Applicable Criteria

.01 Criteria identify the required or desired state or expectation with respect to the program or operation of internal controls. Suitable criteria are relevant, reliable, objective, and understandable and do not result in the omission of significant information, as applicable, to the engagement objectives. Criteria may include the statutes, regulations, executive orders, implementing entity guidance, directives, policies, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated.

.02 Criteria that are commonly applied to IS controls assessments conducted in accordance with FISCAM are discussed below. The engagement team is responsible for identifying and understanding additional criteria that may be applicable to the engagement.

Internal Control Standards

.03 The Federal Managers' Financial Integrity Act (FMFIA)[17] requires federal executive entity management to establish internal accounting and administrative controls consistent with internal control standards prescribed by the Comptroller General. These standards are presented in the *Standards for Internal Control in the Federal Government* (Green Book).[18] The Green Book prescribes these standards and provides criteria for assessing the design, implementation, and operating effectiveness of internal control in federal entities to determine if an internal control system is effective. The Green Book applies to all of an entity's objectives: operations, reporting, and compliance. In implementing the Green Book, management is responsible for designing the policies and procedures to fit an entity's circumstances and building them in as an integral part of the entity's operations.

.04 The critical elements and control objectives included within the FISCAM Framework presented in appendix 500B are consistent with the principles and attributes included in the Green Book.

Office of Management and Budget Information and Guidance

.05 Under the Federal Information Security Modernization Act of 2014 (FISMA),[19] the Office of Management and Budget (OMB), in coordination with the Department of Homeland Security (DHS), is responsible for overseeing civilian executive entity

---

[17]31 U.S.C. § 3512(c), (d).
[18]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).
[19]Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (codified at 44 U.S.C. §§ 3551–3558). This 2014 statute largely superseded the similar Federal Information Security Management Act of 2002, Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (Dec. 17, 2002). A number of FISMA provisions, such as those codified as 44 U.S.C. § 3553 (authority and functions of the OMB Director and the Secretary of Homeland Security) and 44 U.S.C. § 3554 (federal agency responsibilities), establish requirements in reference to the standards developed by NIST and promulgated by the Secretary of Commerce under 40 U.S.C. § 11331.

information security policies and practices based on standards developed by the National Institute of Standards and Technology (NIST) and promulgated by the Secretary of Commerce.[20] OMB uses circulars, bulletins, and memoranda to provide information and guidance, including in areas applicable to information security. OMB information and guidance are published at https://www.whitehouse.gov/omb/information-for-agencies. The following circulars provide guidance that establish information security requirements for federal executive entities:

- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, defines management's responsibilities for enterprise risk management and internal control and requires agencies to integrate these functions.[21]
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*, establishes general policy for the planning, budgeting, governance, acquisition, and management of federal information, workforce, equipment, information technology resources, and supporting infrastructure and services.[22] It also touches on many specific information resources management issues (e.g., privacy, confidentiality, information quality, dissemination, and statistical policy) that are covered more fully in other OMB policy guidance.

NIST Standards and Guidelines

.06 OMB Circular No. A-130 requires federal executive entities to apply the standards and guidelines contained in NIST Federal Information Processing Standards (FIPS) and NIST Special Publications (SP) (e.g., 800 series guidelines) and, where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIR).[23] These standards and guidelines are published at https://csrc.nist.gov/publications.The following standards and guidelines are fundamental to information security requirements, risk assessments, and security and privacy controls for federal executive entities.

Federal Information Processing Standards

.07 NIST develops FIPS for federal information systems in accordance with FISMA. NIST develops these standards and guidelines when there are no acceptable industry standards or solutions for a particular government requirement. NIST

[20]NIST is established within the Department of Commerce as a science, engineering, technology and measurement laboratory and has a statutory role in developing standards and guidelines for federal information systems. 15 U.S.C. §§ 272(a), 278g-3. The Secretary of Commerce has authority for promulgating standards and guidelines pertaining to federal information systems, other than national security systems. 40 U.S.C. § 11331.
[21]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular A-123 (Washington, D.C.: July 15, 2016).
[22]Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (Washington, D.C.: July 15, 2016).
[23]Office of Management and Budget, *Managing Information as a Strategic Resource*, pp. 18, App. I-4.

issues FIPS after approval by the Secretary of Commerce. The applicability section of each FIPS details when a standard is applicable and mandatory.

.08 Pursuant to FISMA, NIST developed and issued the following mandatory FIPSs that are fundamental to categorizing information and information systems and defining minimum security requirements for those systems:

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, establishes standards for the security categorization of federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.[24] Security categories are established for both information and information systems.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, establishes minimum security requirements for information and information systems.[25] The minimum security requirements cover security-related areas that support protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

.09 FIPS publications do not apply to national security systems.[26] The Committee on National Security Systems is responsible for providing system security guidance for national security systems.

Special Publications

.10 The following NIST SPs are fundamental to information system risk management, as well as selecting and implementing appropriate information security and privacy controls:

- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* provides a process that includes preparing an organization to manage its security and privacy risks, categorizing information systems and information, selecting security controls, implementing security

[24]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199 (Gaithersburg, Md.: March 2004).
[25]National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Gaithersburg, Md.: March 2006).
[26]FISMA (44 U.S.C. § 3552) defines a national security system (NSS) as any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. NSS does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). A number of FISMA provisions, such as those codified as sections 3553 and 3554 of Title 44, U.S. Code, establish requirements related to 40 U.S.C. § 11331, which specifically excludes national security systems.

controls, assessing security controls, authorizing information systems, and monitoring the security and privacy posture of the information system and the organization.[27] While mandatory for federal agencies, the NIST Risk Management Framework may be applied to any type of nonfederal organization (e.g., business, industry, and academia). As such, state, local, territorial, and tribal governments as well as private sector organizations are encouraged to use these guidelines on a voluntary basis, as appropriate.

- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organization*s, provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the United States from a diverse set of threats and risks.[28] FIPS 200 mandates the use of NIST SP 800-53 to develop a baseline of security controls for information systems. The control baselines that have previously been included in NIST SP 800-53 have been relocated to NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*.[29] NIST SP 800-53B contains security and privacy control baselines for federal information systems and organizations and provides guidance for tailoring control baselines and for developing overlays to support the security and privacy requirements of stakeholders and their organizations.
- NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, provides guidance for implementing security controls using security configuration checklists specific to IT products or categories of IT products for an operational environment.[30] A security configuration checklist provides a series of instructions or procedures for configuring an IT product to a particular operational environment based on knowledge of security threats and vulnerabilities.

.11 The illustrative control activities included within the FISCAM Framework address information security and privacy control requirements presented in NIST Computer Security Resource Center publications—and specifically include all information security and privacy control requirements presented in NIST SP 800-53.

[27]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, rev. 2 (Gaithersburg, Md.: December 2018).
[28]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, rev. 5 (Gaithersburg, Md.: September 2020).
[29]National Institute of Standards and Technology, *Control Baselines for Information Systems and Organizations*, SP 800-53B (Gaithersburg, Md.: December 2020).
[30]National Institute of Standards and Technology, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, SP 800-70, rev. 4 (Gaithersburg, Md.: December 2018).

DHS Directives and Defense Information Systems Agency Security Technical Implementation Guides

.12 Under FISMA, DHS, in consultation with OMB, is responsible for administering civilian executive entity information security policies, including developing and overseeing the implementation of binding operational directives to agencies to implement these policies; monitoring entities' compliance with those policies; and assisting OMB in developing those policies.[31] DHS's Cybersecurity and Infrastructure Security Agency (CISA) develops and oversees the implementation of binding operational directives and emergency directives. These directives cover entity-wide and infrastructure policies to address cybersecurity vulnerabilities for certain federal entities. These directives are published at https://www.cisa.gov/news-events/directives.

.13 Under FISMA, (1) the Department of Defense (DOD) is responsible for overseeing non-civilian executive entity information security policies for systems operated by DOD, a DOD contractor, or another entity on behalf of DOD; and (2) the Office of the Director of National Intelligence (ODNI) is responsible for overseeing non-civilian executive entity information security policies for systems operated by an element of the intelligence community, an intelligence entity's contractor, or another entity on behalf of an intelligence entity.[32] Within DOD, the Director of the Defense Information Systems Agency (DISA) is responsible for developing Security Technical Implementation Guides (STIG) based on DOD policy and security controls.[33] DISA STIGs provide implementation guidance for specific products and versions. DISA STIGs contain all requirements flagged as applicable for a product that has been selected on a DOD control baseline.

[31]*See* FISMA, *codified, in part, at* 44 U.S.C. § 3553, which sets out the authority and functions of the OMB Director and the Secretary of Homeland Security.
[32]*See* FISMA, *codified, in part, at* 44 U.S.C. § 3553(e), which sets out the authority of the Secretary of Defense in relation to Department of Defense information systems and the Director of National Intelligence in relation to the intelligence community's information systems.
[33]DOD Instruction 8500.01, "Cybersecurity" (rev. Oct. 7, 2019).

160 Overview of the FISCAM Framework

.01 The FISCAM methodology incorporates the FISCAM Framework (app. 500B), which is an objectives-based control framework, to assist the auditor in identifying IS control objectives relevant to the areas of audit interest and selecting the IS control activities (or a combination of IS control activities) that are likely to achieve the relevant IS control objectives and are most efficient for testing. The FISCAM Framework presents control categories, critical elements, control objectives, illustrative control activities, and illustrative audit procedures to facilitate the auditor's planning, testing, and reporting procedures.

.02 The control categories presented in the FISCAM Framework are consistent with those included in GAGAS.[34] The critical elements and control objectives presented within the FISCAM Framework are consistent with the principles and attributes included in the Green Book. Additionally, the illustrative control activities presented in the FISCAM Framework are consistent with information security and privacy control requirements included in NIST Computer Security Resource Center publications—and specifically include all information security and privacy control requirements presented in NIST SP 800-53.

.03 Though the FISCAM Framework presents illustrative control activities and illustrative audit procedures, it is not intended to be used as an audit plan. Rather, it is incumbent upon the auditor to develop an audit plan, which includes subordinate test plans, that responds to risk and adequately supports the achievement of the engagement objectives. Moreover, the illustrative control activities identified in the FISCAM Framework may not align with the information security and privacy controls the entity implemented. Based on a variety of factors, including business requirements, specific technologies employed, and potential adverse impacts, the entity selects and tailors control baselines for its information systems. The auditor is ultimately responsible for developing audit procedures to obtain sufficient, appropriate evidence to conclude on whether the entity's IS controls are designed, implemented, and operating effectively to achieve the relevant IS control objectives for each of the areas of audit interest.

[34]GAO-21-368G, para. 8.63.

SECTION 200

PLANNING PHASE

Contents of the Planning Phase

210 Overview of the Planning Phase

.01 When performing the information system (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.

.02 The overall objective of the planning phase is to determine an effective and efficient approach for obtaining sufficient, appropriate evidence for the design, implementation, and operating effectiveness of IS controls to the extent necessary to support the achievement of the engagement objectives and report on the results. The engagement team meets this objective for the IS controls assessment by performing the following planning activities:

- Perform Preliminary Engagement Activities (section 220)
- Understand the Entity's Operations, and Identify and Understand Significant Business Processes (section 230)
- Identify Areas of Audit Interest and Understand Business Process Controls (section 240)
- Understand the Entity's Information Security Management Program (section 250)
- Assess IS Risk on a Preliminary Basis (section 260)
- Identify Relevant General Control Objectives and Determine Likelihood of Effective General Controls (section 270)
- Prepare Planning Phase Documentation (section 280)

.03 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.

.04 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 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. To illustrate, 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.

.05 The scope is the boundary of the IS controls assessment and is directly tied to the engagement objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular program or aspect of a program, the necessary documents or records, the period of time reviewed, and

the locations that will be included.[35] For the IS controls assessment, the subject matter includes significant business processes and areas of audit interest, as well as the relevant user, application, and general control objectives identified for each area of audit interest. Approach is the nature, extent, and timing of audit procedures applied to the significant business processes and areas of audit interest based on the relevant IS control objectives and control activities selected for testing.

.06 During the planning phase, the concepts of significance and audit risk assist auditors in determining the approach. Significance is the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors.[36] Throughout this manual, the term significance is comparable to the term material as used in the context of 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.[37]

.07 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, in light of 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.

.08 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.[38] Professional judgment includes exercising reasonable care and professional skepticism.

[35]GAO, *Government Auditing Standards: 2018 Revision*, GAO-21-368G (Washington, D.C.: July 2018, updated April 2021), p. 219.
[36]GAO-21-368G, p. 219.
[37]GAO-21-368G, p. 212.
[38]GAO-21-368G, pp. 217–218.

220 Perform Preliminary Engagement Activities

.01 The nature and extent of preliminary engagement activities depend on organizational policies and procedures. For the IS controls assessment, preliminary engagement activities include, among other things, 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.

.02 See *GAO/CIGIIE Financial Audit Manual* (FAM) section 215, *Perform Preliminary Engagement Activities*, for further discussion of preliminary engagement activities relevant to federal financial audits.

Competence

.03 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. For the IS controls assessment, a broad range of skills may be needed to perform effective and efficient audit procedures.

.04 The engagement team may include a combination of auditors, such as IS controls auditors, financial auditors, performance auditors, and other auditors, and IT specialists. IT specialists possess special skill or knowledge in the IT field that extend beyond the skills and knowledge 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. Additionally, the work of other auditors, such as independent public accounting firms, inspectors general, state auditors, and internal auditors, may be used to support findings or conclusions for the IS controls assessment.

.05 The audit organization considers the levels of proficiency needed for each role on the engagement when assigning auditors to the engagement. Roles on the engagement generally include nonsupervisory auditors, supervisory auditors, and partners or directors.

- 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.

.06 The auditor should determine whether other auditors have conducted, or are conducting, audits that are relevant to the engagement objectives.

.07 The auditor may determine that the audit organization will use the work of 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 audit organizations contract for IT support services can be instrumental in determining the scope of the contracted audit services, specifying minimum qualifications for 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.

.08 The auditor should perform procedures that provide a sufficient basis for using the work of other auditors when such work is used. Procedures that the auditor may perform in making this determination include reviewing the other auditors' report, audit plan, or audit documentation, or performing tests of the other auditors' work. The auditor should obtain evidence concerning the other auditors' qualifications and independence and determine whether the scope, quality, and timing of the audit work they performed can be relied on within the context of the current engagement objectives.

.09 For federal financial audits, the auditor should comply with requirements for using the work of other auditors discussed in FAM section 600, Using the Work of Others, when the work of other auditors is used.

.10 The competence, qualifications, and independence of IT specialists significantly affect whether their work will be adequate for the engagement team's purposes and will meet generally accepted government auditing standards (GAGAS) requirements.[39] The auditor should determine that IT specialists assisting the engagement team are qualified and competent in their areas of specialization and are independent. Sources that may inform the auditor's assessment of the competence and professional qualifications of an IT specialist include the following:

[39]GAO, *Government Auditing Standards: 2018 Revision*, GAO-21-368G (Washington, D.C.: July 2018, updated April 2021)

- 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.

.11 For federal financial audits, the auditor should comply with requirements for using the work of specialists discussed in FAM section 620, Using the Work of an Auditor's Specialist, when the work of an IT specialist is used.

Communication of Engagement Information

.12 GAGAS 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 for the auditor not to 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 entity management.
- Address logistical requirements. Logistical requirements may include on-site workspace arrangements and procedures for safeguarding sensitive information.

230 Understand the Entity's Operations, and Identify and Understand Significant Business Processes

.01 Once preliminary engagement activities have been performed, the auditor begins planning the IS controls assessment by obtaining general information about the entity and its operations. Obtaining an understanding of the entity's operations facilitates the identification of significant business processes. This understanding also establishes a foundation for the auditor to assess relevant risks.

.02 Business processes are the primary means through which the entity accomplishes its mission. Business processes transform inputs into outputs through a series of transactions or activities to achieve the entity's operations, reporting, and compliance objectives.[40] 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, property management, or security). Significant business processes are those that are significant to the engagement objectives. Throughout this manual, references to significant business processes may include those the entity performs and those that external entities, including service organizations, contractors, and others, perform on behalf of the entity.

.03 For federal financial audits, further information on identifying significant business processes is discussed in FAM section 240, Identify Significant Accounting Applications, Cycles, and Financial Management Systems. In the context of an IS controls assessment performed in connection with a financial audit, significant accounting applications are significant business processes. Accounting applications comprise the methods and records used to (1) identify, assemble, analyze, classify, and record a particular type of transaction or (2) report recorded transactions and maintain accountability for related assets and liabilities, while a cycle is a grouping of related account applications.

Understand the Entity's Operations

.04 The auditor should obtain an understanding of the entity and its operations sufficient to plan the engagement, including external and internal factors affecting operations. External factors may include (1) the entity's sources of funds and budget for information technology, (2) the needs of external users of entity information systems or services, (3) the current political climate, and (4) provisions of applicable laws and regulations establishing IS control requirements relevant to the engagement objectives.

.05 Internal factors may include (1) the size of the entity; (2) the extent of the entity's use of external entities, such as service organizations or contractors, for information technology; (3) the number of locations, including those of any service providers; (4) the organizational and management structure of the entity, including IT functions; (5) the complexity of operations, including IT operations;

[40]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.

(6) the effect of information systems on business processes; (7) the qualifications and competence of key personnel involved in IT operations; and (8) turnover of key personnel involved in IT operations.

.06 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;
- entity 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 or the audit organization's Office of the General Counsel;
- personnel within the entity or the audit organization's special investigations unit; and
- other relevant reports and articles issued by or about the entity, including
  - GAO reports;
  - Office of Inspector General reports;
  - congressional hearings and reports;
  - consultant reports; and
  - material published about the entity in newspapers, magazines, internet sites, and other publications.

Identify and Understand Significant Business Processes

.07 The auditor should identify and obtain an understanding of the significant business processes. The auditor uses professional judgment in determining which business processes are significant to the engagement objectives. In obtaining an understanding of the significant business processes, the auditor considers

- the manner in which 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 the manner in which inputs and outputs are accessed, updated, and deleted;

- the business or organizational units, including any external entities, involved; and
- the points in the business process at which conditions or events related to the areas of audit interest could significantly (or materially) affect the entity's ability to achieve its information processing objectives (completeness, accuracy, validity) or information security objectives (confidentiality, integrity, availability) (e.g., when data are entered, transferred, changed, or deleted).

.08 The auditor should perform walk-throughs of the significant business processes to identify areas of audit interest—information systems, information system components, and information system resources used in the significant businesses processes—and business process controls. Walk-throughs may be performed during the planning and testing phases of an engagement. During the planning phase, walk-throughs are primarily performed to assist the auditor in obtaining an understanding of the significant business processes and identifying areas of audit interest and business process controls. During the testing phase, walk-throughs are often performed as control tests using nonstatistical selection. Walk-throughs, when properly planned and conducted, allow the auditor to perform and document a combination of control tests involving observation, inquiry, and inspection (which may include reperformance).

.09 When performing walk-throughs of the significant business processes, the auditor may

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

.10 If it is not feasible to perform walk-throughs of the significant business processes, the auditor should perform alternative procedures to obtain an understanding of the significant business processes sufficient to identify areas of audit interest and business process controls. For example, it may not be feasible to perform walk-throughs of significant business processes that external entities perform. In such instances, alternative procedures may include

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

240 Identify Areas of Audit Interest and Understand Business Process Controls

.01 When planning the IS controls assessment, the auditor identifies areas of audit interest and obtains an understanding of the design and implementation of business process controls relevant to the significant business processes. The process for identifying areas of audit interest begins with the auditor's understanding of the significant business processes and continues throughout the planning phase as the auditor identifies and obtains an understanding of the business process controls designed to achieve the entity's information-processing objectives.

.02 Obtaining an understanding of the business process controls relevant to the significant business processes enables the auditor to continue defining the scope of the IS controls assessment by identifying areas of audit interest and relevant IS control objectives.

.03 Areas of audit interest are a subset of the entity's information systems, information system components, and information system resources that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. At the business process level, areas of audit interest may include business process applications, 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.

.04 After identifying areas of audit interest and the relevant IS control objectives for each area of audit interest that are necessary to achieve the engagement objectives, the auditor focuses efforts on these areas and objectives, thereby reducing or eliminating work associated with other areas and objectives.

.05 For federal financial audits, further information on identifying areas of audit interest at the business process level and business process controls relevant to the significant business processes is discussed in FAM section 240, Identify Significant Accounting Applications, Cycles, and Financial Management Systems. FAM section 240 requires the auditor to identify the financial management systems that support the significant accounting applications. FAM section 240 also requires the auditor to identify and document the control activities included in the significant accounting applications that depend on information system processing. In the context of an IS controls assessment performed in connection with a financial audit, financial management systems are areas of audit interest at the business process level. Additionally, control activities included in the significant accounting applications that depend on information system processing are business process controls.

Identify Areas of Audit Interest

.06 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 occurs throughout the engagement. The auditor identifies areas of audit interest at the business process level based on the auditor's understanding of the information systems, information system components, and information system resources used in the significant businesses processes.

.07 The auditor identifies areas of audit interest at the system level based on the auditor's understanding of the security and privacy controls that are inherited by those information systems, information system components, and information system resources used in the significant businesses processes. 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.

.08 The auditor's identification of areas of audit interest at the system level is primarily based on the inspection of system security and privacy plans. Through this inspection, the auditor obtains an understanding of an information system's components, security categorization, impact level, operational environment, control dependencies, system interconnections, security and privacy requirements, and the individuals who fulfill system roles and responsibilities. The content of system security and privacy plans is limited to the information system and information system components within the defined authorization boundary. Each plan also contains an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. Business process applications may be separately authorized or included within a larger information system boundary. An information system boundary comprises all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the information system is connected. Understanding the entity's authorization boundaries and connections assists the auditor in identifying areas of audit interest at the system level.

.09 The auditor's identification of areas of audit interest at the system level may also be based on identifying the access paths into and out of the information systems used in the significant business processes. In identifying the access paths, the auditor obtains an understanding of relevant network and information system topologies, including information system boundaries, system interconnections, and network components that provide inherited controls. The auditor also obtains an understanding of the processes and methods the entity employs (or external entities employ on behalf of the entity) to protect the access paths and control the flow of information. In obtaining an understanding of the 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 entities, 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.

.10 The auditor uses professional judgment when evaluating the significance of areas of audit interest to the engagement objectives. The auditor may characterize the significance of information systems or information system components by

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

Understand Business Process Controls Using the FISCAM Framework

.11 The auditor should 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 businesses processes.

.12 The auditor should review available business process application documentation that explains the processing and flow of data within the application, as well as interfaces to other information systems and the design of the underlying data management systems.

.13 The auditor should use the FISCAM Framework for Business Process Controls (app. 500B, table 8), to identify relevant user and application control objectives related to information processing objectives—completeness, accuracy, and validity—for each area of audit interest at the business process level. The auditor also uses the FISCAM Framework for Business Process Controls to identify user and application control activities intended to achieve the relevant IS control objectives. Relevant IS control objectives, as used in FISCAM, are those that are necessary to achieve the engagement objectives. FAM establishes a basis for determining relevant control objectives for financial audits. See section 320 for further discussion on identifying and selecting IS control activities for testing.

.14 The auditor should use the FISCAM Framework for Business Process Controls to identify general control objectives related to the information security objectives—confidentiality, integrity, and availability—for each area of audit interest at the business process level. Relevant general control objectives for areas of audit interest at the business process level have a direct effect on information processing objectives and are necessary to achieve the engagement objectives. The auditor also uses the framework to identify general control activities intended to achieve the relevant IS control objectives. See section 320 for further discussion on identifying and selecting IS control activities for testing.

.15 The FISCAM Framework for Business Process Controls presents critical elements and associated control objectives, illustrative control activities, and illustrative audit procedures for business process controls. Critical elements BP.01 through BP.03 relate to user and application controls, and critical elements

BP.04 through BP.06 relate to general controls designed to achieve information security objectives and support information processing objectives. Table 1 is an excerpt from the framework that presents the critical elements and associated control objectives for BP.01 through BP.06.

.16 For federal financial audits, further information on identifying relevant control objectives and control activities intended to achieve those objectives is discussed in FAM section 330, *Identify Control Objectives*, and FAM section 340, *Identify and Understand Relevant Control Activities*. Additionally, instructions for completing a Specific Control Evaluation (SCE) worksheet for each significant accounting application is included in FAM section 395G, *Specific Control Evaluation Worksheet*. The internal control activities included on an SCE worksheet comprise the manual and information system controls intended to achieve the financial statement assertions, which include the information processing objectives of completeness, accuracy, and validity. In the context of an IS controls assessment performed in connection with a financial audit, significant accounting applications are significant business processes and financial management systems are areas of audit interest. The auditor may use the FISCAM Framework for Business Process Controls (app. 500B, table 8) to identify business process control objectives for the financial management systems involved in the significant accounting applications. The auditor may also use the framework to identify business process control activities intended to achieve the relevant IS control objectives.

Table 1: Critical Elements and Control Objectives for Business Process Controls (User, Application, and General)

Critical elements	Control objectives
BP.01 Management designs and implements user and application control activities 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 validation rules detect erroneous data values before information system processing.
	BP.01.03 Input data validation errors are researched and resolved on a timely basis.
BP.02 Management designs and implements user and application control activities 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 control activities 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 control activities to reasonably assure that business	BP.04.01 Business process application roles and responsibilities are defined and assigned to appropriate personnel.

Critical elements	Control objectives
process applications are properly managed to support the achievement of information processing objectives.	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, as well as the confidentiality, integrity, and availability of information.
	BP.04.04 Business process applications are designed to facilitate the protection of personally identifiable information.
	BP.04.05 The effectiveness of business process 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 control activities to reasonably assure that information system interfaces are properly managed to support the achievement of information processing objectives.	BP.05.01 Interface roles and responsibilities are defined and assigned to appropriate personnel.
	BP.05.02 Policies and procedures for managing interfaces are developed and implemented.
	BP.05.03 Interfaces are designed to exchange information between systems and reasonably assure the confidentiality, integrity, and availability of interfaced data.
	BP.05.04 Interface errors are identified on a timely basis.
	BP.05.05 Interface errors are researched and resolved on a timely basis.
	BP.05.06 Access to interface data and user-defined processing of data are appropriately controlled.
	BP.05.07 Modifications to interfaces are appropriately controlled.
BP.06 Management designs and implements general control activities to reasonably assure that data management systems are properly managed to support the achievement of 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, as well as the confidentiality, integrity, and availability of application data.

Critical elements	Control objectives
	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 data management systems are appropriately controlled.

.17 The following examples illustrate the use of the FISCAM Framework for Business Process Controls in identifying user, application, and general control objectives relevant to areas of audit interest at the business process level.

- If the auditor has identified a data file, which is a collection of records stored in computerized form, as an 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 user and application control objectives that, if achieved, would provide reasonable assurance of the completeness, accuracy, and validity of the data file and
  - the auditor's understanding of the relevant business process applications, interfaces, and data management systems to identify the general control objectives that, if achieved, would reasonably assure the confidentiality, integrity, and availability of the data file.
- If the auditor has identified a business process application as an 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 user and application control objectives supported by the business process application and
  - the auditor's understanding of the business process application to identify the general control objectives that, if achieved, would reasonably assure the effective operation of application controls.

See section 270 for further discussion on identifying general control objectives relevant to areas of audit interest at the system level.

.18 The auditor should determine whether any business process controls performed by external entities on behalf of the entity, including service organizations and contractors, 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 entities perform include the following:

- the nature and significance (or materiality) of the transactions that the external entity processes and

- the degree of interaction between the entity's internal control and the external entity controls.[41]

.19 If significant business process controls are performed by external entities on behalf of the entity, the auditor should obtain a sufficient understanding of such controls to assess risk and design further audit procedures in response to risk. The auditor may obtain a preliminary understanding of controls external entities perform through the audit procedures performed in connection with general control objective SM.03.02, External entities are held accountable for their assigned internal control responsibilities related to the entity's information security and privacy objectives (see section 250, table 2).

[41]The degree of interaction refers to the extent to which an entity is able to and elects to implement effective controls over transactions that the external entity processes.

250 Understand the Entity's Information Security Management Program

.01 When performing the IS controls assessment, the auditor obtains an understanding of the entity's information security management program to assist in adequately planning the IS controls work necessary to support the achievement of the engagement objectives. 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 responsibilities, identifying and responding to risks, developing and implementing effective information security policies, monitoring the adequacy of the entity's information system controls, and holding individuals and external entities accountable for their internal control responsibilities.

.02 Obtaining an understanding of the entity's information security management program enables the auditor to 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. These components of internal control are defined as follows:

- Control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Risk assessment is the entity's identification, analysis, and management of risks relevant to achieving its objectives. Risk assessment provides the basis for developing appropriate responses to risk.
- Information and communication systems support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Monitoring of controls is a process to assess the effectiveness of internal control performance over time. This consists of activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.[42]

.03 For federal financial audits, further information on assessing the design, implementation, and operating effectiveness of the entity's control environment, risk assessment, information and communication, and monitoring components of internal control is discussed in FAM section 260, Identify Risk Factors, and FAM section 360, Perform Tests of Controls and Compliance with FFMIA. FAM requires financial auditors to test the operating effectiveness of those control activities that the auditor has determined are designed and implemented effectively. Additionally, FAM requires financial auditors to test the operating effectiveness of controls related to the remaining components of internal control—control environment, risk assessment, information and communication,

[42] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014), para. OV2.09.

and monitoring—to support the auditor's overall assessment of internal control over financial reporting.

Understand the Entity's Information Security Management Program Using the FISCAM Framework

.04 The auditor should obtain an understanding of the entity's information security management program sufficient to (1) plan the IS controls work necessary to support the achievement of the engagement objectives and (2) 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. The auditor should use the FISCAM Framework for Security Management (app. 500B, table 9) to develop an understanding of the entity's information security management program.

.05 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 entity-level controls that are important to the auditor's conclusion about whether the entity has effective internal control over financial reporting.

.06 The FISCAM Framework for Security Management presents critical elements and associated control objectives, illustrative control activities, and audit procedures for security management general controls. Table 2 is an excerpt from the framework and presents the critical elements and associated control objectives relevant to an entity's information security management program.

Table 2: Critical Elements and Control Objectives for Security Management

Critical element	Control objective
SM.01 Management establishes organizational structures, assigns 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.

Critical element	Control objective
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.
	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 entities 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 entities 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 entities 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.

.07 To effectively use the FISCAM Framework for Security Management (app. 500B, table 9) to obtain an understanding of the entity's information security management program sufficient to (1) plan the IS controls work necessary to support the achievement of the engagement objectives and (2) 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, the auditor considers the critical elements and control objectives in the context of the areas of audit interest. For example, the auditor may consider the extent to which control activities that the entity designed and implemented to achieve specific security management 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 control activities 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 control activities for the areas of audit interest. The illustrative control activities within the framework are aligned with the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. They are intended to assist the auditor in identifying and assessing the IS control activities that the entity designed, implemented, and operated to achieve its information processing objectives and are necessary to support the achievement of the engagement objectives.

.08 The auditor may use different methods (inquiry, observation, and inspection) to obtain an understanding of the entity's information security management program sufficient to (1) plan the IS controls work necessary to support the achievement of the engagement objectives and (2) 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. In obtaining an understanding of the entity's information security management program, the auditor considers whether entity 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.

260 Assess IS Risk on a Preliminary Basis

.01 When performing the IS controls assessment, the auditor identifies risk factors and assesses risk to determine the nature, extent, and timing of control tests. While the auditor identifies risk factors and assesses risk throughout the engagement, risk assessment activities are concentrated in the planning phase. During the planning phase, the auditor assesses inherent risk and control risk, including fraud risk, to form a preliminary assessment of IS risk.

- Inherent risk is the likelihood that conditions or events, related to the areas of audit interest, could significantly (or materially) affect the entity's ability to achieve its information processing objectives (completeness, accuracy, validity) or information security objectives (confidentiality, integrity, availability), without consideration of related IS controls.
- Control risk is the likelihood that conditions or events, related to the areas of audit interest, that could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives, will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls. Control risk is a function of the design, implementation, and operating effectiveness of the entity's IS controls relevant to the engagement objectives. Some control risk will always exist because of the inherent limitations of internal control.
- IS risk is the auditor's combined assessment of inherent risk and control risk related to the areas of audit interest.

.02 The auditor's preliminary assessment of IS risk 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. Audit risk is a function of IS risk and detection risk. Detection risk is the risk that the nature, extent, and timing of audit procedures will not detect conditions or events related to the areas of audit interest that could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives. Detection risk is a function of the effectiveness of the audit procedures and their application by the auditor.

.03 For federal financial audits, further information on the assessment of inherent and control risk—including risk factors related to information systems—is discussed in FAM section 260, *Identify Risk Factors*. In the context of a financial audit, the auditor's assessment of IS risk is incorporated into the auditor's assessment of the risk of material misstatement.

Identify Inherent and Control Risk Factors

.04 The auditor should identify inherent and control risk factors relevant to the significant business processes and areas of audit interest. The auditor identifies inherent and control risk factors within the context of the information security objectives and the relationship of such objectives to achieving information-processing objectives that are significant to the engagement. The auditor identifies inherent and control risk factors based on information obtained during the planning phase to develop an understanding of the entity's operations, significant business processes, and business process controls, including any operations, processes, or controls external entities perform on behalf of the

entity. The auditor uses professional judgment in determining (1) the extent of audit procedures necessary to identify inherent and control risk factors and (2) the effect of such risk factors on the auditor's preliminary assessment of IS risk.

Inherent Risk Factors

.05 The auditor identifies inherent risk factors based on the auditor's understanding of the areas of audit interest, including the information technology the entity employs in connection with the areas of audit interest. The information technology the entity employs can introduce inherent risk factors, such as the following:

- Certain types of hardware and software in use may be more susceptible to threats than others are. 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 IS 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 entities 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 encounter existing flaws.
- The manner in which the entity's networks are structured as well as 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.

.06 The effect of inherent risk factors may be pervasive in nature depending on the extent to which the same information technology is used in connection with multiple areas of audit interest.

.07 Additionally, the auditor may consider the following risk factors relevant to the significant business processes when assessing inherent risk:

- Uniform processing of transactions: Because information systems process groups of identical transactions consistently, any errors or misstatements arising from erroneous computer programming will occur consistently in similar transactions. However, the possibility of random processing errors is reduced substantially with information system processing.
- Automated processing: Information systems may automatically initiate transactions or perform automated processing steps. Evidence of these processing steps (and any related controls) may or may not be visible to users of the information systems.
- Increased potential for undetected errors: Information systems use and store information in electronic form. This increases the potential for individuals to gain unauthorized access to sensitive information and to alter data without visible evidence. In the electronic form, changes to software programs and data may not be readily detectable. In addition, users may be less likely to challenge the reliability of system-generated reports than that of manually prepared reports.
- Nonroutine transactions: As with manual systems, nonroutine transactions increase inherent risk. Software programs developed to process such transactions may not be subject to the same procedures as those developed to process routine transactions.

Control Risk Factors

.08 The auditor identifies control risk factors based on the auditor's understanding of the entity's information security management program and inherent risk factors, as well as through inquiries of appropriate personnel and the inspection of relevant reports on the entity's control activities, including IS controls. An understanding of the entity's information security management program enables the auditor to identify control 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. The auditor may consider the following control risk factors, which are organized by the security management critical elements from table 10 (in app. 500B):

- SM.01 Management establishes organizational structures, assigns responsibilities, and develops plans and processes to implement an information security management program for achieving the entity's information security and privacy objectives. Control risk factors include
  - 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 (e.g., 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 performed by external entities;
  - 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 an adequate incident response program has been established;
  - the quality of the entity's system security and privacy plans; and
  - the extent to which information security and privacy responsibilities 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. Control risk factors include
  - turnover of key personnel involved in IT operations (e.g., 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 (e.g., 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 entities accountable for their internal control responsibilities related to the entity's information security management program. Control risk factors include
  - 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 and understood by entity personnel responsible for enforcement;
  - the extent to which external entities 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 designed, implemented, and operated by external entities.

- SM.04 Management identifies, analyzes, and responds to risks, including fraud risk, and significant changes related to the entity's information security management program. Control risk factors include
  - 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;
  - 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 in response to changing conditions on a timely basis; and
  - the extent to which entity 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. Control risk factors include
  - the quality of the entity's policies and procedures for managing and using business process applications, 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 entities, such as third party assessors; and
  - the quality of the entity's authorization packages.
- SM.06 Management establishes and performs monitoring activities to evaluate the effectiveness of the entity's information security management program. Control risk factors include

  - the quality of the entity's system-level continuous monitoring strategies;
  - the quality of the entity's security and privacy control assessments;
  - 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 control activities 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. Control risk factors include
  - the extent to which the entity timely and appropriately responds to findings, recommendations, or concerns related to the entity's 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

.09 The auditor should discuss fraud risk factors among the engagement team 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.

.10 Fraud risk factors affect the auditor's assessment of inherent risk and control risk and, therefore, affect the auditor's assessment of IS 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 risk.

.11 The following control risks 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 inappropriate 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.

.12 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.

.13 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.

.14 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 be indicative of fraud. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond auditors' professional expertise and responsibility.

Results of Previous Engagements

.15 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 entity 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 entity 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 should use this information in assessing risk and determining the nature, extent, and timing of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current engagement objectives.

.16 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 (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)[43] and Federal Managers' Financial Integrity Act (FMFIA);[44]

[43]Federal Financial Management Improvement Act of 1996, *reprinted in* 31 U.S.C. § 3512 note. FFMIA only applies to the 15 executive departments and additional 9 large executive agencies listed under 31 U.S.C. § 901(b).
[44]31 U.S.C. § 3512 (c), (d), commonly known as the Federal Managers' Financial Integrity Act (FMFIA).

- other reports by entity management, the auditor, or others that contain information concerning IS controls that are relevant to the audit objectives;
- service organization reports, if available, for any operations, processes, or controls that service organizations perform on behalf of the entity;
- GAO reports;
- IG and internal audit reports (including those for performance audits and other reviews); and
- consultant reports.

Assess IS Risk on a Preliminary Basis

.17 The auditor should assess the level of IS risk for each of the areas of audit interest on a preliminary basis based on the auditor's identification of inherent and control risk factors, including fraud risk factors. Inherent and control risk factors can increase or decrease the auditor's assessed level of IS risk for the areas of audit interest. For each area of audit interest, the auditor assesses preliminary IS risk at one of three levels:

- Low. The auditor believes that IS controls will adequately mitigate inherent risks and support the achievement of information processing and information security objectives that are significant to the engagement objectives.
- Moderate. The auditor believes that IS controls will more likely than not adequately mitigate inherent risks and support the achievement of information processing and information security objectives that are significant to the engagement objectives.
- High. The auditor believes that IS controls will more unlikely than likely adequately mitigate inherent risks and support the achievement of information processing and information security objectives that are significant to the engagement objectives.

.18 The auditor should determine (1) the likelihood that conditions or events related to the areas of audit interest could affect the entity's ability to achieve its information processing or information security objectives and (2) the impact that such conditions or events (e.g., significance or materiality) would have on the entity's achievement of information processing and information security objectives that are significant to the engagement objectives.

.19 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.

.20 The auditor should involve senior members of the engagement team in the assessment of IS 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 risk. However, the auditor is not required or expected to re-perform management's risk assessments when using

the results of such to inform the auditor's assessment of IS risk. The auditor may also consult with an IT specialist when assessing IS risk.

.21 The auditor's assessed level of IS risk for the areas 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 Standards (FIPS) 199, is an important first step in the entity's information security and privacy risk management process.[45] Though considered in the context of the same information security objectives of confidentiality, integrity, and availability, the auditor's assessment of IS risk for the areas of audit interest need not match management's security categorizations for the corresponding information systems.

.22 The auditor should involve senior members of the engagement team in determining the nature, extent, and timing of IS control tests in response to assessed risks. As IS 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. Such actions decrease detection risk and therefore decrease audit risk. Consequently, the auditor's assessment of IS risk affects the nature, timing, and extent of IS controls testing. As IS risk increases, the auditor may expand the nature, extent, and timing of audit procedures in order to conclude on the effectiveness of such controls.

[45]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199 (Gaithersburg, Md.: March 2004).

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

.01 When planning the IS controls assessment, the auditor identifies relevant general control objectives for each area of audit interest at the business process and system levels. The auditor's understanding of the significant business processes, business process controls, and the entity's information security management program provide a general understanding of the design of the entity's general control activities relevant to the areas of audit interest. Specifically, the auditor will have a basic understanding of the general controls applied at the business process, system, and entity levels that support the achievement of the entity's information processing objectives and are necessary to support the achievement of the engagement objectives. This understanding facilitates the auditor's identification of general control objectives relevant to the areas of audit interest at the system level and establishes a foundation for the auditor to determine the likelihood that general control activities will effectively achieve the relevant general control objectives.

.02 The likelihood of effective general control activities informs the nature, extent, and timing of (1) general control tests and (2) user and application control tests.

.03 For federal financial audits, further information on determining the likelihood of effective general control activities is discussed in FAM section 270, Determine Likelihood of Effective IS Controls. The likelihood of effective general control activities also informs the nature, extent, and timing of non-IS control tests (i.e., tests of manual controls or user controls that do not depend on information system processing) performed in connection with financial audits.

Identify Relevant General Control Objectives and Determine Likelihood of Effective General Controls Using the FISCAM Framework

.04 The auditor should identify relevant general control objectives for each area of audit interest at the system level. Relevant general control objectives for areas of audit interest at the system level have an indirect effect on information processing objectives and are necessary to support the achievement of the engagement objectives. The achievement of relevant general control objectives for areas of audit interest at the system level creates a suitable environment to support the effective operation of business process controls. See section 240 for further discussion on identifying relevant general control objectives for areas of audit interest at the business process level.

.05 When identifying relevant general control objectives for areas of audit interest at the system level, 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. The auditor may determine that it is not necessary to identify general control objectives from all five general control categories according to the auditor's professional judgment.

.06 The auditor should determine the likelihood that general control activities will effectively achieve the relevant general control objectives. In determining the likelihood that specific general control activities will be effective, the auditor considers the design of the entity's control environment, risk assessment,

information and communication, and monitoring components of internal control relevant to the IS controls assessment according to the auditor's understanding of the entity's information security management program. See section 250 for further discussion on obtaining an understanding of the entity's information security management program.

Security Management

.07 The auditor should use the FISCAM Framework for Security Management (app. 500B, table 9), to (1) identify security management control objectives relevant to each area of audit interest at the system level and (2) determine the likelihood that security management control activities will effectively achieve the relevant IS control objectives. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that security management control activities will be effective.

.08 Table 2 in section 250 is an excerpt from table 9 (app. 500B) that presents critical elements and control objectives for security management. Regardless of whether the auditor identifies security management general control objectives as being relevant to areas of audit interest at the system level, the auditor is required to obtain an understanding of the entity's information security management program. See section 250 for further discussion on obtaining an understanding of the entity's information security management program sufficient to (1) plan the IS controls work necessary to support the achievement of the engagement objectives and (2) 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.

Logical and Physical Access (Access Controls)

.09 The auditor should use the FISCAM Framework for Access Controls (app. 500B, table 10) to (1) identify access control objectives relevant to each area of audit interest at the system level and (2) determine the likelihood that access control activities will effectively achieve the relevant IS control objectives. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that access control activities will be effective.

.10 Table 3 is an excerpt from the FISCAM Framework for Access Controls and presents the critical elements and associated control objectives for logical and physical access.

Table 3: Critical Elements and Control Objectives for Access Controls

Critical elements	Control objectives
AC.01 Management designs and implements control activities to appropriately protect logical boundaries of information systems in response to risks.	AC.01.01 Connectivity to information system resources is appropriately controlled.
	AC.01.02 Network sessions are appropriately controlled.
AC.02 Management designs and implements control activities to	AC.02.01 Identification and authentication requirements are established.

Critical elements	Control objectives
appropriately restrict logical access to information systems and information system resources to authorized individuals for authorized purposes.	AC.02.02 Information system users, processes, and services are appropriately identified and authenticated before accessing information systems and information system resources.
	AC.02.03. Information system users, processes, and services are appropriately authorized before accessing information systems and information system resources.
	AC.02.04 Access privileges restrict access to information system resources to authorized individuals for authorized purposes.
AC.03 Management designs and implements control activities 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 control activities to appropriately restrict physical access to facilities, information systems, and information system 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 control activities 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.

Segregation of Duties

.11 The auditor should use the FISCAM Framework for Segregation of Duties (app. 500B, table 11) to (1) identify segregation of duties control objectives relevant to each area of audit interest at the system level and (2) determine the likelihood that segregation of duties control activities will effectively achieve the relevant IS control objectives. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that segregation of duties control activities will be effective.

.12 Table 4 is an excerpt from the FISCAM Framework for Segregation of Duties and presents the critical elements and associated control objectives for segregation of duties.

Table 4: Critical Elements and Control Objectives for Segregation of Duties

Critical element	Control objectives
	SD.01.01 Incompatible duties are identified based on risk.

Critical element	Control objectives
SD.01 Management designs and implements control activities to appropriately segregate incompatible duties and mitigate risks resulting from incompatible duties that cannot be segregated.	SD.01.02 Incompatible duties are appropriately segregated when possible.
	SD.01.03 Alternative control activities are implemented to mitigate risks resulting from incompatible duties that cannot be segregated.

Configuration Management

.13 The auditor should use the FISCAM Framework for Configuration Management (app. 500B, table 12) to (1) identify configuration management control objectives relevant to each area of audit interest at the system level and (2) determine the likelihood that configuration management control activities will effectively achieve the relevant IS control objectives. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that configuration management control activities will be effective.

.14 Table 5 is an excerpt from the FISCAM Framework for Configuration Management and presents the critical elements and associated control objectives for configuration management.

Table 5: Critical Elements and Control Objectives for Configuration Management

Critical elements	Control objectives
CM.01 Management designs and implements control activities 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 Baseline configuration settings are developed and documented for configuration items.
CM.02 Management designs and implements control activities 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 baseline configuration settings and unauthorized changes.
	CM.02.04 Logical access controls relevant to configuration management are selected and employed based on risk.

Critical elements	Control objectives
CM.03 Management designs and implements control activities 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.

Contingency Planning

.15 The auditor should use the FISCAM Framework for Contingency Planning (app. 500B, table 13) to (1) identify contingency planning control objectives relevant to each area of audit interest at the system level and (2) determine the likelihood that contingency planning control activities will effectively achieve the relevant IS control objectives. The auditor uses professional judgment in determining the nature and extent of audit procedures necessary to determine the likelihood that contingency planning control activities will be effective.

.16 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: Critical Elements and Control Objectives for Contingency Planning

Critical elements	Control objectives
CP.01 Management designs and implements control activities 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 control activities to prevent	CP.02.01 Environmental controls are appropriately selected and employed based on risk.

Critical elements	Control objectives
or minimize system disruption and potential damage to facilities, information systems, and information system resources due to natural disasters, structural failures, hostile attacks, or errors.	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.

280 Prepare Planning Phase Documentation

.01 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 Preliminary Assessment of IS Risk

.02 The auditor should prepare a written risk assessment that identifies inherent and control risk factors, including fraud risk factors, that significantly increase or decrease the auditor's assessed level of IS risk for each of the areas of audit interest. As part of the auditor's preliminary assessment of IS risk, the auditor documents (1) the likelihood that conditions or events related to the areas of audit interest that could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives could occur and (2) the impact that such conditions or events would have on the entity's achievement of information processing and information security objectives that are significant to the engagement. The auditor also documents other factors or compensating controls that mitigate the effects of identified inherent and control risk factors.

Audit Plan, Planning Memo, and Subordinate Test Plans

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

.04 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;
- the identification of 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 and the auditor's preliminary assessment of IS risk.

.05 The auditor should prepare subordinate test plans to document the approach for testing controls for the relevant IS control objectives for each area of audit interest. See section 350 for further discussion on documentation requirements for written test plans for each area of audit interest.

SECTION 300

TESTING PHASE

Contents of the Testing Phase

310 Overview of the Testing Phase

.01 The overall objective of the testing phase is to obtain sufficient, appropriate evidence for the design, implementation, and operating effectiveness of information system (IS) controls to the extent necessary to support the achievement of the engagement objectives. The engagement team meets this objective for the IS controls assessment by performing the following testing activities:

- Select IS Control Activities for Testing (section 320)
- Determine the Nature, Extent, and Timing of IS Control Tests (section 330)
- Perform IS Controls Tests and Evaluate the Results, Including the Significance of IS Control Deficiencies (section 340)
- Prepare Testing Phase Documentation (section 350)

.02 In the testing phase, the auditor builds on the foundation established in the planning phase to test the design, implementation, and operating effectiveness of IS controls. Throughout the engagement, the concepts of significance and audit risk assist auditors in selecting IS control activities for testing; determining the nature, extent, and timing of IS control tests; and evaluating the results, including the significance of any IS control deficiencies identified. The auditor selects IS control activities for testing that are likely to achieve the relevant IS control objectives and are most efficient for testing. The auditor uses professional judgment in determining that sufficient, appropriate evidence has been obtained to achieve the engagement objectives and report on the results.

320 Select IS Control Activities for Testing

.01 When performing the IS controls assessment, the auditor selects IS control activities for testing. Specifically, the auditor selects the user, application, and general control activities that are likely to achieve the relevant business process and general control objectives and are most efficient for testing.

Select User, Application, and General Control Activities

.02 The auditor should obtain sufficient, appropriate evidence to conclude on whether the relevant business process and general control objectives are achieved by the entity's user, application, and general control activities. The auditor should develop test plans to assist in obtaining sufficient, appropriate evidence to conclude on whether the entity's IS controls are designed, implemented, and operating effectively to achieve the relevant IS control objectives for each area of audit interest. See section 350 for further discussion on documentation requirements for written test plans for each area of audit interest.

.03 The auditor should consider the extent to which control dependencies exist among user, application, and general control activities designed to achieve the relevant business process and general control objectives. When selecting user, application, and general control activities for testing, the auditor considers the extent to which control dependencies exist between such controls and could affect the achievement of the related IS control objectives. A control dependency exists when the effectiveness of a control activity depends on the effectiveness of other control activities. Determining if a control activity is effective would include assessing the effectiveness of other control activities upon which the effectiveness of the control activity is dependent. For example, the effectiveness of a configurable control within application software will depend on the design of the application control, as well as related access and configuration management general controls designed to prevent or detect unauthorized changes to the control. Identifying control dependencies (1) informs the auditor's decisions regarding the nature, extent, and timing of IS control tests and (2) establishes a foundation for evaluating the significance of any IS control deficiencies identified.

.04 The auditor should select the IS control activities that are likely to achieve the relevant IS control objectives and are most efficient for testing. If there are several IS control activities that are likely to be effective in achieving an IS control objective, the auditor selects the control activity that is most efficient to test, considering such factors as (1) the extent to which a control activity achieves several control objectives and thereby reduces the number of controls that would ordinarily need to be tested, (2) the time that would be required to test the control activity, and (3) control dependencies.

.05 The auditor should use the FISCAM Framework (app. 500B) to identify user, application, and general control activities by control objective. The FISCAM Framework presents illustrative control activities for each control objective included in the framework. The illustrative control activities are aligned with the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. They are intended to assist the auditor in identifying, selecting, and testing IS control activities that the entity designed, implemented, and operated to achieve the IS control objectives. Although the FISCAM

Framework presents multiple illustrative IS control activities for each IS control objective included in the framework, the auditor need not test all of the control activities identified. However, the auditor is required to obtain sufficient, appropriate evidence to conclude on whether the relevant IS control objectives are achieved.

.06 Certain user, application, and general control activities may support the achievement of multiple IS control objectives for more than one area of audit interest. In such cases, the auditor may include references to separate test plans for such control activities. Including such references minimizes redundancy in the audit documentation. Control tests for such control activities need only be performed once and linked to the test plans developed for each applicable area of audit interest.

.07 When selecting general control activities for testing, the auditor considers the level (i.e., business process, system, and entity) at which such IS controls are applied and whether it is more efficient to test certain general control activities at the system or entity levels rather than the business process level, assuming they are equally effective. For example, if an entity-level general control activity for user identification and authentication is likely to achieve a control objective for the appropriate restriction of logical access for multiple areas of audit interest, it may be more efficient to test the entity-level control activity. The auditor may implement a tiered approach to evaluating the effectiveness of IS control activities, beginning with entity-level and system-level general control activities, followed by business process-level general control activities, and finishing with user and application control activities. Such an approach may be efficient if (1) the auditor determined in the planning phase that general control activities are not likely to be effective in achieving the general control objectives relevant to areas of audit interest at the business process and system levels and (2) the auditor plans to forgo testing of certain user and application controls if such general control objectives are not achieved. However, in order for such an approach to be both efficient and effective, the auditor needs to have an adequate understanding of IS control dependences.

.08 Without effective general controls, user and application controls may be rendered ineffective. Consequently, if general control activities are not likely to be designed or operating effectively, the auditor may conclude that such general control weaknesses preclude the effective operation of user and application controls and that assessing user and application controls is not necessary to support the achievement of the engagement objectives. In such cases, the auditor develops appropriate findings and considers the effect of risks arising from ineffective general controls on the nature, extent, and timing of further audit procedures.

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

.01 When performing the IS controls assessment, the auditor establishes an efficient and effective approach for performing IS control tests to conclude on whether the entity's IS controls are designed, implemented, and operating effectively to achieve the relevant IS control objectives for each of the areas of audit interest. Once the auditor has selected the IS control activities that are likely to achieve the relevant IS control objectives and are most efficient for testing, the auditor determines the nature, extent and timing of IS control tests. Control tests are a means of obtaining evidence on the design, implementation, and operating effectiveness of internal controls. The nature, extent, and timing of control tests will vary by control activity. When determining the nature, extent, and timing of IS control tests, the auditor considers the following:

- The nature of the IS control activity influences the type of evidence available to the auditor to demonstrate whether the control activity is designed, implemented, and operating effectively.
- The type of evidence available influences the nature of IS control tests that the auditor may perform, as well as the timing of such tests.
- The frequency at which the entity performs the IS control activity, along with the nature of the IS control test the auditor plans to perform, influences the extent and timing of IS control tests.
- The significance of the IS control activity to achieving the related IS control objective(s) influences the nature, extent, and timing of the IS control tests. However, it is particularly important to the auditor's determination of extent, as extent refers to the quantity of control tests to be performed.

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

.02 The auditor should determine the nature, extent, and timing of IS control tests of selected IS control activities and conclude on whether the relevant IS control objectives are achieved by the selected IS controls. Determinations regarding the nature, extent, and timing of IS control tests are interrelated, as the auditor's determination of one will affect the auditor's determination of the others. The nature, extent, and timing of IS control tests affect both the sufficiency and appropriateness of the evidence obtained through control testing.

.03 The auditor should determine whether each selected IS control activity is (1) suitably designed to support achieving the related IS control objective(s), (2) properly implemented (placed in operation), and (3) operating effectively. For those IS control activities that the auditor determines are suitably designed and properly implemented, the auditor considers the extent to which additional IS control tests are needed to determine the operating effectiveness of such controls. Walk-throughs, when properly planned and conducted, allow the auditor to perform and document a combination of control tests involving observation, inquiry, and inspection (including reperformance). As such, walk-throughs are an appropriate means for determining whether IS control activities are suitably designed and properly implemented.

.04 Generally, if selected IS control activities are suitably designed and properly implemented, the auditor will perform additional IS control tests to determine

whether the IS control activities are operating effectively. Testing the operating effectiveness of a control activity is different from understanding and evaluating the design and implementation of the control activity. However, the same methods (inquiry; observation; and inspection, including reperformance) are used. Tests of operating effectiveness are particularly important for control activities that are performed on a frequent or recurring basis because such tests allow the auditor to draw conclusions regarding how consistently the entity performs the control activity throughout the audit period.

.05 In determining whether selected IS control activities are designed, implemented, and operating effectively, the auditor considers whether sufficient, appropriate audit evidence has been obtained to support an assessment of control risk as low. To support a low assessed level of control risk, the auditor should perform IS control tests sufficient to conclude on the operating effectiveness of the selected user, application, and general controls that have been suitably designed and properly implemented.

.06 For federal financial audits, the auditor identifies IS control objectives that, if achieved, support a low assessed level of control risk for the auditor's overall assessment of internal control over financial reporting. Additionally, the auditor is required to perform sufficient tests of IS controls that have been suitably designed and implemented to achieve the relevant IS control objectives and support a low assessed level of control risk for the auditor's overall assessment of internal control over financial reporting.

Nature of IS Control Tests

.07 The auditor should determine the nature of IS control tests (observation, inquiry, or inspection (including reperformance) to be performed for each selected IS control activity. This determination is based on the nature of the IS control activity; the evidence available to demonstrate whether the activity is designed, implemented, and operating effectively; and the significance of the activity to achieving the related IS control objective(s).

.08 The auditor determines the nature of IS control tests based on the appropriateness of the audit evidence available to demonstrate whether the selected IS control activity is designed, implemented, and operating effectively. Appropriateness is the measure of the quality of evidence used for addressing the engagement objectives and supporting findings and conclusions, including its relevance, validity, and reliability. No one specific control test is always necessary, applicable, or equally effective in every circumstance. However, evidence obtained from inquiry alone will not provide sufficient, appropriate evidence of control effectiveness.

.09 When using information officials of the audited entity provided as evidence, the auditor should (1) determine what the officials or other auditors did to obtain assurance over the reliability of the information and (2) test management's procedures to obtain assurance, perform direct testing of the information, or obtain additional corroborating evidence. The nature, timing, and extent of the auditors' procedures will depend on the nature of the information being used and the significance of the information to the auditor's control tests. Using a risk-based approach, the auditor may determine that they need to perform additional procedures if they become aware of evidence that conflicts with that provided by management. In their overall assessment, the auditor documents how they resolved situations involving conflicting evidence.

.10 The auditor should perform other audit procedures in combination with inquiry to obtain sufficient, appropriate audit evidence regarding the design, implementation, and operating effectiveness of IS control activities. Such other audit procedures allow the auditor to draw conclusions on how the IS control activity was applied at relevant times during the period under audit; the consistency with which the IS control activity was applied; and by whom or by what means the IS control activity was applied, including, when applicable, whether the person performing the control possesses the necessary authority and competence to perform the control effectively.

.11 The following provides additional detail on the nature of IS control tests:

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

controls are implemented and operating effectively. To use such documentation as part of the evidence of effective IS control activities, the auditor obtains additional evidence to demonstrate that the IS control activities have been implemented. Inspection is generally a reliable source of audit evidence, and this type of test can be performed at any time since it involves the examination of documents and records.

The auditor may also reperform the procedures or controls evidenced by the documents and records being inspected to determine if they were properly applied. Reperformance is the auditor's independent execution of procedures or IS control activities that were originally performed as part of the entity's internal control. Reperformance tests can be performed manually or with computer-assisted audit techniques. These tests can be applied to user and application controls to determine whether such controls are designed, implemented, and operating effectively. The tests can also be applied to automated business processes performed by business process applications to verify the completeness, accuracy, and validity of the results produced by these applications.

.12 To test the design, implementation, and operating effectiveness of IS controls, auditors use professional judgment in determining and performing an appropriate mix of IS control tests to obtain sufficient, appropriate evidence to support their conclusions.

Extent of IS Control Tests

.13 The auditor should determine the extent of IS control tests to be performed for each IS control activity. The extent of IS control tests refers to the quantity of control tests to be performed for a specific IS control activity. This determination is influenced by the nature of the IS control test, the frequency at which the entity performs the IS control activity, and the significance of the IS control activity to achieving the related IS control objective(s). Additionally, this determination will influence whether the auditor will use statistical sampling or nonstatistical selection methods to determine whether the IS control activity is operating effectively.

.14 For IS control activities that do not leave documentary evidence of existence or performance, the auditor may test their effectiveness through inquiry and observation. However, the appropriate extent of inquiry and observation is a matter of professional judgment. For automated business processes performed by business process applications and application controls, the auditor may observe one or a few instances in which the process or control activity is performed. The auditor may also verify the completeness, accuracy, and validity of the results these applications produce. However, the auditor's determination regarding the design, implementation, and operating effectiveness of automated business processes that business process applications and application controls perform will partially depend on the auditor's conclusions on the related logical access and configuration management general control objectives.

.15 The frequency at which the entity performs an IS control activity will inform the auditor's determination regarding the sufficiency of audit evidence obtained from a given IS control test. Control activities that are performed more frequently will require a greater extent of control tests than control activities that are performed infrequently. For controls that do not operate frequently, such as those that operate only once or twice a year (e.g., periodic access recertification), the

auditor may determine that it is necessary to test all of the items in the population (i.e., all instances in which the control activity was performed during the audit period).

.16 The significance of the IS control activity to achieving the related IS control objective(s) influences the nature, extent, and timing of the IS control tests. However, it is particularly important to the auditor's determination of extent, as extent refers to the quantity of IS control tests to be performed. The auditor considers the sufficiency of audit evidence obtained from the control test when determining the extent of control tests necessary to conclude on the operating effectiveness of the control activity. Sufficiency is a measure of the quantity of evidence used to support the findings and conclusions related to the engagement objectives. The persuasiveness of the audit evidence needed to support the effectiveness of an IS control activity is a function of the degree to which the auditor relies on the effectiveness of the IS control activity in concluding on the achievement of the related IS control objective(s). As the auditor's reliance increases, so too does the necessary persuasiveness of the evidence obtained through control testing. Additionally, although some risk assessment procedures may not have been specifically designed as tests of controls, they may nevertheless provide audit evidence about the operating effectiveness of certain IS control activities and, consequently, serve as tests of IS controls.

.17 When planning additional IS control tests to obtain sufficient, appropriate evidence regarding the operating effectiveness of IS control activities, the auditor may test all instances (the population of items) or some instances in which the IS control activity was performed during the period of audit. If the auditor does not plan to test all of the items within the population, the auditor should use statistical sampling (items intended to be representative of and statistically projected to the population of items) or nonstatistical selection (items not intended to be representative of or statistically projectable to the population of items) to identify items for control testing.

Statistical Sampling for Control Tests

.18 The auditor should use attribute sampling, and select items either through simple random selection (SRS) or through systematic random selection (SYS), when using statistical sampling to identify items within a population for control testing. Attribute sampling achieves the objective of selecting items for the sample in such a way that the auditor may reasonably expect the sample to be representative of the relevant population and likely to provide the auditor with a reasonable basis for conclusions about the population.

.19 When planning IS control tests involving statistical sampling, the auditor should determine a sample size sufficient to reduce sampling risk to an acceptably low level. Sampling risk is the risk that the auditor's conclusions based on a sample may be different from the conclusion if the entire population were subjected to the same audit procedure. For tests of controls, sampling risk is the risk of assessing control risk either too low or too high. For sampling control tests, the auditor should determine

- the objectives of the control test (including what constitutes a deviation),
- the population (including sampling unit and time frame),
- the method of selecting the statistical sample (SRS or SYS), and

- the sample design and resulting sample size.[46]

.20 The auditor should define the objectives of each IS control test, including what constitutes a deviation, when using statistical sampling for IS control testing. Generally, the primary objective of a control test involving statistical sampling is to determine whether or not a specific control activity is operating effectively. When control tests involving statistical sampling are used, the auditor evaluates operating effectiveness in terms of the rate of deviations in units or dollars from prescribed controls. To perform such an evaluation, the auditor first defines (1) the specific control activities to be tested and (2) what constitutes an error, exception, or control failure for each control activity. Control deviations are defined in terms of control activities not followed.

.21 The auditor should define the population by identifying the whole set of items on which the auditor needs to reach a conclusion and from which the statistical sample will be drawn. This includes

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

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

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

.23 The auditor may use statistical sampling to test the operating effectiveness of certain general control activities, such as those involving approvals. For example, the auditor may use statistical sampling to test management approvals related to

[46]See paragraph 330.25 for additional information on determining a sample size.

the entity's change management process. When multiple business process applications and information systems have been identified as areas of audit interest, the auditor may use (1) one population of changes for all or several business process applications or information systems or (2) separate populations of changes for each business process application or information system. However, the auditor will only be able to use one population of changes for multiple business process applications and information systems if the change management process and corresponding approvals are consistent across such applications and systems. In making this decision, the auditor may evaluate such factors as

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

.24 If the auditor concludes that the separate populations of changes will be used for each business process application or information system, the auditor selects separate samples for each population and evaluates the results of each sample separately.

.25 When planning sampling control tests, the auditor should determine a sample size to obtain sufficient, appropriate audit evidence about the operating effectiveness of relevant IS controls. The auditor uses professional judgment in determining the number of items to select and the method used to select them. To determine sample size, the auditor uses professional judgment to determine four factors:

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

Once the auditor determines these factors, the auditor may use automated audit tools to determine sample size and to select samples for testing (see section 330.29).

Nonstatistical Selection for Control Tests

.26 Performing IS control tests that involve nonstatistical selection may provide sufficient evidence, along with other sources of evidence, that an IS control is operating effectively during the year. It may also be the most efficient way to test the control activity. For example, some IS controls may operate biweekly or weekly. For these controls, statistical sampling may not be efficient or even feasible given the small number of items in the population from which the auditor will select the sample. For these controls that operate less frequently, the effect of other sources of evidence is often greater than the effect for more frequent operating controls.

.27 Table 7 provides guidance on the number of items to select when testing small populations associated with controls that operate less frequently. For larger populations, such as IS controls that operate daily, the auditor performs statistical sampling to obtain evidence of control effectiveness.

Table 7: Selecting Items for Testing from Small Populations

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

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

Timing of IS Control Tests

.29 The auditor should determine the timing of control tests to be performed for each IS control activity. This determination is influenced by factors such as (1) the type of evidence available to the auditor to demonstrate whether the IS control activity is designed, implemented, and operating effectively; (2) the nature of the IS control test; and (3) the significance of the IS control activity to achieving the related IS control objective(s).

Automated Audit Tools

.30 Automated audit tools (sometimes referred to as computer-assisted audit techniques, or CAATS) can be used to gather, or assist in gathering, audit evidence and to test the effectiveness of controls. For example, auditors can leverage data analytics tools, such as various programming languages and specialized audit software, in testing IS control activities where discrete data are available. The advantage of using automated audit tools in controls testing is that it is possible to test every item in a population to determine whether there were any control deviations.

.31 To use automated audit tools, the entity needs to provide access to all required resources, including data and other resources. Additionally, obtaining such access may require significant collaboration between the auditor and the entity to reach agreement on the data to be provided and the resources to be used.

.32 If the auditor plans to use automated audit tools, the auditor should understand the following for each:

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

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

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

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

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

- a tool for processing test data that the auditor prepared using the current production version of the client's software but separate from the client's normal input data.

Considerations for Testing IS Controls That Service Organizations Perform

.35 When the auditor identifies user, application, and general control activities that service organizations perform, the auditor obtains evidence about the design, implementation, and operating effectiveness of such controls through one or more of the following procedures:

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

.36 An independent auditor prepares a service organization report for the service organization to be used by entities that use the services provided by the service organization. The intent of the report is to provide assurance over the design of internal controls at a point in time (type 1 report) or the design and operating effectiveness of internal controls over a period of time (type 2 report), including IS controls, based on the service organization's description of controls relevant to the service being provided.[47] A service organization report may be intended to satisfy the needs of multiple auditors conducting engagements with varying objectives. As a result, the service auditor's tests of controls performed by the service organization may or may not address the IS control activities the auditor identified. It is the auditor's responsibility to identify and evaluate the results of relevant tests of controls to determine whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of the relevant IS control activities that the service organization performs.

.37 If the auditor plans to use a service organization report as evidence that IS control activities that a service organization performs are designed, implemented, and operating effectively, the auditor should obtain a report on management's description of a service organization's system and the suitability of the design and operating effectiveness of internal controls over a period of time (type 2 report). The auditor should determine whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and

[47]Type 1 and type 2 reports focus on controls likely to be relevant to entities' internal control over financial reporting, issued under the AICPA's *Clarified Statement on Standards for Attestation Engagements* (AT-C) 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*. There are other types of reports on service organizations that may be available, including reports on controls at a service organization other than those likely to be relevant to entities' internal control over financial reporting (for example, controls that are relevant to entities' compliance with specified requirements of laws, regulations, contracts, or grant agreements).

operating effectiveness of IS control activities to support the auditor's risk assessment by

- assessing the adequacy of the standards under which the service auditor's report was issued;
- evaluating whether the report is for a period that is appropriate for the auditor's purpose;
- determining whether complementary user-entity controls that the service organization identified as relevant to the IS control activities it performs are designed, implemented, and operating effectively;[48]
- evaluating the adequacy of the time period covered by the service auditor's tests of the IS control activities the service organization performs and the time elapsed since performance of such tests; and
- evaluating whether the results of the service auditor's tests of the IS control activities the service organization performs, as described in the service auditor's report, provide sufficient, appropriate evidence to support the auditor's risk assessment.

.38 For federal financial audits, the auditor should refer to the *GAO/CIGIE Financial Audit Manual* (FAM) section 640 when inspecting a service organization report to obtain evidence about the design, implementation, and operating effectiveness of user, application, and general control activities that a service organization performs. The auditor may use FAM section 640A, Service Organization Type 2 Assessment Tool, when determining whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of IS control activities.

.39 For performance audits, the auditor may adapt and apply the assessment tool when determining whether a service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of IS control activities.

.40 There may be instances in which a service organization uses another service organization (subservice organization) to perform services that are likely to be relevant to the user entity's internal control and the auditor's assessment of IS controls. The service organization report will describe either of the following:

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

[48]A service provided by the service organization may be designed with the assumption that certain controls will be implemented by the user entity. In such circumstances, the description of the service organization's system may include a description of the complementary user-entity controls that the user entity is expected to perform.

and from the scope of the service auditor's engagement, the subservice organization's relevant control objectives and related controls.

.41 If the auditor plans to use a type 2 report that excludes the services a subservice organization performs and those services are relevant to the auditor's assessment of IS controls, the auditor should apply the same testing procedures noted in this section to the services that the subservice organization provides.

.42 If the auditor determines that additional evidence about the operating effectiveness of IS control activities that service organization (or subservice organization) performs is required, the auditor may obtain additional evidence by

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

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

.01 Once the auditor has determined the nature, extent, and timing of IS control tests, the auditor performs IS control tests using suitable criteria and evaluates the results, including the significance of any IS control deficiencies identified. In evaluating the results, the auditor performs an overall assessment of the evidence obtained and determines whether the audit procedures performed are adequate to reduce audit risk to an acceptably low level.

Perform IS Control Tests

.02 The auditor should perform control tests of the selected IS control activities using suitable criteria. Criteria may include the statutes, regulations, executive orders, implementing entity guidance, directives, policies, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance of the selected control activity is compared or evaluated. The evidence obtained through the auditor's IS controls tests is included in the auditor's overall assessment of the collective evidence obtained throughout the IS controls assessment.

Determine Whether Relevant IS Control Objectives Are Achieved

.03 The auditor should evaluate the results of control tests to determine whether IS control activities are designed, implemented, and operating effectively to achieve the relevant IS control objectives. Control deviations identified related to the design, implementation, or operating effectiveness of IS control activities are potential IS control deficiencies, which may preclude the achievement of relevant IS control objectives. The auditor investigates and obtains an understanding of the reasons for any deviations from controls noted during control testing.

.04 For control deviations that are not resolved by additional evidence, the auditor should communicate to management, in writing and on a timely basis, the details of the control deviation identified. The auditor should communicate identified control deviations to the entity in sufficient detail for management to consider whether there are additional factors or compensating controls that are relevant to the auditor's determination of whether (1) a control deviation is an IS control deficiency and (2) the related IS control objective is achieved. For example, when the auditor uses statistical sampling for control tests, the auditor considers the tolerable rate of deviation and the rate of control deviations expected (i.e., the deviation rate in the entire population).

.05 The auditor should determine whether there are specific compensating controls that could mitigate each potential IS control deficiency. If the auditor believes that compensating controls could adequately mitigate the potential deficiency and achieve the IS control objective, the auditor should obtain evidence that the compensating controls are designed, implemented, and operating effectively. If such controls effectively mitigate the potential deficiency, the auditor can conclude that the IS control objective is achieved; nonetheless, the auditor communicates any control deviations identified to the entity. If the control deviation is not effectively mitigated, it is a control deficiency, and the auditor documents the criteria, condition, cause, and effect of the finding.

.06 The auditor should communicate to management the criteria, condition, cause, and effect of the IS control deficiencies identified through the IS controls assessment.

Evaluate the Significance of IS Control Deficiencies

.07 The auditor should evaluate and document the significance of identified IS control deficiencies. The auditor evaluates deficiencies individually and in the aggregate and considers the correlation among deficiencies. This evaluation and the audit work performed form the basis of the auditors' determination whether, individually or in combination, the IS control deficiencies are significant in the context of the engagement objectives. In addition, as part of this determination, the auditor considers whether auditor-identified IS control deficiencies were identified in the entity's plans of action and milestones (POA&M) or equivalent records. POA&Ms document the organization's planned actions to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system. POA&Ms are required to be included in authorization packages.[49] If the IS control deficiencies the auditor identified are not identified in the entity's POA&Ms or equivalent records, the auditor attempts to determine why the entity did not identify such deficiencies.

.08 For federal financial audits, the auditor should comply with requirements for classifying control weaknesses as discussed in FAM section 580, Draft Reports.

Assess Sufficiency and Appropriateness of Evidence and Level of Audit Risk

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

.10 The auditor should reassess, based on the audit procedures performed and the collective evidence obtained, the level of IS risk for each of the areas of audit interest. For each area of audit interest, the auditor assesses final IS risk at one of three levels:

[49]Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (July 2016), App. II-16.

- Low. The auditor concludes that IS controls adequately mitigate inherent risks and support the achievement of information processing and information security objectives that are significant to the engagement.
- Moderate. The auditor concludes that IS controls more likely than not adequately mitigate inherent risks and support the achievement of information processing and information security objectives that are significant to the engagement.
- High. The auditor concludes that IS controls more unlikely than likely adequately mitigate inherent risks and support the achievement of information processing and information security objectives that are significant to the engagement.

.11 The auditor should determine whether the audit procedures performed throughout the IS controls assessment are adequate to reduce audit risk to an acceptably low level. Audit risk is a function of IS risk and detection risk. As such, the auditor's overall assessment of the collective evidence obtained and final assessment of IS risk inform the auditor's conclusion regarding audit risk.

.12 For federal financial audits, the auditor should determine whether the IS controls achieve the relevant IS control objectives and support a low assessed level of control risk for the auditor's overall assessment of internal control over financial reporting.

350 Prepare Testing Phase Documentation

.01 The auditor should prepare testing phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand from the audit documentation the nature, timing, extent of audit procedures performed and the results of the IS controls assessment, including the significance of any IS control deficiencies identified.

.02 The auditor should prepare audit documentation containing sufficient, appropriate evidence for the auditor's findings, conclusions, and recommendations before the report is issued.

Completed Audit Plan, Results Memo, and Subordinate Test Plans

.03 The auditor should complete the written audit plan for the IS controls assessment to reflect the results of the audit procedures performed.

.04 The auditor should prepare a written results memo for the IS controls assessment that includes a description of the overall assessment of the collective evidence obtained and the auditor's final determinations regarding IS risk and audit risk.

.05 The auditor should develop and complete subordinate test plans to document the approach for testing controls for the relevant IS control objectives for each area of audit interest. In developing the test plans, the auditor follows the guidance provided in section 320, Select IS Control Activities for Testing, and section 330, Determine the Nature, Extent, and Timing of IS Control Tests. Subordinate test plans for each area of audit interest

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

Sampling Plans

.06 When IS control tests involving statistical sampling are performed, the auditor should prepare written sampling plans that include

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

Technical Reviews

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

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

SECTION 400

REPORTING PHASE

Contents of the Reporting Phase

410 Overview of the Reporting Phase

.01 The reporting phase addresses the auditor's compliance with the *Federal Information System Controls Audit Manual* (FISCAM) methodology and the auditor's responsibilities for communicating the results of an engagement.

.02 The auditor documents compliance with the FISCAM methodology by completing the FISCAM assessment completion checklist (app. 500C). The checklist lists FISCAM's requirements for conducting the information system (IS) controls assessment based on applicable generally accepted government auditing standards (GAGAS) requirements.

.03 Reports are issued to communicate the results of the engagement. In the context of the IS controls assessment, this serves several purposes, including

- clearly communicating IS control deficiencies to those charged with governance, appropriate officials of the audited entity, and appropriate oversight officials and
- providing appropriate officials of the audited entity with recommendations for corrective action.

.04 With regard to communicating the results of an engagement, the auditor considers the engagement objectives, as well as the type of GAGAS engagement (financial audit, attestation engagement, or performance audit), to determine whether a separate report on IS controls is issued or the results of the IS controls assessment are incorporated into another report. For example, when an assessment is performed as part of a financial audit, the results of the IS controls assessment are incorporated into the auditor's report on internal control over financial reporting.

420 Determine Compliance with FISCAM

.01 The auditor should determine whether the FISCAM methodology was followed. The FISCAM assessment completion checklist (app. 500C) includes FISCAM's requirements for conducting the IS controls assessment. If the auditor is using a different IS controls assessment methodology, the auditor may use the FISCAM assessment completion checklist to provide a crosswalk between the audit methodology used and FISCAM.

430 Draft Report

.01 Reports are issued to communicate the results of the engagement. In the context of the IS controls assessment, this serves several purposes, including

- clearly communicating IS control deficiencies to those charged with governance, appropriate officials of the audited entity, and appropriate oversight officials and
- providing appropriate officials of the audited entity with recommendations for corrective action.

.02 Report content related to the IS controls assessment generally includes (1) the objectives, scope, and methodology of the engagement; (2) findings, conclusions, and recommendations, as appropriate; and (3) if applicable, the nature of any confidential or sensitive information omitted from the report. Each of these elements, including any differences in requirements based on engagement type, are discussed below.

Objectives, Scope, and Methodology

.03 Report users need information regarding the engagement objectives, scope, and methodology to understand the purpose of the engagement; the nature and extent of the audit work performed; the context and perspective regarding what is reported; and any significant limitations in the audit objectives, scope, or methodology. Report content relevant to objectives, scope, and methodology differs among engagement types. Depending on the engagement type, the auditor addresses the specific requirements established in GAGAS.

Findings, Conclusions, and Recommendations

.04 Reporting responsibilities vary depending on the nature of the findings and conclusions. Engagement objectives may or may not require an overall conclusion on the effectiveness of IS controls. For example, when reporting on internal control, the audit report may

- provide an overall conclusion (e.g., the entity's IS controls are or are not effective in achieving the IS control objectives relevant to the audit) and communicate identified deficiencies;
- limit reporting to identified IS control deficiencies without providing an overall conclusion (e.g., "based on our work, we identified the following IS control deficiencies"); or
- report findings in the context of the engagement objectives, such as how they relate to (1) the design, implementation, and operating effectiveness of specific controls significant to the achievement of the engagement objectives or (2) the reliability of data intended to materially support findings, conclusions, or recommendations.

.05 Generally, when internal control deficiencies are determined to be significant to the engagement objectives, such deficiencies are reported.[50] Because GAGAS reporting requirements relevant to findings and conclusions vary depending on the engagement type, reporting requirements are discussed below by engagement type.

Financial Audits

.06 GAGAS reporting requirements for financial audits relevant to internal control are addressed in the *GAO/CIGIE Financial Audit Manual* (FAM).[51] For financial audits, the auditor should comply with the reporting requirements in FAM 580. See FAM 580 for detailed reporting requirements, including requirements for classifying control weaknesses and reporting weaknesses relevant to the Federal Managers' Financial Integrity Act (FMFIA) and the Federal Financial Management Improvement Act of 1996 (FFMIA).

Attestation Engagements

.07 For examination-level attestation engagements, the auditor should include in the examination report all internal control deficiencies, even those communicated early, that are considered to be significant deficiencies or material weaknesses that the auditor identified based on the engagement work performed.

Performance Audits

.08 The auditor should include in the audit report any deficiencies in internal control that are significant to the engagement objectives and based upon the audit work performed.

.09 When the auditor detects deficiencies in internal control that are not significant to the engagement objectives but warrant the attention of those charged with governance, the auditor should include those deficiencies in the report or communicate those deficiencies in writing to audited entity officials. If the written communication is separate from the audit report, the auditor should refer to that written communication in the audit report.

Presentation of Findings, Conclusions, and Recommendations

.10 When presenting findings, the auditor should develop the elements of the findings to the extent necessary to assist management or oversight officials of the audited entity in understanding the need for taking corrective action. For performance audits, the extent to which the elements of a finding are developed depends on the engagement objectives.

.11 The elements of a finding are criteria, condition, cause, and effect.

- Criteria identify the required or desired state or expectation with respect to the program or operation. Condition is a situation that exists.

[50]See section 300 for additional information on evaluating the significance of internal control deficiencies. If fraud is discovered as part of the engagement, the auditor addresses reporting requirements established in GAGAS.
[51]See FAM 580.

- Cause is the factor or factors responsible for the difference between the condition and the criteria, and may serve as a basis for recommendations for corrective actions.
- Effect or potential effect is the outcome or consequence resulting from the difference between the condition and the criteria.

This information helps senior management understand the significance of the deficiencies and develop appropriate corrective actions.

.12 The auditor should place audit findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the findings. As appropriate, the auditor should relate the instances identified to the population or the number of cases examined and quantify the results in terms of measures that give the reader a basis for judging the prevalence and consequences of the findings. If the results cannot be projected, the auditor should limit conclusions appropriately. For performance audits, the auditor should describe in the report limitations or uncertainties in the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the audit objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions.

.13 When reporting on the results of the audit work, the auditor should disclose significant facts relevant to the objectives of the work and known to the auditor that if not disclosed could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices. For example, a limited review of controls over a type of operating system relevant to identified areas of audit interest, such as applications that support significant business processes, may not identify any significant weaknesses. However, there may be significant weaknesses in other areas, such as other types of operating systems, that the auditor is unaware of because the scope of the IS controls assessment is limited to areas of audit interest relevant to engagement objectives. As such, the auditor evaluates any potential limitations of the work on the auditor's report and the needs and expectations of users.

.14 The auditor should report conclusions that are logical inferences based on the auditor's findings, not merely a summary of the findings. The strength of the auditor's conclusions depends on the persuasiveness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to recommendations and convince a knowledgeable user of the report that action is necessary.

.15 The auditor should provide recommendations for corrective action for any sufficiently developed findings that are significant to the engagement objectives. The auditor should make recommendations that flow logically from the findings and conclusions, are directed at resolving the causes of identified deficiencies and findings, and clearly state the actions recommended. When feasible, the auditor should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions.

Reporting Confidential or Sensitive Information

.16 IS controls information may be prohibited from public disclosure because it may be designated as or derived from classified, sensitive but unclassified, or proprietary information.[52] Some audit organizations do not have original or derivative classification authority or the ability to identify unclassified information that may be subject to safeguarding or dissemination controls.[53] Therefore, for reports that contain, or may contain, information prohibited from public disclosure, the auditor should request that the source agency perform a classification, security, or sensitivity review of the draft report . The auditor should evaluate entity concerns and make appropriate report revisions or redactions, considering legal or regulatory requirements.

.17 If certain information is prohibited from public disclosure or is excluded from a report because of its confidential or sensitive nature, the auditor should disclose in the report that certain information has been omitted and the circumstances that make the omission necessary.

.18 The auditor should evaluate whether this omission could distort the results or conceal improper or illegal practices and revise the report language as necessary to avoid report users drawing inappropriate conclusions from the information presented.

.19 When the audit organization is subject to public records laws, the auditor should determine whether public records laws could affect the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. Auditors use professional judgment to determine the appropriate means to communicate the omitted information to management and those charged with governance, considering, among other things, whether public records laws could affect the availability of classified or limited use reports.

[52]The federal government is transitioning to the use of the term ‘controlled unclassified information’ in place of terms such as ‘sensitive but unclassified’ or ‘for official use only’.
[53]Original classification is the initial determination by a designated classification authority that an item of information requires, in the interest of national security, protection against unauthorized disclosure. Derivative classification means, in part, incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

440 Prepare Reporting Phase Documentation

.01 The auditor should prepare reporting phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand conclusions reached, including evidence that supports the auditor's conclusions.

Departures from FISCAM

.02 When auditors do not comply with applicable FISCAM requirements because of statute, regulation, scope limitations, restrictions on access to records, or other issues affecting the audit, the auditor should document the departure from the FISCAM requirements and the effect on the engagement and on their conclusions. When documenting departures from the FISCAM requirements, the audit documentation requirements apply to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirements. The auditor may document departures in the FISCAM assessment completion checklist (see app. 500C).

APPENDIX 500A

FISCAM GLOSSARY

Glossary Terms

This glossary is provided to clarify guidance in the *Federal Information System Controls Audit Manual* (FISCAM). When terminology differs from that used at an entity, auditors use professional judgment to determine if there is an equivalent term.

Access agreement	A user-based agreement that specifies user responsibilities when exchanging information or accessing information or systems that contain the exchanged information. Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.
Access control	The process of granting or denying specific requests to (1) obtain and use information and related information processing services and (2) enter specific physical facilities where information systems and information system resources reside. See also logical access control and physical access control.
Access control list	A register of (1) users (including groups of users, devices, and processes) that have permission to use a particular system resource and (2) the types of access they have been permitted.
Access control software	A type of software external to the operating system that provides a means of specifying the users (including groups of users, devices, and processes) that have access to a system, including specific system resources, and the capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection, such as denying access for which the user is not expressly authorized, allowing access that is not expressly authorized but providing a warning, or allowing access to all resources without warning regardless of authority.
Access controls	A general control category within the FISCAM Framework representing the control activities that apply to the process of granting or denying specific requests to (1) obtain and use information and related information processing services and (2) enter specific physical facilities where information systems and information system resources reside.

Access path	The logical route that an end user request takes through hardware and software components to access computer-processed information. An access path typically includes any information system component capable of enforcing access restrictions or any component that could be used to bypass an access restriction, including the telecommunications software, transaction processing software, and application software.
Access privileges	Precise statements that define the extent to which users, programs, or workstations can access computer systems and use or modify (e.g., read, write, execute, create, and delete) the programs and data on a system, and under what circumstances this access will be allowed.
Account management	Involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
Accountability	The security goal that generates the requirement for an entity's actions to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Accreditation	See authorization.
Accreditation boundary	See authorization boundary.
Accuracy	An information processing objective that aims to provide reasonable assurance that data relating to transactions and events are appropriately and timely recorded at each stage of processing.
Adequate security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Alternate processing site	A site geographically distinct from primary processing sites that provides processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as a cloud-based service provider or other

	internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites.
Alternate storage site	A site geographically distinct from primary storage sites that maintains duplicate copies of information and data if the primary storage site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites.
Alternate work site	Entity-authorized work from home (or other designated location) or at geographically convenient satellite offices (e.g., telecommuting, teleworking, or remote working).
Application	A combination of application software, system software, and hardware designed and implemented to serve a particular function.
Application controls	Controls that are incorporated directly into application software to help ensure the completeness, accuracy, and validity of transactions and data. Application controls include controls over the input, processing, and output of data.
Application software	Software designed to serve a particular function that has specific input, processing, and output requirements. Application software uses database management software to store and retrieve application data. Application software relies on system software to run.
Approach	The nature, extent, and timing of audit procedures applied to the significant business processes and areas of audit interest based on relevant IS control objectives and control activities selected for testing.
Areas of audit interest	A subset of the entity's information systems, information system components, and information system resources that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. At the business process level, areas of audit interest may include business process applications, 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.
Assessor	An individual responsible for conducting security and privacy assessment activities under the guidance and direction of a Designated Authorizing Official. For cloud services, the individual is an independent third party.
Audit assurance	The complement of audit risk, which is an auditor judgment.
Attack	Attempt to gain unauthorized access to an information system's services, resources, or information, or an attempt to compromise an information system's integrity, availability, or confidentiality.
Attribute	Any distinctive feature, characteristic, or property of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means.
Attribute sampling	Statistical sampling that reaches a conclusion about a population in terms of a rate of occurrence.
Audit logging	Recording a chronological record of system activities, including records of system accesses and operations performed in a given period.
Audit plan	A description of the audit work to be performed. An audit plan is comprised of the audit strategy and approach for testing controls for each area of audit interest.
Audit procedure	The specific steps and tests auditors perform to address the engagement objectives.
Audit record	An individual entry in an audit log related to an audited event.
Audit risk	The possibility that the auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete. The assessment of audit risk involves both quantitative and qualitative considerations. Audit risk is a function of information

	security (IS) risk (inherent risk and control risk) and detection risk.
Audit strategy	Description of and key decisions about the proposed audit (or engagement) objectives, scope, and the auditor's basis for those decisions.
Audit trail	A chronological record showing user access and activity or security-related event in an information system during a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, process, or device (e.g., passwords, tokens, biometrics, key cards, Public Key Infrastructure certificates, or multifactor authenticator).
Authenticity	The property of being genuine, verifiable, and trusted and establishing confidence in the validity of a transmission, a message, or a message originator.
Authorization	The official management decision given by a senior federal official to authorize operation of an information system and to explicitly accept the risk to entity operations (including mission, functions, image, or reputation), entity assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls in that agency information systems inherit. Authorization is also known as authorization to operate.
Authorization boundary	Includes all components of an information system to be authorized for operation by an authorizing official, and excludes separately authorized systems to which the information system is connected.
Authorizing official	A senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to entity operations (including mission, functions, image, or reputation), entity assets, individuals, other organizations, and the United States.

Availability	Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.
Backup	A copy of files and programs made to facilitate recovery if necessary.
Baseline configuration	A documented set of specifications for an information system or a configuration item within a system that has been formally reviewed and agreed on at a given point in time and can be changed only through change control procedures.
Biometric	Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.
Business process	The primary means through which the entity accomplishes its mission. Business processes transform inputs into outputs through a series of transactions or activities to achieve the entity's operations, reporting, and compliance objectives. Business processes support the business functions the entity performs in accomplishing its mission. Financial management is one example of a business function. Financial management business processes include collections, disbursements, and payroll, as well as the related accounting applications.
Business process application	An application that helps the entity perform a specific business process or related business processes within a business function.
Business process application controls	Application controls applied to business processes to help ensure the completeness, accuracy, and validity of transactions and data.
Business process controls	A control category within the FISCAM Framework representing IS controls that are designed to achieve one or more information processing objectives– completeness, accuracy, and validity. When designed, implemented, and operating effectively, business process controls reasonably assure the completeness, accuracy, and validity of transactions, events, and data. Business process controls consist

	of user and application controls as well as those general controls that are designed to achieve information security objectives but directly support information processing objectives.
Business process level	Consists of the user, application, and general controls relevant to specific business processes.
Certificate	A digital representation of information, which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certificate store	Local storage on the computer where certificates are stored. The certificates stored could be issued from a number of different certification authorities.
Certification authority	A trusted entity that issues and revokes public key certificates.
Certification path	A chain of trusted public key certificates that begins with a certificate whose signature can be verified by a relying party using a trust anchor, and ends with the certificate of the entity whose trust needs to be established.
Chief information officer	Agency official responsible for (1) providing advice and other assistance to the head of the executive entity and other senior management personnel of the executive entity to ensure that information technology is acquired and information resources are managed for the executive entity in a manner that is consistent with statutes, regulations, executive orders, directives, implementing guidance, policies, and priorities established by the head of the executive entity; (2) developing, maintaining, and facilitating the implementation of a sound, secure, and integrated IT architecture for the entity; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive entity, including improvements to work processes of the entity.
Climate controls	A subset of environmental protection controls that prevents or mitigates damage to facilities and

	interruptions in service. Thermostats and dehumidifiers are some examples of climate controls.
Code	Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator. See also object code and source code.
Code analysis	The act of analyzing source code with or without executing the code to identify poor coding practices that might introduce security flaws into code during the code development phase.
Collaborative computing	Applications and technology (e.g., white boarding and group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment.
Common control	A security or privacy control that one or more information systems inherit. See also control inheritance.
Compensating control	A control that reduces the risk of an existing or potential control weakness that could result in errors or omissions.
Compiler	A program that translates source code into object code.
Completeness	An information processing objective that aims to provide reasonable assurance that all transactions and events that should have been recorded have been properly recorded at each stage of processing.
Computer-assisted audit technique	Any automated audit technique, such as audit software, test data generators, computerized audit programs, and special audit utilities.
Computer program	Complete sets of ordered instructions that a computer executes to perform a specific operation or task.
Concept of operations	Verbal and graphic statement, in broad outline, of an organization’s assumptions or intent in regard to an operation or series of operations of new, modified, or existing information systems.

Confidence level	The probability associated with the range of values into which an estimate of a population characteristic is expected to fall.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
Configuration auditing	Procedures for determining alignment between the implemented configuration settings of an information system and the corresponding baseline configuration settings.
Configuration control	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation.
Configuration control board	A group of qualified people with responsibility for regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.
Configuration item	An information system component or an aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process. Configuration items are the information system components, such as the hardware, software, firmware, and documentation, that are placed under configuration management.
Configuration management	A general control category within the FISCAM framework representing a collection of activities that involve identifying and managing security features for all hardware, software, and firmware components of an information system at a given point that systematically controls changes to that configuration during the system's life cycle.
Configuration settings	The set of parameters (e.g., flags, settings, and paths) that can be changed in hardware, software, or firmware that affect the security posture and functionality of the information system.

Contingency plan	A plan that is maintained for disaster response, backup operations, and post disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.
Contingency planning	A general control category within the FISCAM framework representing a collection of activities that provide for the continuation of critical or essential mission and business functions in the event of a system disruption, compromise, or failure and the restoration of the information system following a system disruption.
Continuity of operations plan	A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days during a disaster event before returning to normal operations.
Continuous monitoring strategy	Maintaining ongoing awareness to support organizational risk decisions. This can include the use of automated procedures to ensure that security controls are not circumvented or the use of tools to track actions taken by those suspected of misusing the information system.
Control activities	One of the five components of internal control. Control activities are the policies, procedures, techniques, and mechanisms that help ensure that management directives are carried out and respond to risks in the internal control system, which includes the entity's information system.
Control baseline	A predefined set of minimum privacy or security controls for low-impact, moderate-impact, or high-impact information or information systems that may be tailored to address specific protection needs based on risk.
Control categories	Groupings of related controls pertaining to similar types of risk. FISCAM groups controls into the following categories: business process controls, security management, access controls, configuration management, segregation of duties, and contingency planning.

Control deficiency	A condition when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct errors in information processing on a timely basis. The definition of control deficiency may differ by engagement type. For financial audits, control deficiencies exist when misstatements are unlikely to be prevented or detected and corrected on a timely basis.
Control dependency	Exists when the effectiveness of a control activity depends on the effectiveness of other control activities.
Control environment	One of the five components of internal control. Control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
Control inheritance	A situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.
Control objectives	The aim or purpose of specified controls. Control objectives address the risks that the controls are intended to mitigate.
Control risk	The likelihood that conditions or events, related to the areas of audit interest, that could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives, will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls.
Critical element	Management tasks that are necessary for establishing adequate controls within the FISCAM control category.
Critical infrastructure	System and assets, whether physical or virtual, so vital to the United States that the incapacity or

	destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Cryptographic key	A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually, a sequence of random or pseudorandom bits are used initially to set up and periodically change the operations performed in cryptographic equipment for to encrypt or decrypt electronic signals, or to determine electronic counter-countermeasures patterns, or to produce another key.
Data	Facts and information that can be communicated and manipulated.
Data center	A purpose-built, physically separate, and dedicated space that contains one or more racks of servers and high performance computers; has a dedicated uninterruptable power supply, backup generator for prolonged power outages, or combination of both; and has a dedicated cooling system or zone.
Data communications	The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Data definition	Identification of all fields in the database, how they are formatted, how they are combined into different types of records, and how the record types are interrelated.
Data file	A collection of records stored in computerized form.
Data management system	Includes databases, as well as the middleware, database management software, and data warehouse software, used to define, organize, maintain, and control access to data.
Data owner	Official with statutory or operational authority for specified data and responsibility for establishing the controls for the data's generation, collection, processing, dissemination, and disposal.
Data processing	The collective set of data actions involved in the data life cycle, including data collection, retention,

	logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.
Data strategy	Plan used to identify data needed to support business processes. A clearly defined data strategy minimizes data redundancies fundamental to an efficient, effective transaction processing function.
Data validation	Checking transaction data for any errors or omissions that can be detected by examining the data.
Database	A repository of information or data, which may or may not be a traditional relational database system.
Database administrator	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application software and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database.
Database management	Tasks related to creating, maintaining, organizing, and retrieving information from a database.
Database management software	Software designed to define, organize, maintain, and control access to data. Application software uses database management software to store and retrieve application data. Database management software depends on system software to run. Database management software is often referred to as a database management system, or DBMS.
Denial-of-service-attack	Occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. These attacks can cost an organization both time and money while its resources and services are inaccessible.
Detection risk	The risk that the nature, extent, and timing of audit procedures will not detect conditions or events

	related to the areas of audit interest that could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives. Detection risk is a function of the effectiveness of the audit procedures and their application by the auditor.
Device lock	A temporary action taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences.
Dial-up access	A means of connecting to another computer, or a network similar to the internet, over a telecommunications line using a modem-equipped computer.
Digital media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Digital signature	Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.
Disaster recovery plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to their original state.
Engagement objective	What the engagement is intended to accomplish. Engagement objectives identify the audit subject matter and performance aspects to be included. Engagement objectives can be thought of as questions about the program that the auditors seek to answer based on evidence obtained and assessed against criteria. Engagement objectives may also pertain to the current status or condition of a program.

Entity level	Relevant to the entity or component as a whole. Information system controls applied at the entity level consist of such general controls.
Entry points	Access points to the entity's information systems. This may include remote access through dial-up, wireless devices, or the internet.
Environmental controls	A subset of contingency planning controls that prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls.
Event	Any observable occurrence in a network or system.
Federal Information Security Modernization Act of 2014	A federal law enacted to, among other things, provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, Pub. L. No. 113-283, 129 Stat. 3073 (Dec. 18, 2014). This 2014 statute largely superseded the similar Federal Information Security Management Act of 2002, Pub. L. No. 107-347, title III,116 Stat. 2899, 2946 (Dec. 17, 2002). In particular, this 2014 statute amended the U.S. Code to establish a new subchapter on information security (44 U.S.C. §§ 3551-3558). In the FISCAM, "FISMA" sometimes refers to both the 2014 statute and its 2002 predecessor collectively.
Federal Managers Financial Integrity Act	The objective of 31 U.S.C. § 3512 (c) and (d), commonly referred to as of the Federal Managers' Financial Integrity Act (FMFIA), is to provide reasonable assurance that (1) obligations and costs are in compliance with applicable law; (2) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and (3) revenues and expenditures applicable to executive entity operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

Field	A location in a record in which a particular type of data is stored. In a database, this is smallest unit of data that can be named.
File	A collection of information logically grouped into a single entity and referenced by a unique name, such as a filename.
Financial management systems	Systems that include the financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. This is a statutory definition included in Federal Financial Management Improvement Act of 1996 (FFMIA).
Firecall	Any method established to provide emergency access to a secure information system.
Firewall	Hardware and software components that protect one set of system resources (e.g., computers and networks) from attack by outside network users (e.g., internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.
Firmware	Software that is embedded in the read-only memory of hardware that enables the hardware to function and communicate with other software.
Flow chart	A diagram of the movement of transactions, computer functions, media, and operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, and other categories. to depict the system or program.
Fraud	A type of illegal act involving the obtaining of something of value through willful misrepresentation. Whether an act is fraudulent is determined through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk.

Generally accepted government auditing standards	Also referred to as the Yellow Book, the generally accepted government auditing standards (GAGAS) provide a framework for performing high-quality audits of government organizations, programs, activities, and functions, and of government assistance received by contractors, nonprofit organizations, and other nongovernment organizations, with competence, integrity, objectivity, and independence. These standards are to be followed by auditors and audit organizations when required by law, regulation, agreement, contract, or policy. They pertain to auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports.[54]
General controls	The collection of control categories within the FISCAM Framework representing IS controls that are designed to achieve one or more information security objectives—confidentiality, integrity, and availability. These categories include security management, logical and physical access, configuration management, segregation of duties, and contingency planning. General controls are the policies and procedures that apply to all or a large segment of an entity's information systems. When designed, implemented, and operating effectively, these controls reasonably assure the confidentiality, integrity, and availability of information and information systems. These general controls create a suitable environment to support the effective operation of business process controls.
General support system	An interconnected set of information system resources under the same direct management control that share common functionality. Normally, the purpose of a general support system is to provide processing or communications support.
Hardware	Physical equipment used to process, store, or transmit computer programs or data. It includes computing devices (e.g., servers, workstations, and

[54]GAO, *Government Auditing Standards: 2018 Revision*, GAO-21-368G (Washington, D.C.: July 2018, updated April 2021).

	mobile devices), peripheral equipment (e.g., keyboards, monitors, webcams, and printers), networking devices (e.g., firewalls, routers, and switches), cables, and other telecommunications equipment.
Hashing	The process of using a mathematical algorithm against data to produce a numeric value that is representative of those data.
Impact level	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an information system.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident response program	A process that involves detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference.
Incompatible duties	When work responsibilities are not segregated such that one individual controls critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic,

	cartographic, narrative, electronic, or audiovisual forms.
Information owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information processing objectives	Requirements for effective information processing, including completeness, accuracy, and validity.
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information security management program plan	Formal document that provides an overview of the security requirements for an entity-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information spill	Security incident that results when information that is thought to be at certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level.
Information system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information system boundaries	Logical or physical boundaries around information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Firewall devices represent the most common boundary protection technology at the network level.
Information system component	A discrete identifiable IT asset that represents a building block of a system and may include hardware, software, and firmware.
Information system controls	Consist of those internal controls that depend on information system processing and include user controls, application controls, and general controls. Information system controls help ensure effective information processing.

Information system owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information system processing	Processing performed by information systems through the use of information technology.
Information system resource	Any entity-defined resource that is needed to support information system processing and is protected from unauthorized access, use, modification, or destruction. Information system resources include hardware, software, data, devices, equipment, media, and services.
Information system risk	The auditor's combined assessment of inherent risk and control risk related to the areas of audit interest.
Inherent risk	The likelihood that conditions or events, related to the areas of audit interest, could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives, without consideration of related IS controls.
Input	Any information entered into a computer, or the process of entering data into the computer.
Integration testing	Testing to determine if related information system components perform to specifications.
Integrity	Guarding against improper information modification or destruction, which includes ensuring information's nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
Interconnection security agreement	A document that regulates security-relevant aspects of an intended connection between an entity and an external system. It regulates the security interface between any two systems operating under two distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal memorandum of understanding that defines high-level roles and responsibilities in management of a cross-domain connection.

Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user.
Interface design	Uses guidelines set by the interface strategy and provides specific information for each of the characteristics defined in the interface strategy.
Interface strategy	Describes at the highest level how the interfaces are implemented between two applications. The interface strategy includes an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data are interfaced completely and accurately, timing requirements, assignment of responsibilities, on-going system balancing requirements, and security requirements.
Internal control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of the entity will be achieved.
Intrusion	A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, unauthorized access to an information system or information system resource.
Intrusion detection system	Software that inspects network activity to identify suspicious patterns that may indicate a network or system attack.
Intrusion prevention system	Software that inspects network activity to identify suspicious patterns that may indicate a network or system attack and can also attempt to stop the activity, ideally before it reaches its targets.
Inventory	A listing of items including identification and location information.
Job	A set of data that completely defines a unit of work for a computer. A job usually includes programs, linkages, files, and instructions to the operating system.

Key resources protection plan	A plan that identifies key resources across all types of asset types and the corresponding consequences of loss.
Labeling	The association of attributes with the subjects and objects represented by the internal data structures within information systems. This facilitates system-based enforcement of information security and privacy policies.
Least privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Library	A collection of similar files, such as data sets contained on tape or disks and stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. Libraries are also called program libraries and partitioned data sets. Library can also refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries.
Log	A record of the events occurring within an organization's systems and networks.
Logical access	Ability to interact with information system resources granted using identification, authentication, and authorization.
Logical access control	The policies, procedures, organizational structure, and electronic access controls designed to restrict access to computer software and data files. Such controls are also referred to as logical security.
Log-on	The process of establishing a connection with, or gaining access to, a computer system or peripheral device.
Maintenance	Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time.

Major application	An application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in that application.
Major information system	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Marking	The association of attributes with objects in a human-readable form displayed on system output. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies.
Master data	Referential data that provides the basis for ongoing business activities, for example, data about customers, vendors, and employees.
Material weakness	For financial audits, a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. The definition of material weakness may differ by engagement type.
Materiality	An auditing concept regarding the relative importance of an amount or item. For financial audits, an item is considered not to be material when it is not significant enough to influence decisions or have an effect on the financial statements.
Media controls	Controls implemented to prevent unauthorized physical access to digital (e.g., diskettes, flash drives, thumb drives, and compact disks) and printed (e.g., paper and microfilm) media removed from an

	information system and during pickup, transport, and delivery to authorized users.
Methodology	The nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives.
Middleware	Software designed for data transport and communications.
Mobile code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Multifactor authenticator	An authenticator that provides more than one distinct authentication factor, such as a cryptographic authentication device with an integrated biometric sensor.
Naming conventions	Standards for naming information system resources, such as data files, program libraries, individual programs, and applications.
Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area.
Network administration	The function responsible for maintaining secure and reliable network operations. This function serves as a liaison for user departments to resolve network needs and problems.
Network component	Any device that supports a network, including workstations, servers, switches, and routers.
Network session	A connection between two network component peers.
Nonrepudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual

	took a particular action, such as creating information, sending a message, approving information, and receiving a message.
Object code	Machine-readable instructions translated from source code by a compiler or assembler program. A file of object code may be immediately executable or it may require linking with other object code files (e.g., libraries) to produce a complete executable program. See also code and source code.
Operating system	The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral hardware, and presents a default interface to the user when no application program is running.
Operational environment	Context determining the setting and circumstance of all influences on an information system.
Output	Data and information produced by information system processing, such as graphic display or hard copy.
Output device	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system.
Override	Decision made by entity management or operation staff to bypass established controls to allow a transaction (or transactions) that would otherwise be rejected to be processed.
Owner	Manager or director who has responsibility for an information system resource, such as a data file or application software.
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs.
Partitioning	Process of physically or logically separating different functions, such as applications, security, and communication activities. Separation may be accomplished by using different computers, central processing units, operating systems, network addresses, or combinations of these methods.

Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Patch	An additional piece of code that has been developed to address specific problems or flaws in existing software.
Penetration testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.
Personally identifiable information	Any information about an individual maintained by an entity, including (1) any information that can be used to distinguish or trace an individual's identity, such as that person's name, Social Security number, date of birth, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Physical access control	Involves restricting physical access to information system resources and protecting these resources from intentional or unintentional loss or impairment.
Plan of action and milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Platform	The logical information system resources necessary to run application software, including the operating system and related computer programs, tools, and utilities.
Privacy impact assessment	An analysis of how information is handled to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a

	formal document detailing the process and the outcome of the analysis.
Privacy management program plan	A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the privacy officer and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
Privacy requirements	Requirements levied on an information system that are derived from statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, procedures, organizational mission, or business case needs with respect to privacy.
Privileged account	An authorized information system account with approved authorizations of a privileged user.
Privileged user	A user who is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Process	Systematic sequences of operations to produce a specified result. This includes all functions performed using a computer, such as editing, calculating, summarizing, categorizing, and updating.
Processing	The execution of program instructions by the computer's central processing unit.
Production control and scheduling	The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is used in this task.
Production environment	An environment where functionality and availability must be ensured for the completion of day-to-day activities.

Programmer	A person who designs, codes, tests, debugs, and documents computer programs.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, which prevents others from duplicating a product or program unless an explicit license is purchased.
Protocol	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.
Public Key Infrastructure	A set of policies, processes, server platforms, software, and workstations used for administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Public Key Infrastructure certificate	A digital representation of information that at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Quality assurance testing	The function that reviews software project activities and tests software products throughout the software life cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures and (2) the software meets the user-defined functional specifications.
Query	The process of extracting data from a database and presenting it for use.
Random sample	A method of selecting a sample of items from a population so that every combination of the same number of items has an equal probability of selection.
Record	A unit of related data fields, or the group of data fields that can be accessed by a program and contains the complete set of information on a particular item.
Relevant control objectives	Those control objectives that are necessary to support the achievement of the engagement objectives

Remote access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the internet).
Remote maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).
Residual risk	Portion of risk remaining after security measures have been applied.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk assessment	One of the five components of internal control. Risk assessment is the entity's identification, analysis, and management of risks relevant to achieving its objectives. This assessment provides the basis for developing appropriate responses to risk.
Risk factor	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment.
Risk management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system. The process includes conducting a risk assessment, implementing a risk mitigation strategy, and employing techniques and procedures for the continuous monitoring of the security state of the information system.
Risk management strategy	A strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.
Rogue wireless access point	An unauthorized node on a network that connects to a wired network using a wireless network standard.

Router	An intermediary device on a communications network that expedites message delivery. As part of a local area network, a router receives transmitted messages and forwards them to their destination over the most efficient available route.
Run	A popular, idiomatic expression for program execution.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features; management constraints; personnel security; and security of physical structures, areas, and devices. Safeguards is synonymous with security controls and countermeasures.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Scope	The boundary of the audit that is directly tied to the engagement objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular program or aspect of a program, the necessary documents or records, the period of time reviewed, and the locations that will be included.
Security administrator	Person who is responsible for managing the security program for computer facilities, computer systems, data that are stored on computer systems or transmitted via computer networks, or a combination of these.
Security architecture	A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.
Security categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in Committee on National Security Systems (CNSS)

	Instruction 1253 for national security systems and in Federal Information Processing Standards (FIPS) 199 for other than national security systems.
Security controls	The controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Security management	A general control category within the FISCAM Framework representing a collection of activities that provide the foundation of a security-control structure and reflect senior management's commitment to addressing security risks.
Security objectives	Requirements for effective information security, including confidentiality, integrity, and availability.
Security requirements	Requirements levied on an information system that are derived from laws, executive orders, implementing entity guidance, directives, policies, instructions, regulations, organizational mission, or business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Segregation of duties	A general control category within the FISCAM framework representing a collection of activities that include having policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations and thereby prevent unauthorized actions or unauthorized access to assets or records. Segregation of duties involves segregating work responsibilities so that one individual does not control all critical stages of a process.
Sensitive	The nature of information system resources where the loss, misuse, or unauthorized access or modification could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled.

Server	A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).
Service	See system service.
Service auditor	An independent auditor hired by the service organization to provide a report on internal controls at the service provider.
Service-level agreement	Represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities; details on the type of service; expected performance level (e.g., reliability, acceptable quality, and response times); and requirements for reporting, resolution, and termination.
Service organization	External organizations used to support business processes. Service organizations provide services ranging from performing a specific task (e.g., payroll processing) to replacing entire business units or functions of an entity.
Significant	The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. 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. The term significant is comparable to the term material as used in the context of financial audit engagements.
Significant business process	Business processes that are significant to the engagement objectives. (paragraph 230.02)
Significant deficiency	For financial audits, a deficiency, or a combination of deficiencies, in internal control over financial reporting, that is less severe than a material weakness yet important enough to merit attention by

	those charged with governance. The definition of significant deficiency may differ by engagement type.
Smart card	A plastic card with embedded, integrated circuits that can store, process, and communicate information for authenticating a user.
Software	An integrated set of computer programs that facilitate the use of a computer to perform operations or tasks.
Source code	A set of computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator. A programmer writes source code in a programming language that humans can read and understand. Source code is ultimately translated into object code, which a computer can read. See also code and object code.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Standard	In computing, a set of detailed technical guidelines to establish uniformity in an area of hardware or software development.
Switch	A network component that filters and forwards packets between local area network segments.
System	See information system.
Systematic random sample	A method of selecting a sample of items from a population in which every *n*th item is selected using one or more random starts.
System administrator	An individual, group, or organization responsible for setting up and maintaining a system or specific system elements, implements approved secure baseline configurations, incorporates secure configuration settings for information system components, and conducts or assists with configuration monitoring activities as needed.
System boundary	All components of an information system to be authorized for operation by an authorizing official. The system boundary excludes separately

	authorized systems, to which the information system is connected.
System developer	An individual group or organization that develops hardware and software for distribution or sale.
System development life cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.
System information exchange	Include connections via leased lines or virtual private networks; connections to internet service providers; database sharing or exchanges of database transaction information; connections and exchanges with cloud services; exchanges via web-based services; or exchanges of files via file transfer protocols, network protocols (e.g., IPv4 and IPv6), email, or other organization-to-organization communications.
System interconnection	A direct connection between two or more systems in different authorization boundaries to exchange information; allow access to information, information services, and resources; or both.
System-level	Information system general controls applied to an information system. These controls are more specific than those applied at the entity level and often correspond to one of three sublevels inherent in all information systems—infrastructure, platform, and software.
System privacy plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks. The plan details how the controls have been implemented and describes the methodologies and metrics that will be used to assess the controls.
System security plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System service	A function performed by system software that facilitates information processing, storage, or transmission. Such functions include loading and

	executing computer programs, resource allocation, and error detection.
System software	Software designed to operate and control the processing activities of hardware. It includes the operating system and utility programs and is distinguished from application software.
System utilities	Software used to perform system maintenance routines that are frequently required during normal processing operations. Some of the utilities have powerful features that will allow a user to access and view or modify data or code.
Telecommunications	The preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.
Test plan	A document that describes the approach for testing controls for each area of audit interest.
Those charged with governance	Those who have the responsibility for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit, including related internal controls. For a federal entity, those charged with governance may be members of a board or commission, an audit committee, the secretary of a cabinet-level department, or senior executives and financial managers responsible for the entity.
Threat	Any circumstance or event with the potential to adversely affect entity operations (including mission, functions, image, or reputation), entity assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.
Token	A device used to store cryptographic information and possibly also perform cryptographic functions for use in authentication systems.
Tolerable rate of deviation	A rate of deviation set by the auditor in respect of which the auditor seeks to obtain an appropriate

	level of assurance that the rate of deviation is not exceeded by the actual error in the population. This is also referred to as tolerable error, tolerable rate, or tolerable deviation.
Topology	The physical layout of how computers are linked together.
Transaction	A discrete event captured by a computer system, such as the entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in dollars and cents and entered in accounting records.
Transaction data	The finite data pertaining to a given event occurring in a business process. This process produces documents or postings, such as purchase orders and obligations.
Trust anchor	A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g., in a public key certificate). A trust anchor may have name or policy constraints limiting its scope.
Trust store	A repository that contains cryptographic artifacts like certificates that are used for cryptographic protocols.
Trusted communication path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. Only the user or the security functions of the information system can activate this mechanism, and it cannot be imitated by untrusted software.
Uninterruptible power supply	Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level.
Unit testing	Testing individual program modules to determine if they perform to specifications.
User	Individual or system process authorized to access an information system.

User control	Portions of controls that are performed by people interacting with information systems. A user control is an information system control if its effectiveness depends on information system processing or the reliability (completeness, accuracy, and validity) of information processed by information systems.
User identification (user ID)	Unique symbol or character string used by an information system to identify a specific user.
User-defined processing	When a user is allowed to establish or modify processing steps. This frequently occurs in application-based spreadsheets and report writer tools, and data extraction tools.
Utility program	Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing.
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.
Validity	An information processing objective that aims to provide reasonable assurance that all recorded transactions and events actually occurred, are related to the entity, and were executed according to prescribed procedures.
Virus	A program that “infects” computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the “infected” file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability scanning	Type of network security testing that enumerates the network structure and determines the set of active hosts and associated software and verifies that software (e.g., operating system and major applications) is up-to-date with security patches and software version.

Web application	An application that is accessed over a network, such as the internet or an intranet.
Workstation	A microcomputer connected to a network. Workstation can also refer to a powerful, stand-alone computer that has considerable calculating or graphics capability.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

APPENDIX 500B

FISCAM FRAMEWORK

Introduction

.01 The FISCAM Framework is intended to assist the auditor with (1) identifying relevant business process and general controls at various levels (i.e., application, system, entity, or combination thereof) and (2) evaluating the suitability of the design and operating effectiveness of these controls. It comprises the following six control categories:

- Business Process Controls. The critical elements and associated control objectives that, if satisfied, will address potential risks to information processing objectives arising from information technology are listed in table 8.
- Security Management. The critical elements and associated control objectives that, if satisfied, will address potential risks associated with the following components of internal control: control environment, risk assessment, control activities, and monitoring are listed in table 9.
- Access Controls. The critical elements and associated control objectives that, if satisfied, will address potential risks to security and privacy objectives arising from unauthorized access to information technology are listed in table 10.
- Segregation of Duties. The critical elements and associated control objectives that, if satisfied, will address potential risks to security and privacy objectives arising from unauthorized actions using information technology are listed in table 11
- Configuration Management. The critical elements and associated control objectives that, if satisfied, will address potential risks to security and privacy objectives arising from unauthorized changes to information technology are listed in table 12.
- Contingency Planning. The critical elements and associated control objectives that, if satisfied, will address potential risks to security and privacy objectives arising from unplanned interruptions to information technology are listed in table 13.

.02 This appendix presents the FISCAM Framework with illustrative control activities and audit procedures. These elements are included to provide guidance to the auditor and demonstrate the relationship between the FISCAM Framework and National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*. As discussed in section 160, this appendix is not intended to be an audit program. The auditor is responsible for (1) identifying and evaluating control activities that management designed and implemented and (2) developing appropriate audit procedures for testing those control activities that satisfy the engagement objectives.

FISCAM Framework for Business Process Controls

Table 8. FISCAM framework for business process controls.

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.01 Management designs and implements user and application control activities 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.01.01.01 Input data are derived from appropriate sources.	Obtain an understanding of the entity's processes and methods for preparing data for input through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as source documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Observe appropriate personnel as they prepare data for input and inspect any source documentation or additional support prepared. Observe any reviews of source documentation or additional support prepared. Through inquiry and inspection, obtain an understanding of the entity's processes and methods to maintain evidence of such activities for subsequent review or reference. Inspect a selection of transactions and trace selected data from the information system back to sources from which the data originated.	National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Consider whether any of the selected data have been manipulated from their original form. Determine whether input data are derived from appropriate sources.	
BP.01.01.02 Control totals are employed when practicable.	Obtain an understanding of the entity's use of control totals within the significant business processes through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of control totals to help ensure the completeness of data as they move through the process. Inspect a selection of transactions and assess the use of control totals in the processing of such transactions. Determine whether control totals are appropriately employed when practicable. Note: A control total is the sum of a numerical field contained in a set of records. Control totals are used to verify the completeness of a set of records as it is processed. Control totals are verified by comparing the control totals from a processed set of records (output) to those of the same set of records before processing (input).	NIST SP 800-53, SI-10
BP.01.01.03 Sequence checking is employed when practicable.	Obtain an understanding of the entity's use of sequence checking within the significant business processes through • inquiry of appropriate personnel;	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of sequence checking to help ensure the completeness of data as they move through the process. Observe a user attempt to subvert the sequence-checking process within the information system. Note any error messages and whether the transaction is suspended or processed. Inspect a selection of transactions and assess the use of sequence checking in the processing of such transactions. Determine whether sequence checking is appropriately employed when practicable. Note: Sequence checking is used to verify the completeness of a set of records. A numerical sequence code is used to uniquely identify records. The absence of a number within a range of sequentially numbered records indicates a missing record.	
BP.01.01.04 User-defined processing of data is appropriately controlled.	Obtain an understanding of any user-defined processing within the significant business processes through • inquiry of appropriate personnel and • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals.	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and any user-defined processing of data. Observe appropriate personnel as they perform user-defined processing of data. Observe any reviews of such processing. Through inquiry and inspection, obtain an understanding of the entity's processes and methods to maintain evidence of such activities for subsequent review or reference. Consider whether appropriate controls are in place to prevent data from being inappropriately manipulated. Consider whether management oversight of user-defined processing of data is adequate. Determine whether user-defined processing of data is appropriately controlled. Note: Some business process applications may allow user-defined processing of data, whereby the user may establish or modify information system processing activities. This frequently occurs when business process applications use spreadsheets and report-writer and data-extraction tools to support business processes involving both manual and automated processing steps.	
BP.01.01.05 Data prepared for system input are independently reviewed and approved (1) prior to entry or upload or (2) as part of the application software workflow for data entry. *Related control: BP.04.03.09*	Obtain an understanding of the entity's processes and methods for preparing data for input through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as source documentation.	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Observe appropriate personnel as they independently review data prepared for system input. Consider whether such reviews are performed (1) prior to data entry or upload or (2) as part of the application software workflow for data entry. Through inquiry and inspection, obtain an understanding of the entity's processes and methods to maintain evidence of such activities for subsequent review or reference. Inspect a selection of transactions and verify that data prepared for system input were independently reviewed and approved in accordance with relevant policies and procedures. Consider whether such reviews appropriately verified the completeness, accuracy, and validity of the input data. Determine whether data prepared for system input are independently reviewed and properly approved (1) prior to entry or upload or (2) as part of the application software workflow for data entry.	
BP.01.02 Data validation rules detect erroneous data values before information system processing.		
BP.01.02.01 The system validates that input data match specified definitions for format and content, such as character set, length, numerical range, and acceptable values, and will not accept data that do not satisfy these definitions. *Related controls: BP.01.02.03, BP.02.01.01, BP.04.03.10, BP.04.05.01, and BP.06.03.04*.	Obtain an understanding of the entity's use of data validation controls within the significant business processes through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation.	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of data validation controls to help ensure the accuracy and validity of data as they move through the process. Identify key data input screens or other key system entry points for input data. Observe appropriate personnel as they input data into the system, noting any input data validation errors. Observe a user attempt to subvert the data validation controls to prevent duplicate entries. Note any error messages and whether the transaction is suspended or processed. Inspect system design documentation and applicable system configuration files to assess the design of key data validation controls, including the specified definitions for data format and content. Determine whether relevant information systems appropriately validate that input data match specified definitions for data format and content and will not accept data that do not satisfy these definitions. Note: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the entity specifies that numerical values from 1 to 100 are the only acceptable inputs for a field in a given application, inputs of “387,” “abc,” or “%K%” are invalid inputs and are not accepted as input to the system.	
BP.01.02.02 The system validates that input data have not been entered, uploaded, or accepted in duplicate. *Related control: BP.01.02.03*	Obtain an understanding of the entity’s use of data validation controls within the significant business processes through • inquiry of appropriate personnel;	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of data validation controls to help ensure the accuracy and validity of data as they move through the process. Identify key data input screens or other key system entry points for input data. Observe appropriate personnel as they input data into the system, noting any input data validation errors. Observe a user attempt to subvert the data validation controls to prevent duplicate entries. Note any error messages and whether the transaction is suspended or processed. Inspect system design documentation and applicable system configuration files to assess the design of key data validation controls, including the specified definitions for data format and content. Determine whether relevant information systems appropriately validate that input data have not been entered, uploaded, or accepted in duplicate.	
BP.01.02.03 The system generates error messages, posts log entries, or combinations thereof when input data are not accepted. *Related controls: BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.02.02, and AC.05.02.03*	Obtain an understanding of the entity's use of error messages and event logging within the significant business processes through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and	NIST SP 800-53, AU-2 NIST SP 800-53, AU-12 NIST SP 800-53, SI-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process; the format and content of inputs and outputs involved; and the use of error messages, event logging, or combinations thereof to facilitate error resolution. Observe appropriate personnel as they input data into the system, noting any input data validation errors. Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems and information system resources. Inspect audit records for the event types selected for logging that are applicable to relevant information systems and information system resources. Consider the completeness and accuracy of the documentation obtained, including any reports produced using log management software and reviewed by entity management. Determine whether relevant information systems appropriately generate error messages, post log entries, or combinations thereof when input data are not accepted.	
BP.01.02.04 Rejected input data are held in suspense and identified on error reports until the errors are researched and resolved.	Obtain an understanding of the entity's processes and methods for holding rejected input data in suspense until errors are resolved through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and	NIST SP 800-53, AU-2 NIST SP 800-53, SI-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of other relevant documentation, such as error or suspense reports. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Observe a user attempt to perform an action that would cause input data to be rejected and held in suspense. Consider whether the input data are appropriately held in suspense and identified on an error or suspense report for subsequent review. Determine whether rejected input data are held in suspense and identified on error reports until the errors are researched and appropriately resolved.	
BP.01.03 Input data validation errors are researched and resolved on a timely basis.		
BP.01.03.01 Input data validation errors are researched to identify and remediate the cause(s) of the errors.	Obtain an understanding of the entity's processes and methods for researching and remediating input data validation errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as error or suspense reports. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect a selection of error or suspense reports and consider whether input data validation errors and rejected input data are being researched and resolved on a timely basis. Additionally, consider whether management properly identifies the cause(s) of the errors. Follow-up on any unresolved items identified. Determine whether input data validation errors are appropriately researched to properly identify and remediate the cause(s) of the errors.	
BP.01.03.02 Input data validation errors are resolved through the entry or upload of corrected input data.	Obtain an understanding of the entity's processes and methods for resolving input data validation errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as documentation for error resolution. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Inspect a selection of error or suspense reports and consider whether input data validation errors and rejected input data are being resolved through the entry or upload of corrected input data. Determine whether input data validation errors are appropriately resolved through the entry or upload of corrected input data.	NIST SP 800-53, SI-10
BP.01.03.03 Manual overrides of input data validation errors are (1) used only in limited circumstances that are defined and	Obtain an understanding of the entity's processes and methods for manually overriding input data validation errors through • inquiry of appropriate personnel;	NIST SP 800-53, AU-2 NIST SP 800-53, AU-6 NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
documented, (2) restricted to authorized personnel, and (3) logged and monitored. *Related controls: BP.02.02.03 and BP.03.03.03*	• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as documentation for error resolution. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Inspect a selection of error or suspense reports and consider whether manual overrides of input data validation errors were performed to resolve any of the errors identified. If a log of manual overrides exists, inspect the log to validate that manual overrides are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. Determine whether manual overrides of information system input data validation errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. Note: The use of manual overrides does not on its own indicate that controls are inadequate. However, the auditor needs to examine why manual overrides are being used and whether adequate controls are in place to minimize risks from such actions.	
BP.02 Management designs and implements user and application control activities 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.02.01.01 The system validates that in-process data match definitions for format and	Obtain an understanding of the entity's use of data validation controls within the significant business processes through	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
content, such as character set, length, numerical range, and acceptable values, and will not continue processing data that do not satisfy these definitions. *Related controls: BP.01.02.01, BP.04.03.10, BP.04.05.02, and BP.06.03.04*	• inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of data validation controls to help ensure the accuracy and validity of data as they move through the process. Identify key interfaces or other key system entry points for in-process data. Inspect system design documentation and applicable system configuration files to assess the design of key data validation controls, including the specified definitions for data format and content. Determine whether relevant information systems appropriately validate that in-process data match specified definitions for data format and content and will not continue processing data that do not satisfy these definitions.	
BP.02.01.02 The system logs data processing events to permit management oversight of business processes that the system performs. *Related controls: BP.01.02.03, BP.02.01.05, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.02.02, and AC.05.02.03*	Obtain an understanding of the entity's use of event logging within the significant business processes through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation.	NIST SP 800-53, AU-2 NIST SP 800-53, AU-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See BP.04.02.01 for factors to consider in o assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of event logging to permit management oversight of business processes that the information system performs. Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems and information system resources. Inspect audit records for the event types selected for logging that are applicable to relevant information systems and information system resources. Consider the completeness and accuracy of the documentation obtained, including any reports produced using log management software and reviewed by entity management. Determine whether relevant information systems appropriately log data processing events to permit management oversight of business processes that the information system performs.	
BP.02.01.03 Management reviews system data processing logs on a timely basis.	Obtain an understanding of the entity's processes and methods for reviewing information system data processing logs through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as information system data processing logs. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant	NIST SP 800-53, AU-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	business process, the format and content of inputs and outputs involved, and management's use of information system data processing logs. Inspect a selection of information system data processing logs and consider whether any unusual or unauthorized activity identified on the logs was properly investigated and resolved on a timely basis. Through inquiry and inspection, obtain an understanding of the entity's processes and methods to maintain evidence of such activities for subsequent review or reference. Determine whether management reviews information system data processing logs relevant to the significant business processes on a timely basis.	
BP.02.01.04 The system performs reconciliations to identify potential data processing errors.	Obtain an understanding of the entity's use of automated reconciliations within the significant business processes through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of automated reconciliations to facilitate error identification and resolution. Determine whether relevant information systems perform appropriate reconciliations to identify potential data processing errors.	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.02.01.05 The system generates an error message, posts a log entry when data processing errors occur, or both. *Related controls: BP.01.02.03, BP.02.01.02, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.02.02, and AC.05.02.03*	Obtain an understanding of the entity's use of error messages and event logging within the significant business processes through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as system design documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process; the format and content of inputs and outputs involved; as well as the use of error messages, event logging, or combinations thereof to facilitate error resolution. Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems and information system resources. Inspect audit records for the event types selected for logging that are applicable to relevant information systems and information system resources. Consider the completeness and accuracy of the documentation obtained, including any reports produced using log management software and reviewed by entity management. Determine whether relevant information systems appropriately generate an error message, post a log entry, or combinations thereof when data processing errors occur.	NIST SP 800-53, AU-2 NIST SP 800-53, AU-12 NIST SP 800-53, SI-11
BP.02.01.06 Data affected by processing errors are held in suspense and identified on error reports until the errors are researched and resolved.	Obtain an understanding of the entity's processes and methods for holding data affected by processing errors in suspense until errors are resolved through	NIST SP 800-53, AU-2 NIST SP 800-53, SI-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as error or suspense reports. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing. Inspect a selection of error or suspense reports and consider whether data processing errors are identified. Determine whether data affected by processing errors are held in suspense and identified on error reports until the errors are researched and appropriately resolved.	
BP.02.02 Data processing errors are researched and resolved on a timely basis.		
BP.02.02.01 Data processing errors are researched to identify and remediate the cause(s) of the errors.	Obtain an understanding of the entity's processes and methods for researching and remediating data processing errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as error or suspense reports. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	business process, the format and content of inputs and outputs involved, and controls over data processing. Inspect a selection of error or suspense reports and consider whether data processing errors are being researched and resolved on a timely basis. Additionally, consider whether management properly identifies the cause(s) of the errors. Follow-up on any unresolved items identified. Determine whether data processing errors are appropriately researched to properly identify and remediate the cause(s) of the errors.	
BP.02.02.02 Data processing errors are resolved by correcting data, coding errors in computer programs, or a combination thereof.	Obtain an understanding of the entity's processes and methods for resolving data processing errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as documentation for error resolution. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing. Inspect a selection of error or suspense reports and consider whether data processing errors are being resolved on a timely basis through the correction of data, the correction of coding errors in computer programs, or a combination of such actions.	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether data processing errors are appropriately resolved by correcting data, correcting coding errors in computer programs, or a combination thereof.	
BP.02.02.03 Manual overrides of data processing errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. *Related controls: BP.01.03.03 and BP.03.03.03*	Obtain an understanding of the entity's processes and methods for performing manual overrides of data processing errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as documentation for error resolution. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Inspect a selection of error or suspense reports and consider whether manual overrides of data processing errors were performed to resolve any of the errors identified. If a log of manual overrides exists, inspect the log to validate that manual overrides are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. Determine whether manual overrides of information system data processing errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. Note: The use of manual overrides does not on its own indicate that controls are inadequate. However, the auditor needs to examine why manual overrides are being used and whether adequate controls are in place to minimize risks from such actions.	NIST SP 800-53, AU-2 NIST SP 800-53, AU-6 NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.03 Management designs and implements user and application control activities to reasonably assure that output data are complete, accurate, and valid.		
BP.03.01 Data are approved for output.		
BP.03.01.01 The format and content of output data are aligned with management's definitions. *Related controls: BP.04.03.11 and BP.04.05.03*	Obtain an understanding of the entity's processes and methods for preparing data for output through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such outputs involved in the significant business processes. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and management's definitions for the format and content of output data as well as its distribution. Observe appropriate personnel as they prepare data for output. Through inquiry and inspection, obtain an understanding of the entity's processes and methods to verify that the format and content of output data are aligned with management's definitions. Determine whether the format and content of output data are aligned with management's definitions. Note: Output data may include data files and system-generated reports.	NIST SP 800-53, SI-12 NIST SP 800-53, SI-15
BP.03.02 Output data errors are identified on a timely basis.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.03.02.01 Summarized output data included in reports are reviewed and reconciled to appropriate source data on a timely basis.	Obtain an understanding of the entity's processes and methods to review and reconcile summarized output data included in reports to appropriate source data through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and management's definitions for the format and content of output data as well as its distribution. Inspect available documentation for a selection of reconciliations performed during the audit period. Consider whether such reconciliations were appropriate and performed in accordance with the entity's policies and procedures for timely reviewing and reconciling summarized output data to appropriate source data. Determine whether summarized output data included in reports are reviewed and reconciled to appropriate source data on timely basis.	NIST SP 800-53, SI-12 NIST SP 800-53, SI-15
BP.03.03 Output data errors are researched and resolved on a timely basis.		
BP.03.03.01 Output data errors are researched to identify and remediate the cause(s) of the errors.	Obtain an understanding of the entity's processes and methods for researching and remediating output data errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and	NIST SP 800-53, SI-12 NIST SP 800-53, SI-15

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of other relevant documentation, such as error or suspense reports. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing. Inspect a selection of error or suspense reports and consider whether output data errors are being researched and resolved on a timely basis. Additionally, consider whether management properly identifies the cause(s) of the errors. Follow-up on any unresolved items identified. Determine whether output data errors are researched to identify and remediate the cause(s) of the errors.	
BP.03.03.02 Output data errors are resolved by correcting data, correcting coding errors in computer programs, or a combination thereof.	Obtain an understanding of the entity's processes and methods for resolving output data errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as documentation for error resolution. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing. Inspect a selection of error or suspense reports and consider whether output data errors are being resolved through the correction of data,	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	the correction of coding errors in computer programs, or a combination of such actions. Determine whether output data errors are appropriately resolved by correcting data, correcting coding errors in computer programs, or a combination thereof.	
BP.03.03.03 Manual overrides of output data errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. *Related controls: BP.01.03.03 and BP.02.02.03*	Obtain an understanding of the entity's processes and methods for performing manual overrides of output data errors through • inquiry of appropriate personnel; • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and • inspection of other relevant documentation, such as documentation for error resolution. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data. Inspect a selection of error or suspense reports and consider whether manual overrides of output data errors were performed to resolve any of the errors identified. If a log of manual overrides exists, inspect the log to validate that manual overrides are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored. Determine whether manual overrides of information system output data errors are (1) used only in limited circumstances that are defined and documented; (2) restricted to authorized personnel; and (3) logged and monitored. Note: The use of manual overrides does not on its own indicate that controls are inadequate. However, the auditor needs to examine why	NIST SP 800-53, AU-2 NIST SP 800-53, AU-6 NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	manual overrides are being used and whether adequate controls are in place to minimize risks from such actions.	
BP.04 Management designs and implements general control activities to reasonably assure that business process applications are properly managed to support the achievement of information processing objectives.		
BP.04.01 Business process application roles and responsibilities are defined and assigned to appropriate personnel.		
BP.04.01.01 Business process application ownership is appropriately assigned. *Related controls: SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.05.01.01, and BP.06.01.01*	Obtain an understanding of business process application roles and responsibilities, including business process application and information system ownership, through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system security and privacy plans. Identify the business process application owners for the information systems relevant to the significant business processes. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities. Determine whether business process application and information system ownership has been appropriately assigned. Note: Business process application ownership means the overall responsibility and accountability for management of the business process application, including ensuring that the business process application is properly designed to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information. Thus, any changes to the design of the business process application, modifications to functionality of the business process application through changes to application software or changes to configurable controls within application software, or changes to corresponding access controls generally require the approval of the business process application owner or an authorized delegate of the owner. Depending	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	on the entity's organizational structure and how management has assigned responsibilities and delegated authorities, business process application owner and information system owner responsibilities may be combined within the information system owner or program manager role. Large or complex information systems supporting multiple mission and business functions may have multiple business process application owners who support the system owner. The information system owner is the official responsible for the overall procurement, development, integration, modification, operation, and maintenance of a system.	
BP.04.01.02 Business process application responsibilities are appropriately assigned to information resource owners, users, and security administrators, as well as appropriate authorizing officials. *Related controls: SD.01.01.01, SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.05.01.02, BP.06.01.02, BP.06.01.03, BP.06.01.04, and BP.06.01.05*	Obtain an understanding of the business process application responsibilities for information resource owners, users, and security administrators, as well as appropriate authorizing officials, through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system security and privacy plans. Identify the information resource owners, users, and security administrators, as well as appropriate authorizing officials, for the information systems relevant to the significant business processes. Consider whether they possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Determine whether business process application responsibilities have been clearly defined and appropriately assigned to information resource owners, users, and security administrators, as well as appropriate authorizing officials. Note: Senior management officials are assigned as authorizing officials for information systems and common controls that organizational systems may inherit. Business process applications may be separately authorized or included within a larger information system boundary. An information system boundary comprises all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems	NIST SP 800-53, AC-22 NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	to which the information system is connected. As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.	
BP.04.02 Policies and procedures for administering and using business process applications are developed and implemented.		
BP.04.02.01 Policies and procedures applied at the system and business process levels for administering and using business process applications are developed, documented, approved, and periodically reviewed and updated. Such policies and procedures appropriately • consider risk; • address data management, including data validation and error resolution, in accordance with the entity's data strategy or applicable guidelines established by the entity's data governance body, data integrity board, or management; • address changes to business process application functionality through modifications to application software or changes to configurable controls within application software; • address purpose, scope, roles, responsibilities, coordination among business or organizational units and	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures for administering and using business process applications through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Through inquiry, inspection, and observation, identify information system controls relevant to the significant business processes and areas of audit interest. Throughout the engagement, determine whether the entity's policies and procedures for the application of information system controls are designed, implemented, and operating effectively. Consider whether • policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external entities, and compliance; • procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be held accountable for their actions; and appropriately consider information system general and application controls, as well as segregation of duties controls; and	NIST SP 800-53, AC-1 NIST SP 800-53, AT-1 NIST SP 800-53, AU-1 NIST SP 800-53, CA-1 NIST SP 800-53, CM-1 NIST SP 800-53, CP-1 NIST SP 800-53, IA-1 NIST SP 800-53, IR-1 NIST SP 800-53, MA-1 NIST SP 800-53, MP-1 NIST SP 800-53, PE-1 NIST SP 800-53, PL-1 NIST SP 800-53, PM-1 NIST SP 800-53, PS-1 NIST SP 800-53, PT-1 NIST SP 800-53, RA-1 NIST SP 800-53, SA-1 NIST SP 800-53, SC-1 NIST SP 800-53, SI-1

Illustrative control activities	Illustrative audit procedures	Relevant criteria
with external entities, and compliance; • identify and describe the relevant processes; • consider information system general and application controls; • consider segregation of duties controls; and • help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities.	• policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity's internal control objectives. Throughout the engagement, determine whether the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures are designed, implemented, and operating effectively. Note: Audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its system-level and business process-level policies and procedures are intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of information system controls relevant to the significant business processes and the business process applications and information systems that support them. When effectively designed, the entity's policies and procedures for administering and using business process applications, as well as policies and procedures applicable to the significant business processes, provide suitable criteria for evaluating evidence regarding the implementation and operating effectiveness of information system controls.	NIST SP 800-53, SR-1
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, as well as the confidentiality, integrity, and availability of information.		
BP.04.03.01 Business process application characteristics are defined, implemented, and documented with consideration for information security.	Perform walk-throughs of the significant business processes. Consider whether the automated business processes and corresponding information system general and application controls observed in walk-throughs of the significant business processes are consistent with those documented in system documentation and align with prescribed information protection requirements for the business process applications and information systems.	NIST SP 800-53, CM-12 NIST SP 800-53, PM-11 NIST SP 800-53, PM-32 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5 NIST SP 800-53, SA-8 NIST SP 800-53, SC-27

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Determine whether business process application characteristics are appropriately defined, implemented, and documented to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information. Note: Entities are required to define business processes with consideration for information security and determine the information protection requirements arising from the defined business processes. Business process applications supporting critical or essential mission and business functions may be designed as platform independent to support the ability to reconstitute on different platforms in the event of a system disruption. Additionally, business process applications may be designed to use alternative sources of information to carry out essential functions or services when the primary source of information is corrupted or unavailable. Business process applications and information systems are designed to support specific mission or business functions. Business process application design documentation is maintained to support the entity's authorization process, as well as to facilitate configuration management. Business process application characteristics include the application boundary, application modules and how they interact with one another, and data conventions. Business process application characteristics also include the automated business processes or subprocesses that the application performs, including any system accounts associated with the performance of such processes. Application module interaction may be depicted in call graphs, data flow diagrams, and control flow diagrams. A data dictionary or data	NIST SP 800-53, SI-22

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	inventory may provide useful information about application data, including data names, descriptions, creators, owners, and usage. However, over time, information systems and information system components may be used to support services that are outside of the scope of the intended mission or business functions. As such, the entity periodically reviews the services that the information system supports to help ensure that they are in line with the defined business process application characteristics.	
BP.04.03.02 Business processes are standardized and automated when practicable.	Perform walk-throughs of the significant business processes. Consider the extent to which such business processes are standardized and automated. Consider whether further standardization or automation would reduce control risk. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Determine whether the significant business processes are standardized and automated as practicable.	NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5
BP.04.03.03 Automated business processes and corresponding application controls are designed to help ensure that transactions are complete, accurate, and valid.	Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to help ensure that transactions are complete, accurate, and valid. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business	NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	processes and corresponding application controls. Consider whether the associated general controls are effective. Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that transactions are complete, accurate, and valid. Note: When suitably designed and properly implemented, automated business processes and corresponding application controls provide reasonable assurance that only valid management-approved transactions are input into the application, accepted for processing, processed once and only once by the application, accurately recorded on a timely basis, and properly included in output files or reports.	
BP.04.03.04 Automated business processes and corresponding application controls are designed to help ensure that master and transaction data records maintained in data management systems are complete, accurate, and valid.	Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to help ensure that master and transaction data records maintained in the applicable data management systems are complete, accurate, and valid. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective. Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that master and transaction data	NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	records maintained in data management systems are complete, accurate, and valid. Note: Automated business processes and corresponding application controls (e.g., duplicate checks and system warnings) are often configured into the business process application to prevent or identify potential duplicate master data records as well as to detect data anomalies.	
BP.04.03.05 Automated business processes and corresponding application controls are designed to help ensure that transaction data are in balance across business process application modules.	Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to help ensure that transaction data are in balance across business process application modules. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective. Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that transaction data are in balance across business process application modules. Note: For general ledger systems, automated business processes and corresponding application controls are designed to help ensure that data from subsidiary ledgers are in balance with the general ledger.	NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5
BP.04.03.06 Automated business processes and corresponding application controls are	Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding	NIST SP 800-53, PM-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
designed to help ensure that master data are consistent between business process application modules and among other information systems using the same master data.	application controls are designed to help ensure that master data are consistent between business process application modules and among other information systems using the same master data. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective. Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that master data are consistent between business process application modules and among other information systems using the same master data.	NIST SP 800-53, SA-4 NIST SP 800-53, SA-5
BP.04.03.07 Access controls are incorporated into the design of automated business processes and corresponding application controls to prevent users from executing incompatible transactions within the business process application through menus, screens, or other user interfaces. *Related controls: SD.01.01.01, SD.01.02.01, SD.01.02.02, and SD.01.03.01*	Perform walk-throughs of the significant business processes. Consider whether access controls are incorporated into the design of automated business processes and corresponding application controls to prevent users from executing incompatible transactions. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Determine whether access controls are incorporated into the design of automated business processes and corresponding application controls to prevent users from executing incompatible transactions within the	NIST SP 800-53, AC-5 NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	business process application through menus, screens, or other user interfaces.	
BP.04.03.08 Transaction processing roles are aligned with management's authorizations for users and processes acting on behalf of users. *Related control: BP.04.06.02* *Related control objective: AC.02.03*	Perform walk-throughs of significant business processes. Consider whether transaction processing roles are appropriately aligned with management's authorizations for users and processes acting on behalf of users. Inspect system design documentation, system security and privacy plans, role and permission matrices, and policies and procedures demonstrating the design of transaction processing roles and criteria for role membership. Inspect a system-generated list of accounts for each of the business process applications and information systems relevant to the significant business processes. Consider the transaction processing roles assigned to each account and whether such assignments are appropriate based on the purpose of the account, the type of account, and the users or processes to which the account is assigned. Determine whether transaction processing roles are aligned with management's authorizations for users and processes acting on behalf of users.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6
BP.04.03.09 Approval workflows within the business process application are aligned with management's authorizations for users and appropriately controlled. *Related controls: BP.01.01.05 and BP.04.06.02*	Obtain an understanding of the entity's processes and methods to control approval workflows. Consider whether such processes and methods adequately address access restrictions for workflow development or modification. Inspect system design documentation, system security and privacy plans, role and permission matrices, approval workflow diagrams, and policies and procedures demonstrating the design of approval workflows and the account roles or permissions associated with each processing step or approval included in the workflows. Perform walk-throughs of the significant business processes. Consider whether approval workflows within the business process application	NIST SP 800-53, AC-2 NIST SP 800-53, AC-5 NIST SP 800-53, AC-6 NIST SP 800-53, CM-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	prevent unauthorized users from approving transactions and enforce appropriate segregation of duties. Determine whether approval workflows within the business process application are aligned with management's authorizations for users and appropriately controlled.	
BP.04.03.10 Parameters and tolerances for data input, processing, and output, as well as error conditions and messages, are defined, implemented, and documented. *Related controls: BP.01.02.01, BP.02.01.01, BP.04.05.01, BP.04.05.02, BP.04.05.03, and BP.06.03.04*	Inspect system design documentation, system security and privacy plans, applicable system configuration files, and policies and procedures demonstrating the defined parameters and tolerances for data input, processing, and output, as well as error conditions and messages. Consider whether parameters and tolerances for data input, processing, and output are appropriately defined, implemented, and documented. Consider whether the parameters and tolerances that management identified are appropriate. Determine whether parameters and tolerances for data input, processing, and output, as well as error conditions and messages, are defined, implemented, and documented to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information. Note: Data input, processing, and output parameters and tolerances can be configured based on limits on transaction amounts or based on the nature of transactions. Such parameters and tolerances are aligned with management's definitions for data format and content.	NIST SP 800-53, SI-10 NIST SP 800-53, SI-11 NIST SP 800-53, SI-12 NIST SP 800-53, SI-15
BP.04.03.11 Management defines the format and content of output data and their distribution based on end user needs and in accordance with applicable guidelines that the entity's data governance body established to maintain and use data in accordance with applicable statutes, regulations, executive orders, implementing entity guidance,	Perform a walk-through of significant business processes. Consider whether management appropriately defines the format and content of output data and their distribution based on end user needs. Consider whether management's definitions are in accordance with the entity's data governance body and applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.	NIST SP 800-53, SI-12 NIST SP 800-53, SI-15

Illustrative control activities	Illustrative audit procedures	Relevant criteria
directives, and other specific criteria relevant to data governance. *Related controls: BP.03.01.01 and BP.04.05.03*	Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the format and content of output data and their distribution. Determine whether the format and content of output data and their distribution are based on end user needs and in accordance with applicable guidelines that the entity's data governance body established for maintaining and using data in accordance with applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance. Note: Entity management may have procedures in place to monitor the replication of output data within or outside the entity.	
BP.04.03.12 Management establishes, documents, and periodically reviews and updates user training that focuses on the correct use of the business process application. This includes the operation of information processing, information security, and privacy controls. Management monitors the completion status of applicable mandatory training courses for information system users. *Related controls: SM.02.03.01, SM.02.03.02, and SM.02.03.03*	Obtain an understanding of the entity's processes and methods for establishing, documenting, and periodically reviewing and updating training on the correct use of the business process applications and information systems relevant to the significant business processes through • inquiry of appropriate personnel, including any senior officials responsible for the training, and • inspection of relevant documentation, such as training course materials. Consider whether • training course materials have been recently reviewed and updated, as appropriate; • mandatory training courses are identified and communicated to information system users as a condition for system access, as applicable; and • management adequately monitors the completion status of applicable mandatory training courses for information system users.	NIST SP 800-53, AT-3 NIST SP 800-53, AT-4 NIST SP 800-53, SA-16

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether management has established, documented, maintained, and monitored user training that focuses on the correct use of the business process application. Note: System developers are required to provide training on the correct use and operation of information systems, including the operation of information processing, information security, and privacy controls. Developer-provided training applies to external and internal (in-house) developers. Training personnel contributes to ensuring the effectiveness of the controls implemented within business process applications and information systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Entities can also request training materials from developers to conduct in-house training or offer self-training to entity personnel. Entities determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.	
BP.04.04 Business process applications are designed to facilitate the protection of personally identifiable information.		
BP.04.04.01 Business process application characteristics are defined, implemented, and documented with consideration for privacy.	Perform walk-throughs of the significant business processes. Consider whether the automated business processes and corresponding information system general and application controls observed in walk-throughs of the significant business processes are consistent with those documented in system documentation and align with prescribed personally identifiable information processing needs for the business process applications and information systems. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Determine whether business process application characteristics are defined, implemented, and documented with appropriate consideration for privacy.	NIST SP 800-53, PM-11 NIST SP 800-53, PT-6 NIST SP 800-53, PT-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Entities are required to define business processes with consideration for privacy and determine the personally identifiable information processing needs arising from the defined business processes. The Privacy Act of 1974 (codified, as amended, at 5 U.S.C. § 552a) (PRIVACT) requires that each federal agency publish a system of records notice in the *Federal Register* when they establish or modify a PRIVACT system of records. Under PRIVACT, a system of records is statutorily defined as a group of any records under the control of the agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other individual identifier. Pursuant to PRIVACT and implementing Office of Management and Budget guidance, the notice describes the existence and character of the system and identifies the system of records, the purpose of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in Office of Management and Budget (OMB) Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. Additionally, PRIVACT and implementing guidance establish requirements for federal and nonfederal agencies if they engage in a matching program. In general, a matching program is a computerized comparison of (1) two or more automated PRIVACT systems of records or (2) an automated PRIVACT system of records with automated nonfederal records that a nonfederal agency (or agent thereof) maintains. A PRIVACT matching program pertains either to federal benefit programs or to federal personnel or payroll records. A federal benefit match is performed to determine or verify eligibility for payments under federal benefit programs or to recoup payments or delinquent debts under federal benefit programs. A PRIVACT matching program involves not just the matching activity itself but also the investigative follow-up and ultimate action, if any.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.04.04.02 Automated business processes and corresponding application controls are designed to provide notice to information system users about the processing of personally identifiable information. When appropriate the processes and controls also allow information systems users to consent to the processing of their personally identifiable information.	Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to provide notice to information system users about the processing of personally identifiable information and, when appropriate, allow information system users to consent to the processing of their personally identifiable information. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Confirm whether the associated general controls are effective. Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that notice is provided to information system users about the processing of personally identifiable information and, when appropriate, information system users to consent to the processing of their personally identifiable information. Note: When suitably designed and properly implemented, automated business processes and corresponding application controls provide reasonable assurance that notice is provided to information system users about the processing of personally identifiable information and, when appropriate, information system users to consent to the processing of their personally identifiable information.	NIST SP 800-53, PT-4 NIST SP 800-53, PT-5
BP.04.04.03 Automated business process and corresponding application controls are designed to apply processing conditions for	Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to apply processing conditions for specific categories of personally identifiable information based on risk.	NIST SP 800-53, PT-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
specific categories of personally identifiable information based on risk.	Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Confirm whether the associated general controls are effective. Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that processing conditions for specific categories of personally identifiable information are based on risk. Note: Entities apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, or guidelines. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any particular requirements that apply.	
BP.04.04.04 Management develops, documents, and periodically reviews and updates a map of system data actions that process personally identifiable information.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating a map of system data actions that process personally identifiable information through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the map of system data actions for each of the business process applications and information systems. Consider whether the map of system data actions identifies • discrete data actions,	NIST SP 800-53, CM-13

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• elements of personally identifiable information being processed in the data actions, • system components involved in the data actions, and • the owners or operators of those system components. Determine whether a map of system data actions has been appropriately documented, periodically reviewed and updated, and properly approved for each of the business process applications and information systems relevant to the significant business processes. Note: Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. Understanding what personally identifiable information is being processed (e.g., the sensitivity of the personally identifiable information), how personally identifiable information is being processed (e.g., if the data action is visible to the individual or is processed in another part of the system), and by whom (e.g., individuals may have different privacy perceptions based on the entity that is processing the personally identifiable information) provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system. Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the entity is using. Developing this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system.	
BP.04.05 The effectiveness of business process application controls and the adequacy of automated business processes that business process applications perform are periodically assessed.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.04.05.01 Management periodically reviews implemented configuration settings, parameters, and tolerances for input data validations against specified definitions for input data format and content. *Related control: BP.01.02.01*	Obtain an understanding of the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for input data validations through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings, parameters, and tolerances for input data validations during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures. Inspect implemented configuration settings, parameters, and tolerances for input data validations to independently assess whether such are consistent with management's specified definitions for input data. Determine whether the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for input data validations are designed, implemented, and operating effectively.	NIST SP 800-53, CA-2 NIST SP 800-53, CM-6
BP.04.05.02 Management periodically reviews implemented configuration settings, parameters, and tolerances for data processing events and related logging against specified definitions for in-process data format and content. *Related control: BP.02.01.01*	Obtain an understanding of the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for input data validations through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings,	NIST SP 800-53, CA-2 NIST SP 800-53, CM-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	parameters, and tolerances for in-process data validations during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures. Inspect implemented configuration settings, parameters, and tolerances for in-process data validations to independently assess whether such are consistent with management's specified definitions for in-process data. Determine whether the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for in-process data validations are designed, implemented, and operating effectively.	
BP.04.05.03 Management periodically reviews implemented configuration settings and parameters for output data against specified definitions for output. *Related controls: BP.03.01.01 and BP.04.03.11*	Obtain an understanding of the entity's processes and methods for periodically reviewing implemented configuration settings and parameters for output data through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings and parameters for output data during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures. Inspect implemented configuration settings and parameters for output data to independently assess whether such are consistent with management's specified definitions for output. Determine whether the entity's processes and methods for periodically reviewing implemented configuration settings and parameters for output data are designed, implemented, and operating effectively.	NIST SP 800-53, CA-2 NIST SP 800-53, CM-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.04.05.04 Management periodically determines whether business processes, as well as related logging, that the business process application performs are functioning as intended. It does so through a combination of observing and inspecting output data and manually reperforming automated business processes on a subset of authoritative source data, including approved input data.	Obtain an understanding of the entity's processes and methods for periodically reviewing the adequacy of automated business processes and related logging through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed the adequacy of automated business processes and related logging during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures. Determine whether the entity's processes and methods for periodically reviewing the adequacy of automated business processes and related logging are designed, implemented, and operating effectively.	NIST SP 800-53, CA-2
BP.04.06 Access to business process applications is appropriately controlled.		
BP.04.06.01 Business process application roles and corresponding access privileges are authorized and assigned to users with a valid business purpose (least privilege). *Related control: BP.06.05.01* *Related control objective: AC.02.03*	Inspect a system-generated list of accounts for each of the business process applications and information systems relevant to the significant business processes. Consider the transaction processing roles assigned to each account and whether such assignments are appropriate based on the purpose of the account, the type of account, and the users or processes to which the account is assigned. Determine whether business process application roles and corresponding access privileges are appropriately authorized and assigned to users with a valid business purpose (least privilege). Note: The access privileges authorized and assigned to user accounts are aligned with the transaction processing and approval responsibilities delegated to users and are consistent with	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	management's design of data input, processing, and output procedures.	
BP.04.06.02 The execution of sensitive transactions and the approval of transactions initiated by other users are appropriately controlled. *Related controls: BP.04.03.08, BP.04.03.09, and SD.01.01.01*	Perform walk-throughs of the significant business processes. Obtain an understanding of any sensitive transactions, as well as the processes and methods by which transactions are initiated, recorded, processed, and reported through the use of the business process applications and information systems relevant to the significant business processes. Observe the execution of sensitive transactions. Consider whether the users involved in this process are appropriately authorized to perform such actions. Observe the approval of transactions and inspect any documentary evidence related to such approvals. Consider whether the users involved approving transactions that others initiated are appropriately authorized to perform such actions. Determine whether the execution of sensitive transactions and the approval of transactions initiated by other users are appropriately controlled. Note: Only users authorized to execute sensitive transactions or approve transactions that others initiated are able to access such transactions or functions within the business process application through menus, screens, or other user interfaces.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-5 NIST SP 800-53, AC-6
BP.04.06.03 System accounts are identified for each automated business process or subprocess, and appropriate access privileges are authorized and assigned to such accounts. *Related control objective: AC.02.03*	Through inquiry, inspection, and observation, identify the system accounts for each automated business process or subprocess involved in the significant business processes. Inspect system design documentation, system security and privacy plans, role and permission matrices, and policies and procedures demonstrating the design of transaction processing roles and criteria for role membership. Inspect a system-generated list of accounts for each of the business process applications and information systems relevant to the	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	significant business processes. Consider the transaction processing roles assigned to each account and whether such assignments are appropriate based on the purpose of the account, the type of account, and the users or processes to which the account is assigned. Determine whether system accounts are identified for each automated business process or subprocess and whether appropriate access privileges are appropriately authorized and assigned to such accounts.	
BP.04.06.04 Output data, including reports that business process applications generate, are appropriately restricted to authorized users and other individuals for authorized purposes.	Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identity key output data, including key reports generated by the business process applications and information systems relevant to the significant business processes. Obtain an understanding of the entity's processes and methods to extract key output data and generate key reports relevant to the significant business processes. Consider whether such processes and methods adequately address access restrictions for such output data and reports. Consider whether the users involved in the processes are appropriately authorized to perform such actions. Determine whether key output data, including key reports generated by the business process applications and information systems relevant to the significant business processes, are appropriately restricted to authorized users and other individuals for authorized purposes. Note: User access to output data is aligned with the user's role and the sensitivity of information. User access to reports is aligned with authorization, including the appropriate level of security clearance, where applicable.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6 NIST SP 800-53, SI-12 NIST SP 800-53, SI-15
BP.04.06.05 The business process application logs events associated with failed user attempts to perform unauthorized data input, processing, or output procedures.	Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identity key event types for logging associated with the entity's procedures for data input, processing, and output. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the	NIST SP 800-53, AU-2 NIST SP 800-53, AU-3 NIST SP 800-53, AU-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.05.04.05, BP.06.05.03, AC.05.02.02, and AC.05.02.03	entity's processes and methods for logging and monitoring events at the business process level. Determine whether the business process applications relevant to the significant business processes properly log events associated with failed user attempts to perform unauthorized data input, processing, or output procedures. Note: Logging and monitoring controls are implemented at the business process level to help ensure that incidents are identified, analyzed, and resolved in an appropriate and timely manner based on risk. Logical and physical access controls are designed to enforce management's authorizations for users. Users' attempts to bypass such controls are logged to facilitate the identification of security violations and incidents. Potential security violations are identified on a timely basis. Logging and other mechanisms may be established to notify management of potential security violations immediately as they occur. Additionally, appropriate personnel generate and review exception reports on a timely basis. Exceptions are properly analyzed, and appropriate actions are taken to respond to potential security violations based on the nature of exceptions.	
BP.04.07 Modifications to business process applications and changes to configurable controls within application software are appropriately controlled.		
BP.04.07.01 Modifications to application software are authorized, tested, and approved. *Related control objectives: CM.02.01 and CM.02.02*	Obtain an understanding of the entity's processes and methods to modify application software through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to modify application software. Consider whether such processes and methods	NIST SP 800-53, SA-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk and • reasonably assure that modifications to application software are appropriately authorized, tested, and approved. Inspect available documentation for a selection of modifications to application software that occurred during the audit period. Consider whether adequate documentation exists to support such modifications, including evidence demonstrating that the modifications were appropriately authorized, tested, and approved by management. Consider whether the individuals involved in the modifications are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized modifications to application software. Determine whether modifications to application software are authorized, tested, and approved.	
BP.04.07.02 Changes to configurable controls within application software are appropriately controlled. *Related control objectives: CM.02.01 and CM.02.02*	Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identity configurable controls within application software relevant to the significant business processes. Obtain an understanding of the entity's processes and methods to change configurable controls within application software through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to change configurable controls. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and	NIST SP 800-53, CM-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• reasonably assure that changes to configurable controls within application software are appropriately controlled. Inspect available documentation for a selection of changes to configurable controls within application software that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that the changes were properly verified and approved by management. Consider whether the individuals involved in the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to configurable controls within application software. Determine whether changes to configurable controls within application software are appropriately controlled. Note: Configurable controls are those controls that have been designed into the business process application or information system during system development. These controls address the features most commonly associated with options available to guide end users through their assigned tasks. Approval workflows, acceptable values, and thresholds are examples of configurable controls. For example, configurable controls may be established to validate that commitments do not exceed obligations or that transactions exceeding a certain dollar value threshold are subject to additional approvals.	
BP.04.07.03 Management employs integrity verification tools to detect unauthorized changes to application software. *Related controls: CM.02.03.03 and BP.06.06.05*	Obtain an understanding of the entity's processes and methods for detecting unauthorized changes to application software through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's integrity verification tools, and • inspection of relevant documentation, such as policies and procedures for using and managing the entity's integrity verification tools, as well as implemented configuration	NIST SP 800-53, CM-6 NIST SP 800-53, SI-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	settings, found in system configuration files for the tools employed. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed the output of the entity's integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether such output was properly reviewed by appropriate personnel and whether appropriate action was taken on a timely basis to address any unauthorized changes detected. Inspect the implemented configuration settings for the integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether the implemented configuration settings are appropriate for detecting unauthorized changes to application software. Determine whether management properly employs integrity verification tools to detect unauthorized changes to application software. Note: Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.	
BP.05 Management designs and implements general control activities to reasonably assure that information system interfaces are properly managed to support the achievement of information processing objectives.		
BP.05.01 Interface roles and responsibilities are defined and assigned to appropriate personnel.		
BP.05.01.01 Interface ownership is appropriately assigned. *Related controls: SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.01, and BP.06.01.01*	Obtain an understanding of interface roles and responsibilities, including interface ownership, through • inquiry of appropriate personnel and	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant documentation, such as system security and privacy plans. Identify the interface owners for the information systems relevant to the significant business processes. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities. Determine whether interface ownership has been appropriately assigned. Note: Interface ownership comprises overall responsibility and accountability for management of the interface, including ensuring that the interface is properly processed on a timely basis in a secure manner. Thus, any changes to the design of the interface, modifications to the tools and techniques for interface processing, or changes to corresponding access controls generally require the approval of the interface owner or the owner's authorized delegate.	
BP.05.01.02 Responsibilities for interface processing and correcting any errors are assigned to appropriate personnel, which may include users from the source and target systems. *Related controls: SD.01.01.01, SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.02, BP.05.01.02, BP.05.06.02, BP.06.01.02, BP.06.01.03, BP.06.01.04, and BP.06.01.05*	Obtain an understanding of the responsibilities for interface processing and correcting any errors through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution and system security and privacy plans. See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether assigned individuals possess appropriate skills and technical expertise to satisfy their responsibilities. Determine whether the responsibilities for interface processing and correcting any errors have been clearly defined and assigned to appropriate personnel. Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.	
BP.05.02 Policies and procedures for managing interfaces are developed and implemented.		
BP.05.02.01 Policies and procedures applied at the system and business process levels for managing interfaces are developed, documented, approved, and periodically reviewed and updated. Such policies and procedures appropriately • consider risk; • address the tools and techniques for interface processing, including the use of job scheduling software, the timing of the interface, and any dependences on upstream jobs or processes; • address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external entities, and compliance; • identify and describe the relevant processes; • consider information system general and application controls; • consider segregation of duties controls; and • help ensure that users can be held accountable for their actions through	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures for managing interfaces through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Through inquiry, inspection, and observation, identify information system controls relevant to the significant business processes and areas of audit interest. Throughout the engagement, determine whether the entity's policies and procedures for applying information system controls are designed, implemented, and operating effectively. Consider whether • policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external entities, and compliance; • procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be held accountable for their actions, and appropriately consider information system general and application controls as well as segregation of duties controls; and • policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purposes and support achieving the entity's internal control objectives.	NIST SP 800-53, AC-1 NIST SP 800-53, AT-1 NIST SP 800-53, AU-1 NIST SP 800-53, CA-1 NIST SP 800-53, CM-1 NIST SP 800-53, CP-1 NIST SP 800-53, IA-1 NIST SP 800-53, IR-1 NIST SP 800-53, MA-1 NIST SP 800-53, MP-1 NIST SP 800-53, PE-1 NIST SP 800-53, PL-1 NIST SP 800-53, PM-1 NIST SP 800-53, PS-1 NIST SP 800-53, PT-1 NIST SP 800-53, RA-1 NIST SP 800-53, SA-1 NIST SP 800-53, SC-1 NIST SP 800-53, SI-1 NIST SP 800-53, SR-1

Illustrative control activities	Illustrative audit procedures	Relevant criteria
appropriate logging and monitoring activities.	Throughout the engagement, determine whether the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures are designed, implemented, and operating effectively. Note: Audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its system-level and business process-level policies and procedures are intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of information system controls relevant to the significant business processes and the business process applications and information systems that support them. When effectively designed, the entity's policies and procedures for managing interfaces, as well as policies and procedures applicable to the significant business processes, provide suitable criteria for evaluating evidence regarding the implementation and operating effectiveness of information system controls.	
BP.05.03 Interfaces are designed to exchange information between systems and reasonably assure the confidentiality, integrity, and availability of interfaced data.		
BP.05.03.01 Interface characteristics are defined, implemented, and documented. *Related controls: SM.03.02.01 and AC.01.01.01*	Perform walk-throughs of the significant business processes. Consider whether the interfaces observed in walk-throughs of the significant business processes are consistent with those documented in system documentation and align with prescribed information protection requirements for the business process applications and information systems. Consider whether the design of each interface includes appropriate specifications based on relevant business requirements. Inspect system design documentation, system security and privacy plans, interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, and other exchange agreements, as well as policies and	NIST SP 800-53, CA-3 NIST SP 800-53, CA-9 NIST SP 800-53, CM-12 NIST SP 800-53, PM-11 NIST SP 800-53, SA-5 NIST SP 800-53, SA-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	procedures demonstrating the design of interfaces involved in the significant business processes. Determine whether interfaces are defined, implemented, and documented to reasonably assure the confidentiality, integrity, and availability of information. Note: Interface design documentation is maintained to support the entity's authorization process and to facilitate configuration management and change control procedures. Interface characteristics include the tools and techniques for interface processing, as well as information on the data fields being interfaced, controls designed and implemented to reasonably assure the integrity of the interfaced data, the timing of the interface or interface schedule, and any system balancing requirements and information security requirements. Interface characteristics for information exchanged between information systems are described in the respective system security and privacy plans.	
BP.05.03.02 Hashing algorithms or other mechanisms are employed to help ensure the integrity of interfaced data.	Perform walk-throughs of the significant business processes. Consider whether the interfaces observed in walk-throughs of the significant business processes are consistent with those documented in system documentation and align with prescribed information protection requirements for the business process applications and information systems. Consider whether the design of each interface includes appropriate hashing algorithms or other mechanisms based on relevant business requirements. Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of interfaces involved in the significant business processes. Determine whether hashing algorithms or other mechanisms are employed to help ensure the integrity of interfaced data.	NIST SP 800-53, SC-13

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.05.03.03 Encryption techniques are employed to protect the confidentiality of interfaced data when appropriate. *Related control: AC.03.02.02*	Perform walk-throughs of the significant business processes. Consider whether the interfaces observed in walk-throughs of the significant business processes are consistent with those documented in system documentation and align with prescribed information protection requirements for the business process applications and information systems. Consider whether the design of each interface includes appropriate encryption techniques based on relevant business requirements. Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of interfaces involved in the significant business processes. Determine whether encryption techniques are employed to protect the confidentiality of interfaced data when appropriate.	NIST SP 800-53, SC-8
BP.05.03.04 Automated business processes and corresponding application controls are designed to help ensure that interfaced data are processed once and only once.	Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for interface processing, including the use of job scheduling software, the timing of each interface, and any dependencies on upstream jobs or processes. Consider the extent to which automated business processes and corresponding application controls are designed to help ensure that interfaced data are processed once and only once. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk. Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of interfaces involved in the significant business processes. Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective.	NIST SP 800-53, PM-11 NIST SP 800-53, SA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that interfaced data are processed once and only once. Note: When suitably designed and properly implemented, automated business processes and corresponding application controls provide reasonable assurance that interfaced data are processed once and only once. To help ensure this, interface files may be automatically archived or deleted from the production environment after processing.	
BP.05.04 Interface errors are identified on a timely basis.		
BP.05.04.01 A mechanism is employed to notify users when files sent from a source system are received by the target system.	Obtain an understanding of any mechanisms employed by the entity to notify users when files sent from a source system are received by the target system through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution and system security and privacy plans. See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Observe the use of any mechanisms employed by the entity to notify users when files sent from a source system are received by the target system. Determine whether the mechanisms employed by the entity to notify users when files sent from a source system are received by the target system are suitably designed and properly implemented based on risk. Note: A positive acknowledgment scheme or “handshake” between the systems helps ensure that files are not skipped or lost.	NIST SP 800-53, SI-10 NIST SP 800-53, SI-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.05.04.02 A mechanism is employed to notify users when an interface fails or specific data are rejected.	Obtain an understanding of any mechanisms employed by the entity to notify users when an interface fails or specific data are rejected through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution and system security and privacy plans. See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Observe the use of any mechanisms employed by the entity to notify users when an interface fails or specific data are rejected. Determine whether the mechanisms employed by the entity to notify users when an interface fails or specific data are rejected are suitably designed and properly implemented based on risk.	NIST SP 800-53, SI-10 NIST SP 800-53, SI-11
BP.05.04.03 The status of interfaces processed through job scheduling software is monitored by appropriate personnel. *Related control: BP.05.06.02 and BP.05.07.01*	Obtain an understanding of the entity's processes and methods to monitor the status of interfaces involved in the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution and system security and privacy plans. See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of interfaces processed through job scheduling software. Observe personnel as they perform procedures for monitoring the status of interfaces processed through job scheduling software. Consider whether such individuals possess appropriate skills and	NIST SP 800-53, AU-2 NIST SP 800-53, AU-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	technical expertise to satisfy their assigned business process application responsibilities. Consider whether the procedures observed are consistent with those documented by the entity. Determine whether the status of interfaces processed through job scheduling software is monitored by appropriate personnel. Note: A mechanism may also be employed to notify users when an interface fails or specific data are rejected. For example, an email may be sent to users of the source or target systems or to those individuals responsible for the job schedule.	
BP.05.04.04 Reconciliations of interfaced data from the source and target systems are performed to verify the integrity of interfaced data.	For the interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to reconcile interfaced data from the source and target systems through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to reconcile interfaced data from the source and target systems. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure the integrity of interfaced data. Inspect available documentation for a selection of reconciliations performed during the audit period. Consider whether such reconciliations were appropriate and performed in accordance with the entity's policies and procedures for reconciling interfaced data. Determine whether reconciliations of interfaced data from the source and target systems are appropriately performed to verify the integrity of interfaced data.	NIST SP 800-53, SI-10 NIST SP 800-53, SI-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Reconciliations are performed between source and target systems to help ensure that interfaced data are complete and accurate. Control totals are agreed between the source and target systems. Reports provide adequate information to support the reconciliation of interfaced data between the two systems.	
BP.05.04.05 Interface processing events are logged to permit management oversight. *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.02.02, and AC.05.02.03*	Obtain an understanding of the entity's processes and methods to monitor the status of interfaces involved in the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution and system security and privacy plans. See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of interfaces. Identify the event types for logging relevant to interface processing. Consider whether the event types selected for logging are adequate to support error identification, research, and resolution. Determine whether interface processing events relevant to the significant business processes are appropriately logged to permit management oversight.	NIST SP 800-53, AU-2 NIST SP 800-53, AU-12
BP.05.04.06 Management reviews interface processing logs on a timely basis. *Related control objectives: AC.05.02 and AC.05.03*	Obtain an understanding of the entity's processes and methods to monitor the status of interfaces involved in the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution and system security and privacy plans.	NIST SP 800-53, AU-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures. Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of interfaces. Inspect available audit records for a selection of events that occurred during the audit period applicable to the interfaces involved in the significant business processes. Consider whether the actions taken to review and analyze such records are adequate to support error identification, research, and resolution on a timely basis. Consider whether such actions were performed in accordance with the entity's policies and procedures for logging and monitoring the status of interfaces. Consider the completeness and accuracy of the documentation obtained, including any reports produced by log management software, when performing control tests. Determine whether management appropriately reviews interface processing logs on a timely basis.	
BP.05.05 Interface errors are researched and resolved on a timely basis.		
BP.05.05.01 Interface processing errors are researched to identify and remediate their causes.	For the interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to identify and remediate the causes of interface processing errors through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to identify and remediate the causes of interface processing errors. Consider whether such processes and methods	NIST SP 800-53, SI-10 NIST SP 800-53, SI-12 NIST SP 800-53, SI-15

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk and • reasonably assure that interface processing errors are adequately researched to timely identify and remediate their causes. Inspect available documentation for a selection of interface processing errors that occurred during the audit period. Consider whether the causes of the errors were timely identified and remediated. Consider whether adequate information, such as interface processing logs and audit trails, exists to support error identification, research, and resolution on a timely basis. Consider whether rejected data are isolated to facilitate the process of identifying and remediating the causes of the errors. Determine whether interface processing errors are appropriately researched to identify and remediate their causes. Note: Interface processing logs and audit trails are used to identify and follow up on interface processing errors. The corrections to interface processing errors are included in the audit trail.	
BP.05.05.02 Interface processing errors are resolved by correcting data, coding errors in computer programs, or a combination thereof.	For the interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to identify and remediate the causes of interface processing errors through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to identify and remediate the causes of interface processing errors. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and	NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• reasonably assure that interface processing errors are properly resolved. Inspect available documentation for a selection of interface processing errors that occurred during the audit period. Consider whether adequate documentation exists to support any necessary changes to data or modifications to computer programs, including evidence demonstrating that the corrections were properly verified and approved by management. Determine whether interface processing errors are properly resolved by correcting data, coding errors in computer programs, or a combination thereof.	
BP.05.06 Access to interface data and user-defined processing of data are appropriately controlled.		
BP.05.06.01 User-defined processing of data prior to interface processing is appropriately controlled. *Related control: SD.01.01.01*	Perform walk-throughs of the significant business processes. Obtain an understanding of any user-defined processing of data prior to interface processing, as well as the processes and methods by which user-defined processing of data are controlled. Observe the performance of user-defined processing. Consider whether the users who perform this processing are appropriately authorized to perform such actions. Through a combination of inspection and reperformance, consider whether the results of user-defined processing are complete, accurate, and valid. Observe any approvals of the results of user-defined processing and inspect any documentary evidence related to such approvals. Consider whether the users who approve such results are appropriately authorized to perform such actions and whether such users take adequate steps to assess the completeness, accuracy, and validity of the results. Determine whether user-defined processing of data prior to interface processing is appropriately controlled. Note: Some interfaces may require user-defined processing of data prior to interface processing, whereby a user may establish or modify	NIST SP 800-53, AC-2 NIST SP 800-53, AC-5 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	processing steps to prepare the data for the interface. This frequently occurs when business processes applications rely on data extraction tools and spreadsheets to exchange information between information systems. It is important that entities establish clear policies and procedures governing user-defined processing and employ effective internal controls, including proper segregation of duties, over such processing to reasonably assure the completeness, accuracy, and validity of the corresponding data.	
BP.05.06.02 The execution of interfaces is appropriately controlled. *Related controls: BP.05.01.02 and BP.05.04.03*	Perform walk-throughs of the significant business processes. Obtain an understanding of the processes and methods by which interfaces involved in the significant business processes are executed. Observe the execution of interfaces involved in the significant business processes, including any steps users perform from the source and target systems, as well as any monitoring of the status of interfaces processed through job scheduling software. Consider whether the users involved in the execution of interfaces involving significant business processes are appropriately authorized to perform such actions. Determine whether the execution of interfaces is appropriately controlled.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-5 NIST SP 800-53, AC-6
BP.05.06.03 Any data files generated during interface processing are properly secured from unauthorized access, modification, or disposal.	Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identity key data files generated during interface processing. Obtain an understanding of the entity's processes and methods to secure key data files generated through interface processing from unauthorized access, modification, or disposal. Consider whether such processes and methods adequately address access controls for such data files. Consider whether the users involved in the processes are appropriately authorized to perform such actions.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6 NIST SP 800-53, SI-12 NIST SP 800-53, SI-15

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether key data files generated during interface processing are properly secured from unauthorized access, modification, or disposal.	
BP.05.06.04 Any data files generated during interface processing are automatically archived or deleted from the production environment after processing.	Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identity key data files generated during interface processing. Obtain an understanding of the entity's processes and methods to automatically archive or delete key data files generated through interface processing from the production environment after processing. Determine whether key data files generated during interface processing are automatically archived or deleted from the production environment after processing.	NIST SP 800-53, SI-12
BP.05.07 Modifications to interfaces are appropriately controlled.		
BP.05.07.01 Modifications to the tools and techniques for interface processing, including any job scheduling software employed, are appropriately controlled. *Related control objectives: CM.02.01 and CM.02.02*	For the interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to modify the tools and techniques for interface processing through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to modify the tools and techniques for interface processing. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that modifications to the tools and techniques for interface processing are appropriately controlled.	NIST SP 800-53, CM-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect available documentation for a selection of modifications to the tools and techniques for interface processing, including any changes to the job schedule or job-scheduling software employed, that occurred during the audit period. Consider whether adequate documentation exists to support such modifications, including evidence demonstrating that the modifications were properly verified and approved by management. Consider whether the individuals involved in the modifications are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized modifications to the tools and techniques for interface processing. Determine whether modifications to the tools and techniques for interface processing, including any job-scheduling software employed, are appropriately controlled.	
BP.05.07.02 Changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled. *Related control objectives: CM.02.01 and CM.02.02*	For the interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to change any mapping tables used to convert data from the source system for input to the target system through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for interface processing and error resolution. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to change mapping tables. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled. Inspect available documentation for a selection of changes to mapping tables for the interfaces involved in the significant business processes	NIST SP 800-53, CM-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that management properly verified and approved the changes. Consider whether the individuals who made the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to the mapping tables for the interfaces involved in the significant business processes. Determine whether changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled. Note: When mapping tables are used, it is important that controls are designed and implemented to reasonably assure that mapping tables are only changed when authorized and that historical data on mappings are retained with the previous mapping table. If mapping tables are not used, it is important that appropriate data input, processing, and output controls are designed and implemented in the source and target systems to help ensure that source data from the source system satisfy the target system's specified definitions for data format and content, such as character set, length, numerical range, and acceptable values.	
BP.06 Management designs and implements general control activities to reasonably assure that data management systems are properly managed to support the achievement of information processing objectives.		
BP.06.01 Data management system roles and responsibilities are defined and assigned to appropriate personnel.		
BP.06.01.01 Data ownership is appropriately assigned. *Related controls: SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.01, and BP.06.01.01*	Obtain an understanding of data management system roles and responsibilities, including data ownership, through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system security and privacy plans.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Identify the data owners for the information systems relevant to the significant business processes. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities. Determine whether data ownership has been appropriately assigned. Note: Data ownership comprises overall responsibility and accountability for the management of data, including ensuring that data are processed properly, timely, and securely. Thus, any changes to the design of the data management system, modifications to the schema or structure of the database, modifications to transaction or master data made outside the business process application through the database management software, or changes to corresponding access controls generally require the approval of the data owner or the owner's authorized delegate.	
BP.06.01.02 Responsibilities for requesting, authorizing, and implementing changes to the schema or structure of the database are assigned to appropriate personnel. *Related controls: SD.01.01.01, SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.02, BP.05.01.02, BP.06.01.03, BP.06.01.04, and BP.06.01.05*	Obtain an understanding of the responsibilities for requesting, authorizing, and implementing changes to the schema or structure of the database through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for data management, and system security and privacy plans. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether assigned individuals possess appropriate skills and technical expertise to satisfy their responsibilities. Determine whether the responsibilities for requesting, authorizing, and implementing changes to the schema or structure of the database have been clearly defined and assigned to appropriate personnel. Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.	
BP.06.01.03 Responsibilities for requesting, authorizing, and implementing changes to transaction and master data through the database management software are assigned to appropriate personnel. *Related controls: SD.01.01.01, SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.02, BP.05.01.02, BP.06.01.02, BP.06.01.04, and BP.06.01.05*	Obtain an understanding of the responsibilities for requesting, authorizing, and implementing changes to transaction and master data through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for data management, and system security and privacy plans. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Determine whether the responsibilities for requesting, authorizing, and implementing changes to transaction and master data have been clearly defined and assigned to appropriate personnel. Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24
BP.06.01.04 Responsibilities for database table maintenance are assigned to appropriate personnel. *Related controls: SD.01.01.01, SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.02, BP.05.01.02, BP.06.01.02, BP.06.01.03, and BP.06.01.05*	Obtain an understanding of the responsibilities for database table maintenance through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for data management, and system security and privacy plans.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Determine whether the responsibilities for database table maintenance have been clearly defined and assigned to appropriate personnel. Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.	
BP.06.01.05 Responsibilities for monitoring changes to the database, including changes to transaction and master data, are assigned to appropriate personnel. *Related controls: SD.01.01.01, SM.01.02.02, SM.01.02.03, SM.01.05.05, BP.04.01.02, BP.05.01.02, BP.06.01.02, BP.06.01.03, and BP.06.01.04*	Obtain an understanding of the responsibilities for monitoring changes to the database through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for data management, and system security and privacy plans. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Determine whether the responsibilities for monitoring changes to the database have been clearly defined and assigned to appropriate personnel. Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	entity by considering the need to separate authority, custody, and accounting in the organizational structure.	
BP.06.02 Policies and procedures for managing data management systems are developed and implemented.		
BP.06.02.01 Policies and procedures applied at the system and business process levels for administering data management systems are developed, documented, approved, and periodically reviewed and updated. Such policies and procedures appropriately • consider risk; • address changes to the schema or structure of the database, including any required approvals or authorizations; • address changes to transaction and master data made outside the business process application through the database management software; • address database table maintenance; • address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external entities, and compliance; • identify and describe the relevant processes; • consider information system general and application controls;	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures for administering data management systems through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Through inquiry, inspection, and observation, identify information system controls relevant to the significant business processes and areas of audit interest. Throughout the engagement, determine whether the entity's policies and procedures for applying information system controls are designed, implemented, and operating effectively. Consider whether 1. policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external entities, and compliance; 2. procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be held accountable for their actions, and appropriately consider information system general and application controls and segregation of duties controls; and 3. policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity's internal control objectives. Throughout the engagement, determine whether the entity's processes and methods for developing, documenting, and periodically	NIST SP 800-53, AC-1 NIST SP 800-53, AT-1 NIST SP 800-53, AU-1 NIST SP 800-53, CA-1 NIST SP 800-53, CM-1 NIST SP 800-53, CP-1 NIST SP 800-53, IA-1 NIST SP 800-53, IR-1 NIST SP 800-53, MA-1 NIST SP 800-53, MP-1 NIST SP 800-53, PE-1 NIST SP 800-53, PL-1 NIST SP 800-53, PM-1 NIST SP 800-53, PS-1 NIST SP 800-53, PT-1 NIST SP 800-53, RA-1 NIST SP 800-53, SA-1 NIST SP 800-53, SC-1 NIST SP 800-53, SI-1 NIST SP 800-53, SR-1

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• consider segregation of duties controls; and • help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities.	reviewing and updating system-level and business process-level policies and procedures are designed, implemented, and operating effectively. Note: Audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its system-level and business process-level policies and procedures are intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of information system controls relevant to the significant business processes and the business process applications and information systems that support them. When effectively designed, the entity's policies and procedures for administering data management systems, as well as policies and procedures applicable to the significant business processes, provide suitable criteria for evaluating evidence regarding the implementation and operating effectiveness of information system controls.	
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, as well as the confidentiality, integrity, and availability of application data.		
BP.06.03.01 Data management system characteristics, including the schema or structure of the database, are defined, implemented, and documented.	Perform walk-throughs of the significant business processes. Consider whether the data management systems involved in the significant business processes are implemented consistent with system design documentation and align with prescribed information protection requirements for the business process applications and information systems. Consider whether the design of the schema or structure of the database includes appropriate specifications based on relevant business requirements. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of data management systems involved in the significant business processes. Determine whether data management system characteristics, including the schema or structure of the database, are appropriately	NIST SP 800-53, CM-12 NIST SP 800-53, PM-11 NIST SP 800-53, SA-5 NIST SP 800-53, SA-8 NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	defined, implemented, and documented to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information. Note: Applications that handle significant volumes of data often employ data management systems to perform certain data-processing functions within an application. Data management systems use specialized software that may operate on specialized hardware. Many of the configurable controls, such as data validations involving acceptable values and thresholds, are implemented in functions of data management systems. These types of configurable controls implemented in data management systems are often referred to as business rules.	
BP.06.03.02 Master data requirements are established and implemented into the database design to help ensure that master data are complete, accurate, and valid.	Obtain an understanding of any master data requirements established and implemented into the database design through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of data management systems involved in the significant business processes. Determine whether master data requirements are appropriately established and properly implemented into the database design to help ensure that master data are complete, accurate, and valid.	NIST SP 800-53, PM-11 NIST SP 800-53, SA-5 NIST SP 800-53, SI-10
BP.06.03.03 Transaction data requirements are established and implemented into the database design to help ensure that transaction data are complete, accurate, and valid.	Obtain an understanding of any transaction data requirements established and implemented into the database design through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of data management systems involved in the significant business processes.	NIST SP 800-53, PM-11 NIST SP 800-53, SA-5 NIST SP 800-53, SI-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether transaction data requirements are established and implemented into the database design to help ensure that transaction data are complete, accurate, and valid.	
BP.06.03.04 Null values or invalid values are not accepted in key fields. *Related controls: BP.01.02.01, BP.02.01.01, and BP.04.03.10*	Perform walk-throughs of the significant business processes. Observe appropriate personnel as they input data into key fields, noting any input data validation errors that occur when null values or invalid values are entered. Inspect system design documentation, system security and privacy plans, applicable system configuration files, and policies and procedures demonstrating the defined parameters for key fields. Determine whether the management-identified parameters for key fields are appropriate to reasonably assure that null values or invalid values are not accepted.	NIST SP 800-53, PM-11 NIST SP 800-53, SA-5 NIST SP 800-53, SI-10
BP.06.03.05 Access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data. *Related controls: SD.01.01.01, SD.01.02.01, SD.01.02.02, and SD.01.03.01*	Perform walk-throughs of the significant business processes. Consider whether access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database. Determine whether access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data. Note: Access controls in a data management system include consideration for the access paths to the database. The access paths are clearly documented and updated as changes are made. Generally, access to a database can be obtained in three ways: (1) directly through the database, (2) through access paths facilitated by the business process application, or (3) through the operating system(s) underlying the database.	NIST SP 800-53, AC-5 NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Segregation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Segregation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because segregation of duties violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on segregation of duties.	
BP.06.03.06 The schema or structure of the database is aligned with management's authorizations for users. *Related control objective: AC.02.03*	Obtain an understanding of the database schema or structure through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Identify the access paths to data and the processes and methods for controlling data management system administrative functions. Consider whether the database schema or structure is consistent with access control requirements such that the organization of data and database-hosted functions correspond to the access restrictions that need to be imposed on different groups of users. Determine whether the schema or structure of the database is aligned with management's authorizations for users. Note: Data management systems have built-in privileged accounts that are often used for data management system administrative functions. Such accounts may be controlled through a combination of (1) strong passwords or other authentication mechanisms, (2) highly restrictive assignment of personnel to the accounts, (3) enforcement of	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	unique identification and authentication for each administrator, and (4) effective logging and monitoring of privileged account usage.	
BP.06.03.07 Sensitive application data are appropriately controlled and encrypted when appropriate.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes perform to control logical access to sensitive application data through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the data management system, as well as implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced using access control software. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the processes and methods the relevant information systems perform to control logical access to sensitive application data. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems, business process applications, and data management systems; • employ encryption techniques when appropriate based on risk; • are suitably designed and properly implemented based on risk; and • reasonably assure that access to sensitive application data is restricted to authorized individuals for authorized purposes. Determine whether sensitive application data are appropriately controlled and encrypted when appropriate.	NIST SP 800-53, AC-23 NIST SP 800-53, SC-13 NIST SP 800-53, SC-28

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Entities may employ data-mining protection and detection techniques to protect sensitive application data from unauthorized data mining.	
BP.06.03.08 Access controls are incorporated into the design of the data management system to help ensure that the physical and logical (in terms of connectivity) locations of the data storage and retrieval functions are appropriate.	Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database. Determine whether access controls are incorporated into the design of the data management system to help ensure that the physical and logical (in terms of connectivity) locations of the data storage and retrieval functions are appropriate.	NIST SP 800-53, AC-5 NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5
BP.06.03.09 Access controls are incorporated into the design of the data management system to help ensure that production data are separated from nonproduction systems (such as testing and development) and other production systems with lesser control requirements.	Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database. Determine whether access controls are incorporated into the design of the data management system to help ensure that production data are separated from nonproduction systems (such as testing and development) and other production systems with lesser control requirements.	NIST SP 800-53, AC-5 NIST SP 800-53, PM-11 NIST SP 800-53, SA-4 NIST SP 800-53, SA-5
BP.06.04 The completeness, accuracy, and validity of data maintained in data management systems are periodically assessed.		
BP.06.04.01 Management periodically reviews master data records to verify that master data are complete, accurate, and valid.	Obtain an understanding of the entity's processes and methods for periodically reviewing master data records through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed master data records to verify that master data are complete, accurate, and valid. Consider whether such actions	NIST SP 800-53, SI-10 NIST SP 800-53, SI-18

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	were appropriate and performed in accordance with the entity's policies and procedures. Determine whether the entity's processes and methods for periodically reviewing master data records are designed, implemented, and operating effectively.	
BP.06.04.02 Management periodically reviews master data records to help ensure that master data are consistent between business process application modules and among other information systems using the same master data.	Obtain an understanding of the entity's processes and methods for periodically reviewing master data records through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed master data records to help ensure that master data are consistent between business process application modules and among other information systems using the same master data. Consider whether such actions were appropriate and were performed in accordance with the entity's policies and procedures. Determine whether the entity's processes and methods for periodically reviewing master data records are designed, implemented, and operating effectively.	NIST SP 800-53, SI-10 NIST SP 800-53, SI-18
BP.06.05 Access to data management systems is appropriately controlled.		
BP.06.05.01 Data management system roles and corresponding access privileges are authorized and assigned to users with a valid business purpose (least privilege). *Related control: BP.04.06.01* *Related control objective: AC.02.03*	Inspect a system-generated list of accounts for each of the data management systems relevant to the significant business processes. Consider the roles assigned to each account and whether such assignments are appropriate based on the purpose of the account, the type of account, and the users or processes to which the account is assigned.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-5 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether data management system roles and corresponding access privileges are appropriately authorized and assigned to users with a valid business purpose (least privilege).	
BP.06.05.02 Access control requirements for specialized data management processes used to facilitate interoperability between business process applications and functions not integrated into the applications (such as ad hoc reporting) are consistent with access control requirements for the business process applications, data management systems, and other systems that may be affected.	Perform walk-throughs of the significant business processes. Consider whether access control requirements for specialized data management processes used to facilitate interoperability between business process applications and functions not integrated into the applications (such as ad hoc reporting) are consistent with access control requirements for the business process applications, data management systems, and other systems that may be affected. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the access control requirements for any specialized data management processes. Determine whether access control requirements for specialized data management processes used to facilitate interoperability between business process applications and functions not integrated into the applications (such as ad hoc reporting) are consistent with access control requirements for the business process applications, data management systems, and other systems that may be affected.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-5 NIST SP 800-53, AC-6
BP.06.05.03 The data management system logs events associated with changes to business process application data, including master data. *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.02.02, and AC.05.02.03*	Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identity key event types for logging associated with the entity's procedures for data input, processing, and output. Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the entity's processes and methods for logging and monitoring events at the business process level. Determine whether the data management systems relevant to the significant business processes properly log events associated with changes to business process application data, including master data.	NIST SP 800-53, AU-2 NIST SP 800-53, AU-3 NIST SP 800-53, AU-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.06.06 Modifications to data management systems and data maintained in data management systems are appropriately controlled.		
BP.06.06.01 Changes to the schema or structure of the database are appropriately controlled.	Obtain an understanding of the entity's processes and methods to change the schema or structure of databases through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to change the schema or structure of databases. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that changes to the schema or structure of the database are appropriately controlled. Inspect available documentation for a selection of changes to the schema or structure of databases relevant to the significant business processes that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that management properly verified and approved changes. Consider whether the individuals involved in the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to the schema or structure of databases relevant to the significant business processes. Determine whether changes to the schema or structure of the database are appropriately controlled.	NIST SP 800-53, CM-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.06.06.02 Changes to transaction and master data made through the database management software are appropriately controlled.	Obtain an understanding of the entity's processes and methods to change transaction and master data through the database management software through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to change transaction and master data through the database management software. Consider whether such processes and methods • are suitably designed and properly implemented based on risk; • address the entity's approach for de-identification, if applicable; and • reasonably assure that changes to transaction and master data made through the database management software are appropriately controlled. Inspect available documentation for a selection of changes to transaction and master data relevant to the significant business processes that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that management properly verified and approved the changes. Consider whether the individuals involved in the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to transaction and master data through the database management software.	NIST SP 800-53, CM-3 NIST SP 800-53, SI-19

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether changes to transaction and master data made through the database management software are appropriately controlled. Note: De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many data sets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records. Data sets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Trained individuals remove personally identifiable information from data sets when it is not (or no longer) necessary to satisfy the requirements envisioned for the data.	
BP.06.06.03 Data owners monitor changes to the schema or structure of the database, as well as changes to transaction and master data made through the database management software.	Obtain an understanding of the entity's processes and methods to monitor changes to the schema or structure of databases through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Observe personnel as they perform procedures for monitoring changes to the schema or structure of the database, as well as changes to transaction and master data made through the database management software. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Consider whether the procedures observed are consistent with those documented by the entity. Determine whether data owners monitor changes to the schema or structure of the database, as well as changes to transaction and master data made through the database management software.	NIST SP 800-53, CM-3 NIST SP 800-53, CM-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
BP.06.06.04 Management regularly performs database table maintenance.	Obtain an understanding of the entity's processes and methods to regularly perform database table maintenance through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Observe personnel as they perform database table maintenance. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Consider whether the procedures observed are consistent with those documented by the entity. Determine whether management regularly performs database table maintenance.	NIST SP 800-53, SC-28
BP.06.06.05 Management employs integrity verification tools to detect unauthorized changes to data management systems and data maintained in these systems. *Related controls: CM.02.03.03 and BP.04.07.03*	Obtain an understanding of the entity's processes and methods for detecting unauthorized changes to data management systems and data maintained in these systems through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's integrity verification tools, and • inspection of relevant documentation, such as policies and procedures for using and managing the entity's integrity verification tools, as well as implemented configuration settings, found in system configuration files for the tools employed. See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed the output of the entity's integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business	NIST SP 800-53, CM-6 NIST SP 800-53, SC-28 NIST SP 800-53, SI-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	processes. Consider whether such output was properly reviewed by appropriate personnel and whether appropriate action was taken on a timely basis to address any unauthorized changes detected. Inspect the implemented configuration settings for the integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether the implemented configuration settings are appropriate for detecting unauthorized changes to data management systems and data maintained in these systems. Determine whether management properly employs integrity verification tools to detect unauthorized changes to data management systems and data maintained in these systems.	

FISCAM Framework for Security Management

Table 9. FISCAM framework for security management.

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.01 Management establishes organizational structures, assigns 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.01.01.01 An information security management organizational structure that has adequate independence, authority, expertise, and resources is established and documented.	Obtain an understanding of the organizational structure supporting the entity's information security management program through • inquiry of appropriate personnel and • inspection of relevant documentation, such as applicable organizational charts, business or organizational unit descriptions, and staffing plans. Determine whether the organizational structure supporting the entity's information security management program has adequate independence, authority, expertise, and resources to achieve the entity's information security objectives.	NIST SP-800-53, PL-9 NIST SP 800-53, SA-2
SM.01.01.02 A privacy management organizational structure that has adequate independence, authority, expertise, and resources is established and documented.	Obtain an understanding of the organizational structure supporting the entity's privacy management program through • inquiry of appropriate personnel and • inspection of relevant documentation, such as applicable organizational charts, business or organizational unit descriptions, and staffing plans. Determine whether the organizational structure supporting the entity's privacy management program has adequate independence, authority, expertise, and resources to achieve the entity's privacy objectives.	NIST SP 800-53, PL-9 NIST SP 800-53, SA-2
SM.01.01.03 A supply chain risk management organizational structure that has adequate	Obtain an understanding of the organizational structure supporting the entity's supply chain risk management activities through • inquiry of appropriate personnel and	NIST SP 800-53, PL-9 NIST SP 800-53, SA-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
independence, authority, expertise, and resources is established and documented.	• inspection of relevant documentation. Determine whether the organizational structure supporting the entity's supply chain risk management activities has adequate independence, authority, expertise, and resources.	
SM.01.02 Responsibilities are assigned to senior management positions within the information security and privacy functions.		
SM.01.02.01 An information security officer is appointed and given the authority and resources to coordinate, develop, implement, and maintain the entity's information security management program.	Obtain an understanding of the responsibilities of the information security officer through • inquiry of appropriate personnel and • inspection of information security management program documentation. Determine whether an information security officer has been appointed and given appropriate authority and resources. Consider whether the appointed information security officer possesses appropriate skills and technical expertise to satisfy the responsibilities of the position.	NIST SP 800-53, PM-2
SM.01.02.02 Senior management officials are assigned as authorizing officials for information systems and for common controls that organizational systems may inherit. *Related controls: BP.04.01.01, BP.04.01.02, BP.05.01.01, BP.05.01.02, BP.06.01.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, and BP.06.01.05*	Identify the assigned authorizing officials for the information systems relevant to the significant business processes and the common controls inherited by such systems. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy the responsibilities. Obtain an understanding of the tasks senior management officials perform to satisfy their responsibilities as authorizing officials through • inquiry of appropriate personnel, including the authorizing officials, and • inspection of information security management program documentation. Determine whether senior management officials have been assigned as authorizing officials for the information systems relevant to the significant business processes and the common controls that such systems inherit.	NIST SP 800-53, CA-6 NIST SP 800-53, PM-10 NIST SP 800-53, SA-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: The authorization process is a federal responsibility; therefore, authorizing officials are required to be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Additionally, authorizing officials are responsible for managing risks from the use of external system services.	
SM.01.02.03 In coordination with the data governance body and data integrity board, information security responsibilities are defined and assigned to (1) senior management, (2) information resource owners and users, (3) IT management personnel, and (4) security administrators. *Related controls: BP.04.01.01, BP.04.01.02, BP.05.01.01, BP.05.01.02, BP.06.01.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, SD.01.01.01, and SD.01.01.02*	Obtain an understanding of the information security responsibilities of senior management, information resource owners and users, IT management personnel, and security administrators through • inquiry of appropriate personnel and • inspection of information security management program documentation. Determine whether information security responsibilities have been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned information security responsibilities. Note: To achieve the entity's objectives, management assigns responsibility and delegates authority to key roles throughout the entity. To do so, management considers the overall responsibilities assigned to each business or organizational unit, determines what key roles are needed to fulfill the assigned responsibilities, and establishes the key roles. Management also determines what level of authority each key role needs to fulfill a responsibility. As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.01.02.04 A privacy officer is appointed and given the authority and resources to coordinate, develop, implement, and maintain the entity's privacy management program.	Obtain an understanding the responsibilities of the privacy officer through • inquiry of appropriate personnel and • inspection of privacy management program documentation. Determine whether a privacy officer has been appointed and given appropriate authority and resources. Consider whether the appointed privacy officer possesses appropriate skills and technical expertise to satisfy the responsibilities of the position.	NIST SP 800-53, PM-19
SM.01.02.05 In coordination with the data governance body and data integrity board, privacy responsibilities are defined and assigned to (1) senior management, (2) information resource owners and users, (3) IT management personnel, and (4) security administrators.	Obtain an understanding of the privacy responsibilities of senior management, information resource owners and users, IT management personnel, and security administrators through • inquiry of appropriate personnel and • inspection of privacy management program documentation. Determine whether privacy responsibilities have been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned information security responsibilities.	NIST SP 800-53, PM-3 NIST SP 800-53, PM-23 NIST SP 800-53, PM-24
SM.01.02.06 A chief risk officer is appointed and given the authority and resources to align information security and privacy management processes with strategic, operational, and budgetary planning processes and to reasonably assure consistent risk management practices across the organization.	Obtain an understanding of the responsibilities of the chief risk officer through • inquiry of appropriate personnel and • inspection of relevant documentation. Determine whether a chief risk officer has been appointed and given appropriate authority and resources. Consider whether the appointed risk management officer possesses appropriate skills and technical expertise to satisfy the responsibilities of the position.	NIST SP 800-53, PM-29
SM.01.03 Planning documentation related to the entity's information security management program is developed and maintained.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.01.03.01 Management develops, documents, and periodically reviews and updates an entity-level information security management program plan that is aligned with the entity-level strategic plan. This program plan includes • approval by a senior official with responsibility and accountability for the risk being incurred; • requirements of the entity's information security management program, including the coordination among organizational entities responsible for information security; • descriptions of the program management controls and common controls for meeting requirements; and • assignment of roles and responsibilities for the information security management program.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level information security management program plan through • inquiry of appropriate personnel, including the senior official responsible for the plan, and • inspection of relevant documentation. Inspect the entity-level information security management program plan. Consider whether the plan • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); • is aligned with the entity-level strategic plan; • includes required information in accordance with authoritative criteria; and • is adequate to guide the implementation of the entity's information security management program and achieve the entity's information security objectives. Determine whether the entity-level information security management program plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, determine whether the entity-level information security management program plan has been implemented.	NIST SP 800-53, PM-1 NIST SP 800-53, PM-2
SM.01.03.02 Management develops, documents, and periodically reviews and updates an entity-level privacy management program plan. This program plan includes • approval by a senior official with responsibility and accountability for the risk being incurred;	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level privacy management program plan through • inquiry of appropriate personnel, including the senior official responsible for the plan, and • inspection of relevant documentation.	NIST SP 800-53, PM-18 NIST SP 800-53, PM-19 NIST SP 800-53, PM-20 NIST SP 800-53, PM-21 NIST SP 800-53, PM-22 NIST SP 800-53, PM-25

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• descriptions of the privacy management program strategic goals and objectives; • descriptions of the requirements of a privacy management program, including the coordination among organizational entities responsible for information security; • descriptions of the privacy controls for meeting those requirements; and • assignment of roles and responsibilities for the privacy management program.	Inspect the entity-level privacy management program plan. Consider whether the plan • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); • includes required information in accordance with authoritative criteria; and • is adequate to guide the implementation of the entity's privacy management program and achieve the entity's privacy objectives. Determine whether the entity-level privacy management program plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, determine whether the entity-level privacy management program plan has been implemented.	NIST SP 800-53, PM-26 NIST SP 800-53, PM-27 NIST SP 800-53, PT-2 NIST SP 800-53, PT-3
SM.01.04 System development life cycle processes that incorporate information security and privacy considerations are established.		
SM.01.04.01 System development life cycle processes are developed, documented, and periodically reviewed and updated. *Related controls: SD.01.02.05, CM.02.01.01, and CM.02.02.01*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating its system development life cycle processes through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the entity's system development life cycle processes. Consider whether the processes • identify roles and responsibilities; • are integrated with the entity's risk management processes; • address the entity's application of security and privacy engineering principles in the specification, design, development, implementation, and modification of information systems and information system components;	NIST SP 800-53, SA-3 NIST SP 800-53, SA-8 NIST SP 800-53, SA-10 NIST SP 800-53, SA-11 NIST SP 800-53, SA-15 NIST SP 800-53, SA-17 NIST SP 800-53, SA-22 NIST SP 800-53, SC-4 NIST SP 800-53, SC-31 NIST SP 800-53, SC-36 NIST SP 800-53, SC-38 NIST SP 800-53, SI-23 NIST SP 800-53, SR-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• incorporate operations security controls; • require developers to design information systems, information system components, and information system services to align with the system-level security and privacy architectures and the enterprise architecture of the entity; • facilitate tracing of source code to design specifications and functional requirements during testing; • establish the standards, tools, and tool configurations used in source code development; • provide for validation, verification, and flaw remediation used in source code development; • facilitate replacing or providing alternative support for system components that the developer, vendor, or manufacturer no longer supports; • establish system documentation requirements; • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and • are adequate to provide a foundation for the successful development, implementation, and operation of entity information systems. Determine whether the system development life cycle processes have been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, consider whether the system development life cycle processes have been implemented. Note: Effective system development life cycle processes provide a foundation for the successful development, implementation, and operation of entity information systems. Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	processes helps to reduce the number and severity of latent errors within information systems, information system components, and information system services. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, and service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.	
SM.01.04.02 An enterprise architecture that addresses security and privacy considerations is developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating an enterprise architecture that addresses security and privacy considerations through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the enterprise architecture of the entity. Consider whether the enterprise architecture • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); • is integrated with the entity's risk management processes; and • adequately addresses security and privacy considerations for the entity. Determine whether the enterprise architecture has been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, determine whether the enterprise architecture has been implemented. Note: The effective integration of security and privacy requirements into the enterprise architecture helps ensure that important security and privacy considerations are addressed throughout the system development life cycle and that those considerations are directly	NIST SP 800-53, PM-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	related to entity's mission and business functions. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the entity-level risk management strategy.	
SM.01.05 An incident response program is established.		
SM.01.05.01 The entity has developed and documented and periodically reviews and updates an entity-level incident response plan that • provides the entity with a road map for implementing its incident response capability; • describes the structure and organization of the incident response capability; • provides a high-level approach for how the incident response capability fits into the entity's organizational structure; • meets the unique requirements of the entity, which relate to mission, size, structure, and functions; • defines reportable incidents; • provides metrics for measuring the incident response capability within the entity; • defines the resources and management support needed to effectively maintain and mature an incident response capability;	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level incident response plan through • inquiry of appropriate personnel, including the senior officials responsible for the plan, and • inspection of relevant documentation. Inspect the entity-level incident response plan. Consider whether the plan • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); • includes required information in accordance with authoritative criteria; and • is adequate to guide the implementation of the entity's incident response program and achieve the entity's information security and privacy objectives. Determine whether the entity-level incident response plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, determine whether the entity-level incident response plan has been implemented.	NIST SP 800-53, IR-8 NIST SP 800-53, SR-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• addresses the sharing of incident information; • is reviewed and approved by management; and • explicitly designates responsibility for incident response to appropriate personnel. *Related control: AC.05.01.02*		
SM.01.05.02 An incident response program is implemented in accordance with the entity-level incident response plan. The program includes • incident response training to system users consistent with their assigned roles and responsibilities; • documented testing of the entity's incident response capabilities and follow up on findings; • appropriate incident handling activities supported by automated mechanisms and incident response team members with the necessary knowledge, skills, and abilities; • appropriate incident monitoring mechanisms to track and document incidents; • a means for reporting incident information; • appropriate incident response assistance;	Obtain an understanding of the entity's incident response program through • inquiry of appropriate personnel, including the senior officials responsible for the plan, and • inspection of relevant documentation. Inspect documentation for the entity's incident response program. Consider whether • incident response training is associated with the assigned roles and responsibilities of entity personnel to reasonably assure that the appropriate content and level of detail are included in such training; • the entity tests its incident response capabilities to determine their effectiveness and identifies potential weaknesses or deficiencies for follow-up; • incident handling activities are consistent with the incident response plan and supported by automated mechanisms and incident response team members with the necessary knowledge, skills, and abilities to perform preparation, detection and analysis, containment, eradication, and recovery procedures; • incident monitoring mechanisms maintain records about each incident, the status of the incident, and other pertinent	NIST SP 800-53, IR-2 NIST SP 800-53, IR-3 NIST SP 800-53, IR-4 NIST SP 800-53, IR-5 NIST SP 800-53, IR-6 NIST SP 800-53, IR-7 NIST SP 800-53, PE-20 NIST SP 800-53, PM-15 NIST SP 800-53, SC-5 NIST SP 800-53, SC-6 NIST SP 800-53, SC-26 NIST SP 800-53, SC-30 NIST SP 800-53, SC-40 NIST SP 800-53, SC-42 NIST SP 800-53, SC-44 NIST SP 800-53, SC-48 NIST SP 800-53, SR-8 NIST SP 800-53, SI-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• a process for gathering forensic evidence and conducting forensic analysis; • links to other relevant security and privacy groups and associations; • monitoring, generating, and disseminating security alerts, advisories, and directives, as applicable; and • protection against denial-of-service attacks. *Related controls: SM.02.03.01 and SM.02.03.02*	information necessary for forensic analysis, as well as the evaluation of incident details, trends, and handling activities; • incidents are reported in accordance with applicable statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, and guidelines, as well as whether incident information is used to inform risk assessments or control assessments; • incident response support resources are adequate; • forensic evidence is gathered and forensic analysis is performed when appropriate; • there are links to other relevant security and privacy groups and associations; • security alerts, advisories, and directives are monitored, generated, and disseminated, as applicable; • techniques are employed to prevent adversarial attacks based on risks; and • denial-of-service attacks can be limited or eliminated. Inspect the results of the entity's incident response testing. Consider whether tests of the entity's incident response capabilities were coordinated with business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, and other relevant plans, as applicable. Consider whether appropriate follow-up was performed for potential findings, weaknesses, or deficiencies related to the entity's incident response capabilities. Inspect available documentation for a selection of incident records for incidents that occurred during the audit period and verify whether the incidents were tracked and documented in accordance with the entity's policies and procedures. Also, determine whether any associated forensic analysis or reporting was performed as appropriate. Consider whether adequate information was available for the entity to perform appropriate forensic analysis.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the incident response program is implemented in accordance with the entity's incident response plan and includes required elements in accordance with authoritative criteria.	
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.01.06.01 An entity-level inventory of major information systems (i.e., all major applications and general support systems) is developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level inventory of major information systems through • inquiry of appropriate personnel and • inspection of relevant documentation, including management's criteria for designating information systems as major information systems. Inspect the entity-level inventory of major information systems. Consider whether • the information systems relevant to the significant business processes are appropriately included in the inventory; • management's criteria for designating information systems as major information systems are suitable and consistently applied; and • the inventory has been recently reviewed and updated and is complete. Determine whether the entity-level inventory of major information systems has been appropriately documented, periodically reviewed and updated, and properly approved.	NIST SP 800-53, PM-5
SM.01.06.02 An entity-level process for selecting and implementing security controls for major applications and general support systems that satisfies minimum security requirements for information and information systems is established and implemented.	Obtain an understanding of the entity-level process for selecting and implementing security controls for major applications and general support systems through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and	NIST SP 800-53, PL-10 NIST SP 800-53, PL-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related control: SM.04.02.01	• inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the control baseline for each of the information systems relevant to the significant business processes. Consider whether each control baseline has been selected and tailored based on • the impact level of the corresponding system and • the entity-level process for selecting and implementing security controls. Determine whether the entity-level process for selecting and implementing security controls is effectively designed and implemented to reasonably assure that minimum security requirements for information and information systems are satisfied. Throughout the engagement, determine whether the security controls included in the control baselines for relevant information systems are designed, implemented, and operating effectively. Note: Control baselines are predefined sets of controls that represent a starting point for the protection of information and information systems. Subsequent tailoring of selected control baselines allows for management of risk in accordance with mission, business, or other constraints. Federal information system control baselines are provided in NIST SP 800-53B, which states that its security and privacy control baselines are based on the requirements in the Federal Information Security Modernization Act of 2014 (FISMA, Public Law 113-283) and the Privacy Act of 1974 (codified, as amended, at 5 U.S.C. § 552a) (PRIVACT). To prepare for selecting and tailoring the appropriate control baseline for an information system and its respective environment of operation, the entity first determines the criticality and sensitivity of the information the system is to process, store, or transmit. The process of determining information criticality and sensitivity is known as security	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	categorization and is described in FIPS 199. Security categorization of federal information and information systems, as required by FIPS 199, is the first step in the risk management process. Subsequent to the security categorization process, entities select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in FIPS 200. Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular system, the high water mark concept introduced in FIPS 199 is used in FIPS 200 to determine the system's impact level. The impact level, in turn, is used to select the applicable control baseline. Thus, a low-impact system is defined as a system in which all three of the security objectives are low. A moderate-impact system is a system in which at least one of the security objectives is moderate and no security objective is high. Finally, a high-impact system is a system in which at least one security objective is high.	
SM.01.06.03 System-level concept of operations (CONOPS) documents that describe the operation of the information system from the perspective of information security and privacy are developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level CONOPS documents through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the system-level CONOPS documents for each of the information systems relevant to the significant business processes. Consider whether CONOPS documents • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and • are adequate to describe the operation of the information systems from the perspective of information security and privacy.	NIST SP 800-53, PL-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the system-level CONOPS documents for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.	
SM.01.06.04 System-level security and privacy architectures that are consistent with the enterprise architecture and are integrated with the risk management and system development life cycle processes are developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level security and privacy architectures through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the system-level security and privacy architectures for each of the information systems relevant to the significant business processes. Consider whether the security and privacy architectures • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); • are consistent with the enterprise architecture; • are integrated with the risk management and system development life cycle processes; and • are adequate to describe the structure and behavior for the system's security and privacy processes. Determine whether the system-level security and privacy architectures for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, determine whether the system-level security and privacy architectures for relevant information systems have been implemented. Note: A security architecture is a set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected. The system-level security and	NIST SP 800-53, PL-8 NIST SP 800-53, PM-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	privacy architectures describe the structure and behavior for a system's security and privacy processes.	
SM.01.06.05 System security and privacy plans for each major information system included in the systems inventory are developed, documented, and periodically reviewed and updated. *Related control: BP.04.01.01, BP.04.01.02, BP.05.01.01, BP.05.01.02, BP.06.01.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, and SM.04.02.01*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system security and privacy plans for each major information system through • inquiry of appropriate personnel and • inspection of relevant documentation, including the entity-level inventory of major information systems. Inspect the system security and privacy plans for each of the information systems relevant to the significant business processes. Consider whether the plans • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); • include required information in accordance with authoritative criteria; and • are adequate to provide an overview of the security and privacy requirements for the system and describe the controls designed and implemented to satisfy such requirements. Determine whether the system security and privacy plans for relevant information systems are effectively designed and have been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, determine whether the system security and privacy plans for relevant information systems have been implemented. Note: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The	NIST SP 800-53, AC-14 NIST SP 800-53, PL-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	plans describe the intended application of each selected control in the context of the system in sufficient detail to allow for correctly implementing the control and to subsequently assessing the effectiveness of the control. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle. Updates to system security and privacy plans are made to address changes to the system and environment of operation or deficiencies identified through control assessments. The auditor may use system security and privacy plans to obtain an understanding of an information system's components, security categorization, impact level, operational environment, control dependencies, system interconnections, security and privacy requirements, and the individuals who fulfill system roles and responsibilities.	
SM.01.06.06 System-level supply chain risk management plans for information systems are developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level supply chain risk management plans for information systems through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the system-level supply chain risk management plan for each of the information systems relevant to the significant business processes. Consider whether the plans • have been recently reviewed and updated, as appropriate; • include required information in accordance with authoritative criteria; and • are adequate to identify, assess, and manage supply chain risks relevant to the system. Determine whether the system-level supply chain risk management plans for relevant information systems re effectively designed, have	NIST SP 800-53, SR-2 NIST SP 800-53, SR-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	been appropriately documented, and are periodically reviewed and updated. Throughout the engagement, determine whether the system-level supply chain risk management plans for relevant information systems have been implemented. Note: System-level supply chain risk management plans can be stand-alone plans or part of system security and privacy plans.	
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.		
SM.02.01.01 A security and privacy workforce development and improvement program is established and documented. *Related controls: SM.02.03.01 and SM.02.03.02*	Obtain an understanding of the entity's security and privacy workforce development and improvement program through • inquiry of appropriate personnel and • inspection of relevant documentation. Determine whether a security and privacy workforce development and improvement program has been established and documented.	NIST SP 800-53, PM-13
SM.02.01.02 Information security and privacy roles and responsibilities, as well as position risk designation, are included in position descriptions.	Inspect a selection of position descriptions for senior management, information resource owners, IT management personnel, and security administrators. Determine whether the information security and privacy roles and responsibilities, as well as position risk designation, are accurately identified and included in position descriptions. Note: Position risk designations reflect the degree of potential damage that could occur from the misconduct of an incumbent of a position. Position risk designations inform the nature, extent, and timing of the entity's screening activities.	NIST SP 800-53, PS-2 NIST SP 800-53, PS-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.02.01.03 Incompatible duties are included in position descriptions. *Related controls: SD.01.01.01 and SD.01.01.02*	Inspect a selection of position descriptions for senior management, information resource owners, IT management personnel, and security administrators. Determine whether incompatible duties are accurately identified and included in position descriptions.	NIST SP 800-53, AC-5
SM.02.02 Screening activities are completed and access agreements are signed prior to access authorization.		
SM.02.02.01 References for prospective employees are contacted and background investigations and agency checks are performed based on position risk designations.	Obtain an understanding of the entity's processes and methods for contacting references for prospective employees and performing background investigations and agency checks through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect relevant documentation for a selection of recently hired IT management personnel to verify that references have been contacted and background investigations and agency checks have been performed in accordance with the entity's policies and procedures. Determine whether references for prospective employees are contacted and background investigations and agency checks are properly performed based on position risk designations. Note: Position risk designations inform the nature, extent, and timing of screening activities performed by the entity, including contacting references and performing background investigations and agency checks.	NIST SP 800-53, PS-2 NIST SP 800-53, PS-3 NIST SP 800-53, SA-21
SM.02.02.02 Rescreening activities, including periodic reinvestigations, are performed based on position risk designations as	Obtain an understanding of the entity's processes and methods for performing rescreening activities, including periodic reinvestigations, through	NIST SP 800-53, PS-2 NIST SP 800-53, PS-3 NIST SP 800-53, SA-21

Illustrative control activities	Illustrative audit procedures	Relevant criteria
required by applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria.	• inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect relevant documentation for a selection of IT management personnel to verify that rescreening activities, including periodic reinvestigations, have been performed in accordance with the entity's policies and procedures. Determine whether rescreening activities, including periodic reinvestigations, are performed based on position risk designations as required by applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria.	
SM.02.02.03 Individuals sign access agreements prior to being granted access to information and information systems. *Related controls: AC.02.03.03 and SM.02.03.03*	Obtain an understanding of the entity's process and methods for obtaining signed access agreements from individuals through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect available documentation for a selection of accounts that were created during the audit period. Determine whether the entity obtains signed access agreements prior to granting access to information and information systems. Note: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.	NIST SP 800-53, CM-10 NIST SP 800-53, CM-11 NIST SP 800-53, MP-7 NIST SP 800-53, PL-4 NIST SP 800-53, PS-6
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.02.03.01 An information security and privacy literacy training and awareness	Obtain an understanding of the entity's processes and methods for establishing, documenting, and periodically reviewing and updating	NIST SP 800-53, AT-2 NIST SP 800-53, AT-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
program that incorporates lessons learned from internal or external security incidents or breaches and awareness techniques is established, documented, and periodically reviewed and updated. The completion status of applicable mandatory training courses for information system users is monitored. *Related controls: BP.04.03.12, SM.02.01.01, and SM.02.03.02*	information security and privacy literacy training and awareness techniques through • inquiry of appropriate personnel, including any senior officials responsible for the information security and privacy literacy training and awareness program, and • inspection of relevant documentation, such as literacy training course materials demonstrating the incorporation of lessons learned from internal or external security incidents or breaches. Inspect documentation for the information security and privacy literacy training and awareness program. Consider whether • training course materials are consistent with information system user roles and responsibilities and the content has been reviewed and updated when required because of system changes and at an appropriate frequency; • lessons learned from internal or external security incidents or breaches are incorporated into literacy training course materials and awareness techniques; • mandatory training courses are identified and communicated to information system users as a condition of system access, as applicable; and • management monitors and maintains records of the completion status of applicable mandatory training courses for information system users. Determine whether the information security and privacy literacy training and awareness program is effectively designed, appropriately documented, and periodically reviewed and updated and user attendance and completion are monitored. Throughout the engagement, determine whether the information security and privacy literacy training and awareness program has been implemented.	NIST SP 800-53, PM-14

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.02.03.02 A role-based information security and privacy training program that incorporates lessons learned from internal or external security incidents or breaches is established, documented, and periodically reviewed and updated. The completion status of applicable mandatory training courses for information system users is monitored. *Related controls: BP.04.03.12, SM.02.01.01, and SM.02.03.01*	Obtain an understanding of the entity's processes and methods for establishing, documenting, and periodically reviewing and updating role-based information security and privacy training through • inquiry of appropriate personnel, including any senior officials responsible for the role-based information security and privacy training program, and • inspection of relevant documentation, such as role-based training course materials demonstrating the incorporation of lessons learned from internal or external security incidents or breaches. Inspect documentation for the role-based information security and privacy training program. Consider whether • training course materials are consistent with information system user roles and responsibilities and the content has been reviewed and updated when required by system changes and at an appropriate frequency; • lessons learned from internal or external security incidents or breaches are incorporated into role-based training content; • mandatory training courses are identified and communicated to information system users as a condition of system or role-based access, as applicable; and • management monitors and maintains records of the completion status of applicable mandatory training courses for information system users. Determine whether the role-based information security and privacy training program is effectively designed, appropriately documented, and periodically reviewed and updated and user attendance and completion are monitored. Throughout the engagement, determine whether the role-based information security and privacy training program has been implemented.	NIST SP 800-53, AT-3 NIST SP 800-53, AT-4 NIST SP 800-53, PM-14

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.02.03.03 Current rules that describe the responsibilities and expected behavior for information and information system usage, security, and privacy have been acknowledged in writing by individuals prior to their being granted access to information and information systems. *Related controls: BP.04.03.12, AC.02.03.03, and SM.02.02.03*	Obtain an understanding of the entity's processes and methods for obtaining written acknowledgment of rules and expected behavior from individuals who access information and information systems through • inquiry of appropriate personnel, including information system users, and • inspection of relevant documentation, including access agreements. Inspect available documentation for a selection of accounts that were created during the audit period. Determine whether current rules that describe the responsibilities and expected behavior for information and information system usage, security, and privacy have been acknowledged in writing by individuals prior to their being granted access to information and information systems.	NIST SP 800-53, CM-10 NIST SP 800-53, CM-11 NIST SP 800-53, MP-7 NIST SP 800-53, PL-4 NIST SP 800-53, PS-6
SM.02.04 Training activities are documented, monitored, retained, and evaluated.		
SM.02.04.01 Employee training records are documented, monitored, and retained.	Obtain an understanding of the entity's processes and methods for documenting, monitoring, and retaining employee training records through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect relevant documentation for a selection of IT management personnel to verify that employee training records have been documented, monitored, and retained in accordance with the entity's policies and procedures.	NIST SP 800-53, AT-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether employee training records are appropriately documented, monitored, and retained.	
SM.02.04.02 Results of employee training are evaluated by appropriate personnel and appropriate actions are taken.	Obtain an understanding of the entity's processes and methods for evaluating the results of employee training and taking appropriate action through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect relevant documentation for a selection of training courses, such as information security and privacy literacy training or role-based information security and privacy training. Consider whether • results of employee training, including employee feedback, are retained and evaluated by personnel with the authority to take or delegate appropriate actions, and • actions, such as updates to course materials or instruction methods, are taken in response to evaluations of training, as appropriate. Determine whether the results of employee training are evaluated by appropriate personnel and appropriate actions are taken.	NIST SP 800-53, AT-6
SM.02.05 Transfer and termination activities are completed on a timely basis.		
SM.02.05.01 Where appropriate, the following transfer and termination activities are completed on a timely basis: • review ongoing need for logical and physical access authorizations;	Obtain an understanding of the entity's processes and methods for completing transfer and termination activities through • inquiry of appropriate personnel and • inspection of relevant documentation.	NIST SP 800-53, PS-4 NIST SP 800-53, PS-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• modify, disable, or remove accounts when associated access privileges or accounts are no longer needed; • collect property, equipment, and physical access authorization credentials; • conduct exit interviews; • escort terminated employees out of the entity's facilities; and • identify the period during which nondisclosure requirements remain in effect for terminated employees. *Related control: AC.02.03.04*	Inspect relevant documentation for a selection of recently transferred or terminated IT management personnel to verify that appropriate transfer and termination activities were completed on a timely basis. Consider whether • logical and physical access authorizations for transferred personnel were reviewed to determine whether an ongoing need for such access exists; • accounts were timely modified, disabled, or removed when associated access privileges or accounts are no longer needed due to transfer or termination; • property, equipment, and physical access authorization credentials were timely collected; • exit interviews were conducted; • terminated employees were escorted out of the entity's facilities; and • the period during which nondisclosure requirements remain in effect was identified for terminated employees. Inspect a system-generated list of enabled user accounts and a list of terminated personnel to verify that user accounts for terminated personnel have been promptly disabled after the termination date. Consider the completeness and accuracy of the documentation obtained, including any system-generated listings, when determining whether accounts are timely modified, disabled, or removed in accordance with the entity's policies and procedures. Determine whether appropriate transfer and termination activities are completed on a timely basis.	
SM.03 Management holds individuals and external entities 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.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.03.01.01 A formal sanctions process for individuals failing to comply with information security and privacy policies and procedures is employed.	Obtain an understanding of the entity's formal sanctions process and methods for individuals failing to comply with information security and privacy policies and procedures through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in to assessing the adequacy of policies and procedures. Inspect relevant documentation for a selection of IT management personnel who have recently been subject to the entity's formal sanctions process. Determine whether the entity's formal sanctions process and methods for individuals failing to comply with information security and privacy policies and procedures are appropriately employed.	NIST SP 800-53, PS-8
SM.03.02 External entities are held accountable for their assigned internal control responsibilities related to the entity's information security and privacy objectives.		
SM.03.02.01 The terms and conditions for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems are developed; documented; and periodically reviewed, updated, and approved. *Related controls: BP.05.03.01, AC.01.01.01, and AC.05.02.05*	Obtain an understanding of the entity's processes and methods for developing, documenting, periodically reviewing and updating, and approving the terms and conditions for protecting controlled unclassified information that is processed, stored, or transmitted on external systems through • inquiry of appropriate personnel and • inspection of relevant documentation, such as interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, or other exchange agreements. Inspect the interconnection security agreements, information exchange security agreements, memorandums of understanding or	NIST SP 800-53, AC-20 NIST SP 800-53, AC-21 NIST SP 800-53, CA-3 NIST SP 800-53, PM-17 NIST SP 800-53, PS-7 NIST SP 800-53, SA-4 NIST SP 800-53, SA-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	agreement, service-level agreements, user agreements, nondisclosure agreements, or other exchange agreements for the information systems relevant to the significant business processes. Consider whether such documentation • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); and • is adequate to reasonably assure the protection of controlled unclassified information that is processed, stored, or transmitted on external systems. Inspect the contracts executed between the entity and external entities for the acquisition of information systems, information system components, or information system services. Consider whether the contracts include, either explicitly or by reference to an exchange agreement, the following requirements, descriptions, and criteria: • security and privacy functional requirements and related controls; • strength of mechanism requirements; • security and privacy assurance requirements; • security and privacy documentation requirements and related controls; • descriptions of the system development environment and the environment in which the system is intended to operate; • roles and responsibilities for information security, privacy, and supply chain risk management; and • acceptance criteria. Determine whether the terms and conditions for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems have been appropriately documented, periodically reviewed and updated, and properly approved.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Throughout the engagement, determine whether the terms and conditions for the protection of controlled unclassified information have been implemented. Note: Entities may incorporate provisions related to exchange agreements into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Exchange agreements are also used to facilitate the exchange of information within the entity, as information exchange requirements apply to exchanges between two or more systems.	
SM.03.02.02 An entity-level process for assessing the effectiveness of information security and privacy controls that external entities design, implement, or operate is established and implemented. *Related control: SM.03.03.01*	Obtain an understanding of the entity-level process for assessing the effectiveness of information security and privacy controls that external entities design, implement, or operate through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, • inspection of relevant service organization reports, and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Through inquiry, inspection, and observation, identify information system controls relevant to the significant business processes and areas of audit interest that external entities design, implement, or operate. Consider the control baseline for each of the information systems relevant to the significant business processes when identifying such controls. See also SM.01.05.01. Inspect relevant documentation related to the entity's assessment of information security and privacy controls designed, implemented, and operated by external entities. Consider whether the entity's assessment	NIST SP 800-53, CA-1 NIST SP 800-53, CA-6 NIST SP 800-53, PS-7 NIST SP 800-53, SA-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• is based on current information; • addresses any controls the entity designs, implements, or operates that are necessary to achieve the external entities' control objectives; and • is adequate to support the entity's conclusions on the effectiveness of information security and privacy controls that external entities design, implement, or operate. Determine whether the entity-level process for assessing the effectiveness of information security and privacy controls that external entities design, implement, or operate is effectively designed and implemented to achieve the entity's information security and privacy objectives and hold external entities accountable for their assigned internal control responsibilities. Throughout the engagement, determine whether information system controls relevant to the significant business processes and areas of audit interest that external entities design, implement, or operate are effective. See also section 330 for guidance on using service organization reports. Note: Entity management may engage external parties, referred to as service organizations, to perform certain operational processes, including designing, implementing, and operating related information security and privacy controls. However, management retains responsibility for processes assigned to service organizations. Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned operational processes and how the service organization's internal control system affects the entity's internal control system. Management retains responsibility for monitoring the effectiveness of internal control over the assigned processes that service organizations perform and holds service organizations accountable for their	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	assigned internal control responsibilities. Management uses ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of the service organization's internal controls over the assigned processes. Monitoring activities related to service organizations may include the use of work performed by external parties, such as service auditors, and reviewed by management. Additionally, if controls that service organizations perform are necessary for the entity to achieve its objectives and address risks related to the assigned operational process, the entity's internal controls may include complementary user-entity controls that the service organization or its auditors identified that are necessary to achieve the service organization's control objectives.	
SM.03.02.03 An interorganizational joint authorization process for systems with multiple authorizing officials and at least one authorizing official from an external entity may be implemented for connected systems, shared systems or services, and systems with multiple information owners.	If applicable, obtain an understanding of the entity's interorganizational joint authorization process and methods for systems with multiple authorizing officials and at least one authorizing official from an external entity through • inquiry of appropriate personnel, such as authorizing officials and information system owners; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. See also SM.05.02.01, SM.05.02.02, and SM.05.02.03. If applicable, determine whether the interorganizational joint authorization process for systems with multiple authorizing officials and at least one authorizing official from an external entity is effectively designed and implemented to achieve the entity's information security and privacy objectives and hold external entities accountable for their assigned internal control responsibilities.	NIST SP 800-53, CA-6 NIST SP 800-53, SA-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.03.03 Complementary user-entity controls related to external entities are identified, implemented, and operating effectively.		
SM.03.03.01 Complementary user-entity controls related to external entities are identified, implemented, and operating effectively. *Related control: SM.03.02.02*	Obtain an understanding of the entity's processes and methods for identifying, implementing, and testing complementary user-entity controls through • inquiry of appropriate personnel • inspection of relevant policies and procedures and • inspection of other relevant documentation, such as service organization reports and internal control testing results. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether management identified all relevant complementary user-entity controls from the external entity's service organization reports, and consider whether the corresponding controls have been implemented. Consider whether the management has appropriate procedures in place to periodically test the effectiveness of relevant complementary user entity controls. Perform tests of effectiveness over relevant complementary user entity controls, as appropriate. Inspect the external entity's service organization report and consider whether relevant controls at the external entity are appropriately designed, implemented, and operating effectively. Determine whether the complementary user-entity controls related to external entities are identified, implemented, and operating effectively. Note: Complementary user-entity controls are controls that management of the service organization assumes, in the design of its service, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the service organization's system.	NIST 800-53, SA-9
SM.04 Management identifies, analyzes, and responds to risks, including fraud risk, and significant changes related to the entity's information security management program.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.04.01 Risk management strategies are developed, documented, and maintained.		
SM.04.01.01 An entity-level risk management strategy for information security and privacy risks is developed, documented, and periodically reviewed and updated. To guide and inform risk-based decisions, the strategy includes determination of assumptions and constraints affecting entity risk assessments, organizational risk tolerance, and entity-level priorities. *Related controls: SM.01.05.01, CM.03.01.01, and CM.03.02.01*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level risk management strategy for information security and privacy risks through • inquiry of appropriate personnel, including the senior officials responsible for the strategy, and • inspection of relevant documentation. • Inspect the entity-level risk management strategy for information security and privacy risks. Consider whether the strategy • has been recently reviewed and updated, as appropriate; • includes required information in accordance with authoritative criteria; • demonstrates the entity has determined assumptions and constraints affecting risk assessments, organizational risk tolerance, and priorities to guide and inform risk-based decisions; and • is adequate for prioritizing the entity's implementation of activities to assess, respond to, and monitor information security and privacy risks, including physical and environmental hazards. Determine whether the entity-level risk management strategy for information security and privacy risks is effectively designed, has been appropriately documented, and is periodically reviewed and updated. Throughout the engagement, determine whether the entity-level risk management strategy has been implemented.	NIST SP 800-53, PE-23 NIST SP 800-53, PM-9 NIST SP 800-53, PM-10 NIST SP 800-53, PM-12 NIST SP 800-53, PM-16 NIST SP 800-53, PM-28
SM.04.01.02 An entity-level continuous monitoring strategy that establishes the metrics, frequency, and type(s) of control	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level continuous monitoring strategy through	NIST SP 800-53, PM-14 NIST SP 800-53, PM-31

Illustrative control activities	Illustrative audit procedures	Relevant criteria
assessments and monitoring, as well as the process for correlating, analyzing, and responding to control assessment and monitoring results, is developed, documented, and periodically reviewed and updated. *Related controls: SM.06.01.01, CM.03.01.01, and CM.03.02.01*	• inquiry of appropriate personnel, including the senior officials responsible for the strategy, and • inspection of relevant documentation. Inspect the entity-level continuous monitoring strategy. Consider whether the strategy • has been recently reviewed and updated, as appropriate; • includes required information in accordance with authoritative criteria; • establishes the metrics, frequency, and type(s) of control assessments and the monitoring to be performed; • defines the process for correlating, analyzing, and responding to control assessment and monitoring results; and • is adequate for prioritizing the entity implementing activities that facilitate ongoing awareness of the security and privacy posture across the entity and for supporting entity risk management decisions. Determine whether the entity-level continuous monitoring strategy is effectively designed, has been appropriately documented, and is periodically reviewed and updated. Throughout the engagement, determine whether the entity-level continuous monitoring strategy has been implemented.	
SM.04.01.03 An entity-level supply chain risk management strategy is developed, documented, and periodically reviewed and updated. The strategy should manage risks associated with developing, acquiring, maintaining, and disposing of systems, system components, and system services.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the entity-level supply chain risk management strategy through • inquiry of appropriate personnel, including the senior officials responsible for the strategy, and • inspection of relevant documentation. Inspect the entity-level supply chain risk management strategy. Consider whether the plan • has been recently reviewed and updated, as appropriate;	NIST SP 800-53, PM-30 NIST SP 800-53, SR-3 NIST SP 800-53, SR-4 NIST SP 800-53, SR-5 NIST SP 800-53, SR-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• is aligned with the entity-level risk management strategy for information security and privacy risks; • includes required information in accordance with authoritative criteria; • addresses the development, acquisition, maintenance, and disposal of systems, system components, and system services; and • is adequate for prioritizing the entity's implementation of activities to assess, respond to, and monitor supply chain risks. Determine whether the entity-level supply chain risk management strategy is effectively designed, has been appropriately documented, and is periodically reviewed and updated. Throughout the engagement, determine whether the entity-level supply chain risk management strategy has been implemented.	
SM.04.02 Risk identification, analysis, and response activities are conducted.		
SM.04.02.01 Security categorization of the information system and the information it processes, stores, and transmits has been completed based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals. The security categorization has been documented and approved. *Related controls: SM.01.05.01 and SM.01.05.04*	Obtain an understanding of the entity's process and methods for categorizing information systems and the information processed, stored, and transmitted by such systems through • inquiry of appropriate personnel, including authorizing officials responsible for approving security categorization decisions; • inspection of relevant documentation, including system security and privacy plans; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.	NIST SP 800-53, RA-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect the system security and privacy plans for each of the information systems relevant to the significant business processes. Consider whether the plans • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and • provide an adequate supporting rationale for the security categorization of the information system, based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals. Determine whether the security categorization for each of the relevant information systems flows logically from the supporting rationale documented within the respective system security and privacy plan.	
SM.04.02.02 Risk assessments are conducted and documented to • identify threats to and vulnerabilities in the system; • determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and • determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information. *Related controls: SM.04.02.03, SM.04.02.04, SM.04.02.05*	Obtain an understanding of the entity's processes and methods for conducting and documenting risk assessments through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of other relevant documentation, including risk assessments relevant to the significant business processes and areas of audit interest that demonstrate the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the risk assessments relevant to the significant business processes and areas of audit interest, including any risk assessments conducted and documented for the information systems relevant to the significant business processes. Consider whether the risk assessments • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s);	NIST SP 800-53, RA-3 NIST SP 800-53, RA-6 NIST SP 800-53, RA-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• identify threats to and vulnerabilities in the respective systems; • determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the respective systems, as well as the information processed, stored, or transmitted by such systems; and • determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information. Determine whether the entity's processes and methods for conducting and documenting risk assessments are effectively designed and implemented to reasonably assure that risks are properly identified and analyzed. Determine whether the risk assessments relevant to the significant business processes and areas of audit interest have been conducted and documented in accordance with the entity's policies and procedures. Note: Risk assessments may be documented within risk assessment reports, security and privacy plans, or other entity-defined documents detailing the results of entity risk assessments. Reviewing the results of entity risk assessments may be useful in assessing risk and determining the nature, extent, and timing of further audit procedures.	
SM.04.02.03 Vulnerability scan reports and results from vulnerability monitoring inform the entity's risk assessment process. The results of penetration testing, when conducted, also inform the entity's risk assessment process. *Related controls: SM.04.02.02 and CM.05.01.01*	Inspect risk assessment reports, security and privacy plans, or other entity-defined documents detailing the results of risk assessments conducted and documented for the information systems relevant to the significant business processes. Determine whether applicable vulnerability scan reports and results from vulnerability monitoring, as well as results of penetration testing, have been appropriately considered as part of the risk assessments conducted and documented for relevant information systems.	NIST SP 800-53, CA-8 NIST SP 800-53, RA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.04.02.04 Risk assessment results, including validation and mitigation, are documented, analyzed, and approved by management. *Related controls: SM.04.02.03 and SM.04.02.06*	Obtain an understanding of the entity's processes and methods for analyzing and responding to risks through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of other relevant documentation, including risk response documentation, demonstrating the design and implementation of the process. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect risk response documentation for the risk assessments relevant to the significant business processes and areas of audit interest, including any risk assessments conducted and documented for the information systems relevant to the significant business processes. Consider whether the risk response documentation • has been approved by the appropriate senior official(s) and • is adequate to demonstrate that risks identified through the risk assessment process have been appropriately analyzed as part of the risk response process. Determine whether the entity's processes and methods for analyzing and responding to risks are effectively designed and implemented to reasonably assure that risks are properly validated and mitigated. Determine whether the risk response documentation for the risk assessments relevant to the significant business processes and areas of audit interest has been prepared in accordance with the entity's policies and procedures.	NIST SP 800-53, RA-3 NIST SP 800-53, RA-7
SM.04.02.05 Risks are reassessed periodically or to address changes to the system, its environment of operation, or other conditions that may affect the security or privacy state of the system.	Inspect risk assessment reports, security and privacy plans, or other entity-defined documents detailing the results of risk assessments conducted and documented for the information systems relevant to the significant business processes.	NIST SP 800-53, RA-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related control: SM.04.02.02	Determine whether risks are reassessed periodically or to address changes to relevant information systems, the system's environments of operation, or other conditions that may affect the security or privacy state of the systems. Determine whether the frequency of the entity's reassessment of risks is appropriate.	
SM.04.02.06 Findings from risk assessments, security and privacy assessments, monitoring activities, and audits are addressed within appropriate time frames in accordance with organizational risk tolerance. *Related control: SM.04.02.04*	Inspect documentation detailing the status of actions taken or in progress to address findings from risk assessments, security and privacy assessments, monitoring activities, and audits, which are relevant to the significant business processes and areas of audit interest. Determine whether relevant findings from risk assessments, security and privacy assessments, monitoring activities, and audits are addressed within appropriate time frames in accordance with organizational risk tolerance.	NIST SP 800-53, RA-7
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.05.01.01 Management develops, documents, and periodically reviews and updates information security and privacy policies and procedures. These policies and procedures are implemented at the entity-level and system-level and are approved by management. They also appropriately • consider risk; • address purpose, scope, roles, responsibilities, coordination among business or organizational units as	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating entity-level and system-level information security and privacy policies and procedures through • inquiry of appropriate personnel and • inspection of relevant documentation, including the entity's policies and procedures relevant to the significant business processes and areas of audit interest. Throughout the engagement, determine whether the entity's processes and methods for developing, documenting, and periodically reviewing and updating entity-level and system-level information	NIST SP 800-53, AC-1 NIST SP 800-53, AT-1 NIST SP 800-53, AU-1 NIST SP 800-53, CA-1 NIST SP 800-53, CM-1 NIST SP 800-53, CP-1 NIST SP 800-53, IA-1 NIST SP 800-53, IR-1 NIST SP 800-53, MA-1 NIST SP 800-53, MP-1

Illustrative control activities	Illustrative audit procedures	Relevant criteria
well as external entities, and compliance; • describe the process; • consider information system general and application controls; • consider segregation of duties controls; and • ensure that users can be held accountable for their actions. Note: Information security and privacy policies and procedures may be applicable across multiple FISCAM control categories—business process controls, security management, access controls, segregation of duties, configuration management, and contingency planning.	security and privacy policies and procedures are designed, implemented, and operating effectively. Through inquiry, inspection, and observation, identify information system controls relevant to the significant business processes and areas of audit interest. Throughout the engagement, determine whether the entity's policies and procedures for the application of information system controls are designed, implemented, and operating effectively. Consider whether • policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external entities, and compliance; • procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be held accountable for their actions, and appropriately consider information system general and application controls and segregation of duties controls; and • policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity's internal control objectives. Note: The auditor performs audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its entity-level and system-level information security and privacy policies and procedures. Such assessment is intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of information system controls relevant to the significant business processes and the information systems that support them. When effectively designed, the entity's information security and privacy policies and procedures, as well as policies and procedures applicable to the significant business processes, provide suitable criteria for evaluating evidence regarding	NIST SP 800-53, PE-1 NIST SP 800-53, PL-1 NIST SP 800-53, PM-1 NIST SP 800-53, PS-1 NIST SP 800-53, PT-1 NIST SP 800-53, RA-1 NIST SP 800-53, SA-1 NIST SP 800-53, SC-1 NIST SP 800-53, SI-1 NIST SP 800-53, SR-1

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	the implementation and operating effectiveness of information system controls.	
SM.05.02 Information systems are authorized to operate.		
SM.05.02.01 Common controls are authorized for inheritance before commencing operations and are reauthorized on a periodic basis thereafter. *Related control: SM.01.02.02*	Obtain an understanding of the entity's processes and methods for authorizing and periodically reauthorizing common controls for inheritance through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; • inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the information systems relevant to the significant business processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the authorization packages for each of relevant information systems. Consider whether • the information contained in the authorization package is updated on an ongoing basis through comprehensive continuous monitoring activities, • authorization decisions flow logically from the supporting rationale documented within the authorization package, • authorization decisions are made on a timely basis in accordance with the entity-defined frequency, and • the entity-defined frequency for reauthorizations is appropriate. Determine whether the authorizing official(s) for relevant information systems appropriately authorized inherited common controls before commencing operations and has since appropriately reauthorized the inheritance of such controls on a periodic basis.	NIST SP 800-53, CA-6 NIST SP 800-53, PM-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: An authorization package comprises the information that an authorizing official uses to determine whether to authorize the operation of an information system or the provision of a designated set of common controls. At a minimum, the authorization package includes an executive summary, system security and privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.	
SM.05.02.02 The information system is authorized to operate before commencing operations, is authorized to use inherited common controls, and is reauthorized periodically thereafter.	Obtain an understanding of the entity's processes and methods for authorizing and periodically reauthorizing an information system to operate, including the use of inherited common controls, through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the information systems relevant to the significant business processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the authorization packages for each of relevant information systems. Consider whether • the information contained in the authorization package is updated on an ongoing basis through comprehensive continuous monitoring activities, • authorization decisions flow logically from the supporting rationale documented within the authorization package, • authorization decisions are made on a timely basis in accordance with the entity-defined frequency, and • the entity-defined frequency for reauthorizations is appropriate.	NIST SP 800-53, CA-6 NIST SP 800-53, PM-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the authorizing official(s) for relevant information systems appropriately authorized the information system to operate before commencing operations, authorized the information system to use inherited common controls, and has since appropriately reauthorized the information system to operate and use inherited common controls periodically.	
SM.05.02.03 The authorization to operate is documented within an authorization package, which includes an executive summary, system security and privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.	Obtain an understanding of the entity's processes and methods for preparing and assembling authorization packages through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the information systems relevant to the significant business processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the authorization packages for each of relevant information systems. Consider whether each authorization package • includes required information in accordance with authoritative criteria and • is adequately documented to support the authorization decisions expressed therein. Note: Reviewing the authorization packages may be useful in assessing risk and determining the nature, extent, and timing of further audit procedures.	NIST SP 800-53, CA-6
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.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SM.06.01.01 Management develops, documents, and periodically reviews and updates system-level continuous monitoring strategies. Such a strategy establishes the metrics, frequency, and type(s) of control assessments and monitoring, as well as the process for correlating, analyzing, and responding to control assessment and monitoring results, in accordance with the entity-level continuous monitoring strategy. *Related controls: SM.04.01.02, CM.03.01.01, and CM.03.02.01*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level continuous monitoring strategies through • inquiry of appropriate personnel, including the senior official(s) responsible for the strategies, and • inspection of relevant documentation. Inspect the system-level continuous monitoring strategy for each of the information systems relevant to the significant business processes. Consider whether each of the strategies • has been recently reviewed and updated, as appropriate; • is aligned with the entity-level continuous monitoring strategy; • includes required information in accordance with authoritative criteria; • establishes the metrics, frequency, and type(s) of control assessments and monitoring to be performed; • defines the process for correlating, analyzing, and responding to control assessment and monitoring results; and • is adequate for prioritizing the entity's implementation of activities to facilitate ongoing awareness of the security and privacy posture of the information system. Determine whether the system-level continuous monitoring strategy for each of relevant information systems is effectively designed, has been appropriately documented, and is periodically reviewed and updated. Throughout the engagement, determine whether the system-level continuous monitoring strategy for each of relevant information systems has been implemented.	NIST SP 800-53, CA-7 NIST SP 800-53, PM-31
SM.06.01.02 System-level control monitoring activities are implemented in accordance with the system-level continuous monitoring	Obtain an understanding of management's process for performing system-level control monitoring activities to assess controls and identify risks through	NIST SP 800-53, CA-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
strategy to assess controls and identify risks at a frequency sufficient to support risk-based decisions. *Related control: SM.06.01.03*	• inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the process, such as relevant system-level control monitoring documentation, the system-level continuous monitoring strategy, and the entity-level continuous monitoring strategy. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect relevant system-level control monitoring documentation for each of the information systems relevant to the significant business processes. Consider whether • system-level control monitoring activities are implemented in accordance with the system-level continuous monitoring strategy and • system-level control monitoring documentation is adequate to facilitate ongoing awareness of the security and privacy posture of the information system. Determine whether system-level control monitoring activities are implemented in accordance with the system-level continuous monitoring strategy to assess controls and identify risks at a frequency sufficient to support risk-based decisions. Note: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support entity risk management decisions. “Continuous” implies that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. Control monitoring activities may include a combination of ongoing monitoring activities and separate evaluations. The use of separate evaluations includes entity self-assessments, as well as results of audits, examinations, and other independent assessments performed by internal auditors, external	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	auditors, inspectors general, or other assessors. Reviewing system-level control monitoring documentation may be useful in assessing risk and determining the nature, extent, and timing of further audit procedures.	
SM.06.01.03 Assessors with appropriate skills and technical expertise periodically perform security and privacy control assessments. *Related controls: SM.06.01.02 and SM.06.01.04*	Obtain an understanding of the entity's processes and methods for conducting security and privacy control assessments through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the process, such as relevant control assessment plans and reports. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect relevant control assessment plans and reports for each of the information systems relevant to the significant business processes. Consider whether • the security and privacy control assessment was performed recently and used current information, • the control assessment plan was reviewed and approved by the authorizing official prior to conducting the assessment, • the security and privacy control assessment was performed by assessors with appropriate skills and technical expertise, and • the control assessment report is adequate to facilitate communication of the security and privacy posture of the information system. Determine whether security and privacy control assessments for the information system relevant to the significant business processes are properly performed on a periodic basis by assessors with appropriate skills and technical expertise.	NIST SP 800-53, CA-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Security and privacy control assessments may be performed as part of continuous monitoring activities, initial and ongoing system authorizations, federal agencies' annual assessments required by the Federal Information Security Modernization Act of 2014 (FISMA, Public Law 113-283) (codified, in part, at 44 U.S.C. § 3554), system design and development, system security engineering, privacy engineering, and the system development life cycle.	
SM.06.01.04 Control assessment reports are shared with appropriate personnel." These reports document the assessment results in sufficient detail to enable such personnel to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. *Related control: SM.06.01.03*	Inspect relevant control assessment reports for each of the information systems relevant to the significant business processes and inquire with appropriate personnel to obtain an understanding of how control assessment results are documented and shared. Consider whether • the control assessment reports include sufficient detail to enable personnel to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements and • communication mechanisms exist to facilitate the sharing of control assessment reports with appropriate personnel. Determine whether control assessment reports are shared with appropriate personnel and document the assessment results in sufficient detail.	NIST SP 800-53, CA-2
SM.06.01.05 Performance measures and compliance metrics are periodically evaluated and appropriately employed to measure the effectiveness or efficiency of information security and privacy functions.	Obtain an understanding of the entity's processes and methods for evaluating and employing performance measures and compliance metrics for information security and privacy functions through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the process.	NIST SP 800-53, PM-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the performance measures and compliance metrics for information security and privacy functions applicable to the information systems relevant to the significant business processes. Consider whether • the performance measures and compliance metrics are periodically evaluated by entity management and • the performance measures and compliance metrics are appropriately employed by entity management to measure the effectiveness or efficiency of the information security and privacy functions. Determine whether performance measures and compliance metrics are periodically evaluated and appropriately employed to measure the effectiveness or efficiency of information security and privacy functions.	
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.		
SM.07.01.01 Management develops, documents, and periodically reviews and updates plans of action and milestones for remediation of information security, privacy, and supply chain control deficiencies and vulnerabilities identified during control assessments, audits, and continuous monitoring. These plans respond to risk and focus on remediating the root causes of identified deficiencies and vulnerabilities.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating plans of action and milestones through • inquiry of appropriate personnel, including the authorizing officials for information systems relevant to the significant business processes, and • inspection of relevant documentation, including plans of action and milestones included in the authorization packages for relevant information systems. Inspect plans of action and milestones for relevant information systems. Consider whether the plans of action and milestones	NIST SP 800-53, CA-5 NIST SP 800-53, PM-4 NIST SP 800-53, SR-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related controls: SM.07.01.02 and SM.07.01.03	• have been recently reviewed and updated, as appropriate; • are consistent with the entity-level risk management strategy; • respond to risk; • focus on remediating the root causes of identified deficiencies and vulnerabilities; and • are adequate to assign responsibilities and guide the implementation of corrective actions to fully resolve (or substantially mitigate risks associated with) identified deficiencies and vulnerabilities on a timely basis. Determine whether the plans of action and milestones for relevant information systems have been appropriately documented and periodically reviewed and updated. Note: A plan of action and milestones is a document that identifies tasks needing to be accomplished and details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.	
SM.07.01.02 Control deficiencies and vulnerabilities are analyzed in relation to the entire entity and appropriate corrective actions are applied entity-wide. *Related control: SM.07.01.01*	Inspect plans of action and milestones for the information systems relevant to the significant business processes. Inquire with appropriate personnel to obtain an understanding of the entity's processes and methods for analyzing control deficiencies and vulnerabilities to determine whether entity-wide corrective actions should be applied. Consider whether the plans of action and milestones • specify when entity-wide corrective actions are necessary and • are adequate to guide the implementation of entity-wide corrective actions to fully resolve (or substantially mitigate risks associated with) identified deficiencies and vulnerabilities.	NIST SP 800-53, PM-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether control deficiencies and vulnerabilities are adequately analyzed in relation to the entire entity and appropriate corrective actions are applied entity-wide.	
SM.07.01.03 Remediation tasks and milestones are accomplished by scheduled completion dates. *Related control: SM.07.01.01*	Inspect plans of action and milestones for the information systems relevant to the significant business processes and inquire with appropriate personnel to obtain an understanding of how entity management reasonably assures that remediation tasks and milestones are accomplished within scheduled completion dates. Consider whether the plans of action and milestones • have been recently reviewed and updated, as appropriate; • reflect reasonable scheduled completion dates; and • are adequate to demonstrate progress the entity made in accomplishing remediation tasks and milestones to fully resolve (or substantially mitigate risks associated with) identified deficiencies and vulnerabilities on a timely basis. Determine whether remediation tasks and milestones are accomplished by scheduled completion dates.	NIST SP 800-53, CA-5

FISCAM Framework for Access Controls

Table 10. FISCAM framework for access controls.

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.01 Management designs and implements control activities to appropriately protect logical boundaries of information systems in response to risks.		
AC.01.01 Connectivity to information system resources is appropriately controlled.		
AC.01.01.01 System information exchanges, including access paths and control technologies between systems and to internal system resources, are established, documented, periodically reviewed and updated, and approved. *Related controls: BP.05.03.01 and SM.03.02.01*	Obtain an understanding of the entity's processes and methods for establishing, documenting, periodically reviewing and updating, and approving system information exchanges through • inquiry of appropriate personnel, including authorizing officials, network engineers, system developers, and network and system administrators, and • inspection of relevant documentation, such as network maps, system security and privacy plans, and exchange agreements. Inquire of appropriate personnel and inspect network maps to obtain an understanding of relevant network and system topologies, including information system boundaries, system interconnections, and key devices, for the information systems relevant to the significant business processes. Identify the access paths and control technologies relevant to the significant business processes and obtain an understanding of the entity's processes and methods to protect the access paths and control the flow of information. Identify key system information exchanges relevant to the significant business processes. Determine whether key system information exchanges were appropriately established based on risk. Inspect system security and privacy plans, interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, or other	NIST SP 800-53, AC-4 NIST SP 800-53, CA-3 NIST SP 800-53, CA-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	exchange agreements applicable to the key system information exchanges. Consider whether such documentation • has been recently reviewed and updated, as appropriate; • has been approved by appropriate senior official(s); • includes required information in accordance with authoritative criteria; • accurately describes the key system information exchanges; and • is adequate to communicate and reinforce the entity's processes and methods to protect the access paths, control the flow of information, and reasonably assure that connectivity to system resources is appropriately controlled. Determine whether key system information exchanges have been appropriately documented, periodically reviewed and updated, and properly approved. Note: Authorizing officials determine the risk associated with system information exchanges and the controls needed for appropriate risk mitigation. The type of exchange agreement selected is based on factors such as the impact level of the information being exchanged, the relationship between the entities exchanging information, and the level of access to the organizational system granted to users of the other system.	
AC.01.01.02 Networks are appropriately structured and network components are properly configured to protect access paths within and between systems. *Related control: CM.01.04.01*	Obtain an understanding of the entity's processes and methods for structuring networks and configuring network components through • inquiry of appropriate personnel, including network engineers, system developers, and network and system administrators; • inspection of relevant policies and procedures; and • inspection of other relevant documentation demonstrating the design and implementation of the processes.	NIST SP 800-53, AC-4 NIST SP 800-53, SC-7 NIST SP 800-53, SC-37 NIST SP 800-53, SC-46 NIST SP 800-53, SC-49 NIST SP 800-53, SC-50

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inquire of appropriate personnel and inspect network maps to obtain an understanding of relevant network and system topologies, including information system boundaries, system interconnections, and key devices, for the information systems relevant to the significant business processes. Identify the access paths and control technologies relevant to the significant business processes and obtain an understanding of the entity's processes and methods to protect the access paths and control the flow of information. Identify key network components for controlling the flow of information relevant to the significant business processes. Determine whether networks are appropriately structured and network components are properly configured to protect access paths within and between relevant information systems.	
AC.01.01.03 The system uniquely identifies and authenticates devices before establishing connections.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to uniquely identify and authenticate devices before establishing a connection through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to uniquely identify and authenticate devices. Consider whether such processes and methods • adequately address the access paths within and between the relevant information systems; • adequately address the components of the information systems, including related operating systems and data management systems;	NIST SP 800-53, IA-3 NIST SP 800-53, IA-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk; and • reasonably assure that devices are properly identified and authenticated before connections to relevant information systems or their components are established. Determine whether relevant information systems uniquely identify and authenticate devices before establishing a connection.	
AC.01.01.04 Remote access is appropriately controlled and protected. *Related control: AC.01.01.05*	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to control and protect remote access (dial-up or broadband) through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to control and protect remote access. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems; • are suitably designed and properly implemented based on risk; and • reasonably assure that remote access to information systems or their components is appropriately controlled and protected. Observe appropriate personnel as they obtain remote access to relevant information systems and their components. Consider whether the processes and methods observed to control and protect remote access are consistent with those the entity has documented.	NIST SP 800-53, AC-3 NIST SP 800-53, AC-17

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Obtain an understanding of the entity's processes and methods to log and monitor remote access to relevant information systems and their components through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software as well as reports that log management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether remote access is appropriately controlled and protected for relevant information systems. Note: Remote access is access to organizational systems (or process acting on behalf of user) that communicate through external networks, such as the internet Types of remote access include dial-up, broadband, and wireless.	
AC.01.01.05 Wireless access is appropriately controlled and protected. *Related control: AC.01.01.04*	Obtain an understanding of the entity's processes and methods to control and protect wireless access to entity networks, network components, information systems, and information system components through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to control and protect wireless access to entity networks, network components, information systems,	NIST SP 800-53, AC-18 NIST SP 800-53, SC-43

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	and information system components. Consider whether such processes and methods • include procedures for identifying and remediating rogue wireless access points; • are suitably designed and properly implemented based on risk; and • reasonably assure that wireless access to entity networks, network components, information systems, and information system components is appropriately controlled and protected. Observe appropriate personnel as they obtain wireless access to entity networks, network components, information systems, and information system components, as applicable. Consider whether the processes and methods observed to control and protect wireless access are consistent with those the entity has documented. Observe appropriate personnel as they perform procedures for identifying and remediating rogue wireless access points. Consider whether the procedures observed are consistent with those the entity has documented. Obtain an understanding of the entity's processes and methods to log and monitor wireless access to entity networks, network components, information systems, and information system components through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See AC.05.01and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether wireless access to entity networks, network components, information systems, and information system components is appropriately controlled and protected.	
AC.01.01.06 System connectivity through the use of mobile devices and personally owned systems, components, or devices is approved only when appropriate to perform assigned official duties.	Obtain an understanding of the entity's processes and methods to enable or prevent the use of mobile devices and personally owned systems, components, or devices through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to enable or prevent the use of mobile devices and personally owned systems, components, or devices. Consider whether such processes and methods • include entity-level policies on the use of mobile devices and personally owned systems, components, or devices; • include procedures for requesting and approving the use of mobile devices and personally owned systems, components, or devices; • include software update or configuration requirements imposed on individual users to mitigate risks associated with the use of mobile devices and personally owned systems, components, or devices; • include mechanisms to monitor and enforce software update or configuration requirements imposed on individual users; • are suitably designed and properly implemented based on risk; and • reasonably assure that system connectivity through the use of mobile devices and personally owned systems,	NIST SP 800-53, AC-17 NIST SP 800-53, AC-18 NIST SP 800-53, AC-19 NIST SP 800-53, AC-20 NIST SP 800-53, SC-43

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	components, or devices is approved only when appropriate to perform assigned official duties. Inquire with appropriate personnel to obtain an understanding of the extent to which entity personnel may use mobile devices and personally owned systems, components, or devices when performing significant business processes. If applicable, observe personnel as they use mobile devices and personally owned system, components, or devices to perform significant business processes. Determine whether system connectivity through the use of mobile devices and personally owned systems, components, or devices is approved only when appropriate to perform assigned official duties.	
AC.01.02 Network sessions are appropriately controlled.		
AC.01.02.01 Where connectivity is not continual, the network connection automatically disconnects at the end of a communications session.	Obtain an understanding of the entity's processes and methods to automatically disconnect network connections at the end of communications sessions through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as policies and procedures for managing network connectivity and implemented configuration settings, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to automatically disconnect network connections at the end of communications sessions. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that network connections are appropriately disconnected.	NIST SP 800-53, SC-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether network connections are automatically disconnected at the end of communications sessions where connectivity is not intended to be continual.	
AC.01.02.02 Unauthorized access to the system is prevented by allowing users to initiate a device lock before leaving the system unattended and by configuring the system to initiate a device lock after a specified period of inactivity. Device locks remain in effect until users reestablish access using identification and authentication procedures.	Obtain an understanding of the entity's processes and methods to use device locks to prevent unauthorized access to systems through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for managing device locks and implemented configuration settings for initiating device locks after a specified period of inactivity, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to use device locks to prevent unauthorized access to systems. Consider whether such processes and methods • include entity-level policies on the use of device lock before leaving systems unattended, • are suitably designed and properly implemented based on risk, and • reasonably assure that device locks are consistently and properly initiated and remain in effect until users reestablish access using identification and authentication procedures. Observe a user initiate a device lock. Observe the system to determine whether the system automatically initiates a device lock after a period of inactivity. Determine whether device locks are properly used to prevent unauthorized access to systems.	NIST SP 800-53, AC-11
AC.01.02.03 A user session is automatically terminated when certain conditions or events occur.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes	NIST SP 800-53, AC-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	employ to automatically terminate user sessions when certain conditions or events occur through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for managing user sessions and implemented configuration settings for terminating user sessions when certain conditions or events occur, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to automatically terminate user sessions when certain conditions or events occur. Consider whether such processes and methods • identify the conditions or events that will prompt the information system to automatically terminate a user session, • are suitably designed and properly implemented based on risk, and • reasonably assure that user sessions are appropriately terminated. Observe the occurrence of the conditions or events that should prompt an information system to automatically terminate a user session. Determine whether user sessions for relevant information systems are automatically terminated when certain conditions or events occur.	
AC.01.02.04 Appropriate notifications are displayed on screen • before users log onto a system and until they acknowledge the notifications (for example, U.S. government system, consent to monitoring, penalties for	Inquire of appropriate personnel, including users, to obtain an understanding of the entity's use of system notifications for the information systems relevant to the significant business processes. Observe appropriate personnel as they obtain access to relevant information systems. Determine whether appropriate notifications are displayed on screen before users log onto a system and after successful log-on.	NIST SP 800-53, AC-8 NIST SP 800-53, AC-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
unauthorized use, privacy notices) and • after successful log-on to the system (for example, date and time of last log-on and unsuccessful log-ons).		
AC.02 Management designs and implements control activities to appropriately restrict logical access to information systems and information system resources to authorized individuals for authorized purposes.		
AC.02.01 Identification and authentication requirements are established.		
AC.02.01.01 Identification and authentication is unique to each user (or process acting on behalf of user), except in specially approved instances (for example, when individuals access public websites or other publicly accessible systems).	Obtain an understanding of the entity's processes and methods to reasonably assure that identification and authentication is unique to each user (or process acting on behalf of user) through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and authentication parameters evidenced by system configuration files and reports produced by access control software. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to reasonably assure that identification and authentication is unique to each user (or process acting on behalf of user). Consider whether such processes and methods • include entity-level policies requiring unique identification and authentication of users and processes; • identify (preferably within the entity-level policies) any specific conditions or circumstances in which unique identification and authentication may not be necessary and for which an exception may be requested and approved;	NIST SP 800-53, IA-2 NIST SP 800-53, IA-8 NIST SP 800-53, IA-9 NIST SP 800-53, AC-14

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• include procedures for requesting and approving exceptions to the requirement for unique identification and authentication of users and processes; • maintain a complete listing of any specially approved instances in which unique identification and authentication is not required, which is shared with authorizing officials and other IT management personnel; • are suitably designed and properly implemented based on risk; and • reasonably assure that identification and authentication is unique to each user (or process acting on behalf of user), except in specially approved instances. Inquire of appropriate personnel to obtain an understanding of any specially approved instances in which unique identification and authentication is not required. Inspect documentation for any specially approved instances in which unique identification and authentication is not required. Consider whether the documentation for any specially approved instances • has been recently reviewed and updated, as appropriate; • describes the current status of any mitigating factors or compensating controls cited as part of the entity's approval of the exception; • accurately describes the impact of the exception on information systems and common controls available for inheritance to enable authorizing officials to assess risk and determine whether the mitigating factors or compensating controls sufficiently reduce risk to an acceptable level; and • demonstrates that the exception was properly approved in accordance with the entity's procedures. Identify any specially approved instances that affect the information systems relevant to the significant business processes or the	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	components of such information systems, including related operating systems and data management systems. Obtain an understanding of any compensating controls cited as part of the entity's approval of relevant exceptions through • inquiry of appropriate personnel; • inspection of relevant documentation, such as policies and procedures; and • observation of the entity's application of compensating controls. Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated with any specially approved instances affecting relevant information systems or their components. Determine whether identification and authentication applicable to relevant information systems and their components is unique to each user (or process acting on behalf of user), except in specially approved instances.	
AC.02.01.02 Authenticators (for example, passwords, tokens, biometrics, key cards, Public Key Infrastructure (PKI) certificates, or multifactor authenticator), including strength of mechanism, are selected and employed based on risk. *Related control: AC.02.04.01*	Obtain an understanding of any entity-level policies or procedures governing the selection of authenticators through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of authenticators selected for use in connection with relevant information systems and their components. Consider whether the authenticators • have sufficient strength of mechanism for their intended use, • were selected in accordance with the entity's policies and procedures, and	NIST SP 800-53, IA-5 NIST SP 800-53, IA-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk. Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components. Determine whether the authenticators selected for use in connection with the relevant information systems and their components, are appropriate based on risk.	
AC.02.01.03 Authenticators and authentication information feedback are adequately protected from unauthorized disclosure or modification.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to protect authenticators and authentication information feedback from unauthorized disclosure or modification through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as entity-level or system-level policies and procedures for authenticator management, system security and privacy plans, and access control software authentication parameters. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to protect authenticators and authentication information feedback from unauthorized disclosure or modification. Consider whether such processes and methods are suitably designed and properly implemented based on risk. Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. Consider whether authentication information feedback is obscured. Determine whether the authenticators and authentication information feedback applicable to relevant information systems and their	NIST SP 800-53, IA-5 NIST SP 800-53, IA-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	components are adequately protected from unauthorized disclosure or modification.	
AC.02.01.04 PKI-based authentication • validates certificates by constructing a certification path to an accepted trust anchor, • establishes user control of the corresponding private key, and • maps the authenticated identity to the user account. *Related control: AC.02.02.02*	Obtain an understanding of any entity-level policies or procedures governing PKI-based authentication methods through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of any PKI-based authentication methods used in connection with relevant information systems and their components. Consider whether the PKI-based authentication methods • validate certificates by constructing a certification path to an accepted trust anchor, • establish user control over the corresponding private key, • map the authenticated identity to the user account, and • satisfy information security requirements in accordance with authoritative criteria. Inspect certificate parameters. Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components. Determine whether any PKI-based authentication methods used in connection with relevant information systems and their components are suitably designed and properly implemented based on risk.	NIST SP 800-53, IA-5
AC.02.01.05 Password-based authenticators • are not displayed when entered;	Obtain an understanding of any entity-level policies or procedures governing the use of password-based authenticators through	NIST SP 800-53, IA-5 NIST SP 800-53, IA-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• are changed periodically (e.g., every 30 to 90 days); • contain alphanumeric and special characters; • are sufficiently complex (e.g., not easily guessed, minimum length, no words, etc.); • have an appropriate life (e.g., automatically expire); • are prohibited from reuse for a specified period of time (e.g., at least six generations); and • are not the same as the user ID.	• inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of any password-based authenticators used in connection with relevant information systems and their components. Consider whether the password based authenticators • are not displayed when entered; • are changed periodically (e.g., every 30 to 90 days); • contain alphanumeric and special characters; • are sufficiently complex (e.g., not easily guessed, minimum length, no words, etc.); • have an appropriate life (e.g., automatically expire); • are prohibited from reuse for a specified period of time (e.g., at least six generations); • are not the same as the user ID; and • satisfy information security requirements in accordance with authoritative criteria. Inspect access control software authentication parameters. Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components. Determine whether any password-based authenticators used in connection with relevant information systems and their components are suitably designed and properly implemented based on risk.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.02.01.06 Shared or group authenticators are only used in specially approved instances.	Obtain an understanding of the entity's processes and methods to reasonably assure that shared or group authenticators are not used through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and authentication parameters evidenced by system configuration files and reports produced using access control software. Inspect documentation demonstrating the design and implementation of the entity's processes and methods for approving shared or group authenticators in special instances. Consider whether such processes and methods • include entity-level policies requiring unique identification and authentication of users and processes; • identify (preferably within the entity-level policies) any specific conditions or circumstances in which unique identification and authentication may not be necessary and for which an exception may be requested and approved; • include procedures for requesting and approving exceptions to the requirement for unique identification and authentication of users and processes; • maintain a complete listing of any specially approved instances in which unique identification and authentication is not required, which is shared with authorizing officials and other IT management personnel; • are suitably designed and properly implemented based on risk; and • reasonably assure that shared or group authenticators are not used, except in specially approved instances.	NIST SP 800-53, AC-2 NIST SP 800-53, IA-2 NIST SP 800-53, IA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inquire of appropriate personnel to obtain an understanding of any specially approved instances in which shared or group authenticators are permitted. Inspect documentation for any specially approved instances in which shared or group authenticators are permitted. Consider whether the documentation for any specially approved instances • has been recently reviewed and updated, as appropriate; • describes the current status of any mitigating factors or compensating controls cited as part of the entity's approval of the exception; • accurately describes the impact of the exception on information systems and common controls available for inheritance to enable authorizing officials to assess risk and determine whether the mitigating factors or compensating controls sufficiently reduce risk to an acceptable level; and • demonstrates that the exception was properly approved in accordance with the entity's procedures. Identify any specially approved instances that affect the information systems relevant to the significant business processes or the components of such information systems, including related operating systems and data management systems. Obtain an understanding of any compensating controls cited as part of the entity's approval of relevant exceptions through • inquiry of appropriate personnel; • inspection of relevant documentation, such as policies and procedures; and • observation of the entity's application of compensating controls. Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	with any specially approved instances affecting relevant information systems or their components. Determine whether shared or group authenticators are only used in specially approved instances. Note: Unique identification of individuals in group accounts is required for detailed accountability of individual activity. If shared or group authenticators are used, the authenticators should be promptly changed when membership to the shared or group account changes to ensure that former members do not retain access to the shared or group account. Management should only authorize the use of shared or group authenticators for specific shared or group accounts.	
AC.02.01.07 Vendor-supplied default passwords are replaced during software or hardware installation.	Obtain an understanding of any entity-level policies or procedures governing the replacement of vendor-supplied default passwords during software or hardware installation through • inquiry of appropriate personnel and • inspection of relevant policies and procedures for system component installation and configuration. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect password files using audit software to verify whether common vendor-supplied passwords are in use. Determine whether vendor-supplied default passwords are replaced during installation for relevant systems.	NIST SP 800-53, IA-5
AC.02.01.08 Authenticators embedded in programs are only used in specially approved instances.	Obtain an understanding of the entity's processes and methods to reasonably assure that passwords embedded in programs are not used through • inquiry of appropriate personnel, including network engineers, system developers, and network and system administrators, and	NIST SP 800-53, IA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and authentication parameters, as well as relevant programs or program source code, as applicable. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to reasonably assure that passwords embedded in programs are not used. Consider whether such processes and methods • include entity-level policies prohibiting passwords embedded in programs; • identify (preferably within the entity-level policies) any specific conditions or circumstances in which the use of passwords embedded in programs may be necessary and for which an exception may be requested and approved; • include procedures for requesting and approving exceptions to the prohibition for passwords embedded in programs; • maintain a complete listing of any specially approved instances in which the use of passwords embedded in programs is necessary, which is shared with authorizing officials and other IT management personnel; • are suitably designed and properly implemented based on risk; and • reasonably assure that passwords embedded in programs are not used, except in specially approved instances. Identify any specially approved instances that affect the information systems relevant to the significant business processes or the components of such information systems, including related operating systems and data management systems. Obtain an understanding of any compensating controls cited as part of the entity's approval of relevant exceptions through • inquiry of appropriate personnel;	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant documentation, such as policies and procedures; and • observation of the entity's application of compensating controls. Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated with any specially approved instances affecting relevant information systems or their components. Determine whether passwords embedded in programs are only used in specially approved instances. Note: An embedded password is a password that is included into the source code of an application or utility. Applications often need to communicate with other applications and systems, and this requires an "authentication" process, which is sometimes accomplished through the use of embedded passwords.	
AC.02.01.09 Authenticator management processes are implemented to prevent improper duplication of authenticators and to administer lost, compromised, or damaged authenticators (e.g., passwords, tokens, biometrics, key cards, or PKI certificates).	Obtain an understanding of the entity's processes and methods for managing authenticators applicable to the information systems relevant to the significant business processes through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed to prevent improper duplication of authenticators and to administer lost, compromised, or damaged authenticators (e.g., passwords, tokens, biometrics, key cards, or PKI certificates).	NIST SP 800-53, IA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the authenticator management processes applicable to relevant information systems are designed, implemented, and operating effectively to prevent improper duplication of authenticators and to administer lost, compromised, or damaged authenticators.	
AC.02.01.10 Account policies (including password, authentication, and lockout policies) are appropriate based on risk and enforced.	Obtain an understanding of the entity's processes and methods for establishing and implementing account policies through • inquiry of appropriate personnel, including users, and • inspection of relevant documentation and account policy settings. Inspect relevant documentation and account policy settings for a selection of account policies (including password, authentication, and lockout policies) applicable to relevant information systems and their components. Determine whether enabled account policies applicable to relevant information systems and their components are appropriate based on risk and enforced.	NIST SP 800-53, AC-7
AC.02.01.11 Consecutive attempts to log on with invalid passwords within a certain period are limited (e.g., three to seven attempts).	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to limit consecutive log-on attempts through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to limit consecutive log-on attempts. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems;	NIST SP 800-53, AC-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk; and • reasonably assure that consecutive attempts to log on with invalid passwords within a certain period are limited. Observe users as they repeatedly attempt to log onto relevant information systems and their components using invalid passwords. Consider whether the processes and methods observed to limit consecutive log-on attempts are consistent with those documented by the entity. Obtain an understanding of the entity's processes and methods to log and monitor consecutive log-on attempts to relevant information systems and their components through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether relevant information systems and their components appropriately limit consecutive attempts to log on with invalid passwords within a certain period.	
AC.02.02 Information system users, processes, and services are appropriately identified and authenticated before accessing information systems and information system resources.		

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.02.02.01 Evidence of an individual's identity is presented, validated, and verified based on applicable identity assurance-level requirements before the entity provides user credentials.	Obtain an understanding of the entity's processes and methods for presenting, validating, and verifying evidence of an individual's identity through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Inspect available documentation for a selection of individuals for whom user credentials were established during the audit period. Consider whether evidence of each individual's identity was presented, validated, and verified • based on applicable identity assurance-level requirements and • before the entity provides user credentials for the individual. Determine whether evidence of an individual's identity is presented, validated, and verified based on applicable identity assurance-level requirements before the entity provides user credentials.	NIST SP 800-53, IA-12
AC.02.02.02 PKI certificates are issued in accordance with an approved certificate policy or obtained from an approved service provider. Only approved trust anchors are included in trust stores or certificate stores that the entity manages. *Related control: AC.02.01.04*	Obtain an understanding of the entity's process and methods for issuing PKI certificates through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect available documentation for a selection of user accounts applicable to relevant information systems and their components for which PKI certificates were issued during the audit period. Consider whether the PKI certificates were either • issued in accordance with an approved certificate policy or • obtained from an approved service provider. Determine whether PKI certificates are issued in accordance with an approved certificate policy or obtained from an approved service provider.	NIST SP 800-53, SC-17

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether only approved trust anchors are included in trust stores or certificate stores that the entity manages.	
AC.02.02.03 Appropriate session-level controls are implemented (e.g., name and address resolution service and session authenticity).	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to implement session-level controls through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as policies and procedures for managing sessions, as well as implemented configuration settings, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to implement session-level controls. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems; • are suitably designed and properly implemented based on risk; and • reasonably assure that appropriate session-level controls are implemented. Consider the adequacy of session-level controls, including name and address resolution service, session authenticity, protection of session-level information held in temporary storage, and other controls to reasonably assure that one session ends before the next session begins (i.e., prevent overlapping sessions). Determine whether appropriate session-level controls are implemented.	NIST SP 800-53, SC-20 NIST SP 800-53, SC-21 NIST SP 800-53, SC-22 NIST SP 800-53, SC-23

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.02.02.04 User reauthentication is required when specific circumstances or situations occur (e.g., changes in roles, authenticators, or credentials).	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to require user reauthentication when specific circumstances or situations occur through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for managing user reauthentication, as well as implemented configuration settings requiring user reauthentication when specific circumstances or situations occur, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to require user reauthentication when specific circumstances or situations occur. Consider whether such processes and methods • identify the specific circumstances or situations (e.g., changes in roles, authenticators, or credentials) that will prompt the information system to require a user to reauthenticate; • are suitably designed and properly implemented based on risk; and • reasonably assure that user reauthentication is required as appropriate. Observe the occurrence of the specific circumstances or situations that should prompt the information system to require a user to reauthenticate. Determine whether specific circumstances or situations that require the information systems to re-authenticate users are appropriate based on risk.	NIST SP 800-53, IA-11
AC.02.02.05 Concurrent sessions are appropriately controlled.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to control concurrent sessions through	NIST SP 800-53, AC-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as policies and procedures for managing user sessions, as well as implemented configuration settings for controlling concurrent sessions, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to control concurrent sessions. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that concurrent sessions are appropriately controlled. Observe appropriate personnel as they initiate concurrent sessions on relevant information systems. Consider whether the processes and methods observed to control concurrent sessions are consistent with those the entity has documented. Consider whether concurrent sessions could be used to (1) enable an unauthorized individual to access the information system or (2) enable an authorized user to circumvent information system segregation of duties controls. Obtain an understanding of the entity's processes and methods to log and monitor concurrent sessions on relevant information systems through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether concurrent sessions on relevant information systems are appropriately controlled.	
AC.02.02.06 When appropriate, digital signatures and other nonrepudiation mechanisms are employed to provide irrefutable evidence that a user (or a process acting on behalf of a user) performed a certain action.	Obtain an understanding of any entity-level policies or procedures governing the use of digital signatures and other nonrepudiation mechanisms through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of digital signatures and other nonrepudiation mechanisms employed in connection with the significant business processes, the information systems relevant to the significant business processes and their components. Consider whether the digital signatures and other nonrepudiation mechanisms • were selected in accordance with the entity's policies and procedures and • are suitably designed and properly implemented based on risk. Observe appropriate personnel as they employ digital signatures and other nonrepudiation mechanisms in connection with the significant business processes, the relevant information systems and their components. Determine whether the digital signatures and other nonrepudiation mechanisms are appropriately employed in connection with the	NIST SP 800-53, AU-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	significant business processes, the relevant information systems and their components. Note: Nonrepudiation mechanisms provide (1) protection when an individual falsely denies having performed a certain action and (2) the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.	
AC.02.03. Information system users, processes, and services are appropriately authorized before accessing information systems and information system resources.		
AC.02.03.01 The types of accounts that are allowed and specifically prohibited for use for the system are defined and documented.	Obtain an understanding of the entity's processes and methods for defining and documenting the types of accounts that are allowed and specifically prohibited for use for the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and • inspection of relevant documentation. Inspect relevant system documentation identifying the types of accounts allowed and specifically prohibited for use for relevant information systems. Consider whether • the definitions include usage and restriction conditions and • the criteria for group and role membership are specified. Determine whether the types of accounts, their usage and restriction conditions, and if applicable criteria for group and role membership have been appropriately documented and are appropriate based on risk. Inspect a system-generated list of accounts. Consider whether the list includes undefined or prohibited types of accounts. Determine whether the types of accounts established are appropriate.	NIST SP 800-53, AC-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service.	
AC.02.03.02 System users and their authorized access are defined, documented, and periodically reviewed and updated. *Related controls: AC.02.03.05, AC.02.04.01, and SD.01.02.02*	Obtain an understanding of the entity's processes and methods for defining, documenting, and periodically reviewing and updating the information system users and their authorized access through • inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and • inspection of relevant documentation. Inspect relevant policies and procedures for access authorization and account management, system security and privacy plans, and other documentation identifying the information system users and their authorized access to the information systems relevant to the significant business processes. Consider whether • privileged and nonprivileged users and their authorized access are accurately identified and • the access that information system users are authorized to have is compatible with segregation of duties requirements. Determine whether the information system users and their authorized access to relevant information systems are appropriate based on risk and consistent with the concept of least privilege. Determine whether the information system users and their authorized access to relevant information systems have been appropriately documented and periodically reviewed and updated.	NIST SP 800-53, AC-2
AC.02.03.03 Account management processes are implemented to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed.	Obtain an understanding of the entity's processes and methods for creating, enabling, modifying, disabling, and removing accounts applicable to the information systems relevant to the significant business processes through	NIST SP 800-53, AC-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; • inspection of relevant policies and procedures for access authorization and account management; and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed. Inspect available documentation for a selection of accounts that were created, enabled, modified, disabled, or removed during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for access authorization and account management. Consider whether the administrators responsible for account management actions identify and discuss any questionable authorizations with information resource owners. Determine whether the account management processes applicable to relevant information systems are designed, implemented, and operating effectively to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed.	
AC.02.03.04 Account management processes are implemented to reasonably assure that accounts are timely modified, disabled, or removed when associated access privileges or accounts are no longer required.	Obtain an understanding of the entity's processes and methods for modifying, disabling, or removing accounts applicable to the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials;	NIST SP 800-53, AC-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant policies and procedures for account management; and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed to reasonably assure that accounts are timely modified, disabled, or removed when associated access privileges or accounts are no longer required. Inspect available documentation for a selection of accounts that were modified, disabled, or removed during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for account management. Inspect access control software parameters for disabling inactive accounts and verify whether such are consistent with the entity's policies and procedures for account management. Inquire of the administrators responsible for account management actions and inspect a system-generated list of disabled accounts to determine why the disabled accounts have not been removed. Consider the completeness and accuracy of the documentation obtained, including any system-generated listings, when performing control tests. Inspect a system-generated list of enabled user accounts and a list of recently separated personnel to determine whether user accounts for recently separated personnel remain enabled after their separation dates. Consider the completeness and accuracy of the documentation obtained, including any system-generated listings, when performing control tests. Determine whether the account management processes applicable to relevant information systems are designed, implemented, and operating effectively to reasonably assure that accounts are timely	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	modified, disabled, or removed when associated access privileges or accounts are no longer required.	
AC.02.03.05 Access to systems and system resources is limited to individuals with a valid business purpose (least privilege). *Related controls: AC.02.03.02 and AC.02.04.01*	Obtain an understanding of the entity's processes and methods for limiting system access to individuals with a valid business purpose for the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials, and • inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and other documentation identifying the information system users and their authorized access. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to reasonably assure that system access is limited to individuals with a valid business purpose. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that system access is limited to individuals with a valid business purpose. Inspect available documentation for a selection of user accounts that were created, enabled, or modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for account management. Inspect system-generated listings of user accounts and privileged user accounts to determine whether the access privileges associated with such accounts are consistent with the access privileges defined and documented for such users. Consider the completeness and accuracy of the documentation obtained, including any system-generated listings, when performing control tests.	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether system access is limited to individuals with a valid business purpose (least privilege) for relevant information systems.	
AC.02.03.06 Emergency and temporary access to systems and system resources is appropriately controlled.	Obtain an understanding of the entity's processes and methods to control emergency and temporary access to the information systems and information system resources relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for the use of emergency and temporary accounts, including firecall IDs. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to control emergency and temporary access to the information systems and information system resources relevant to the significant business processes. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems; • include entity-level policies governing the use of emergency and temporary accounts, including firecall IDs; • identify (preferably within the entity-level policies) the specific conditions or circumstances in which emergency or temporary accounts may be used, as well as the specific functions or tasks that individuals may perform while using emergency or temporary accounts; • maintain a complete listing of individuals who are authorized to use emergency or temporary accounts, which is shared with authorizing officials and other IT management personnel; • include procedures for requesting and approving the use of emergency and temporary accounts;	NIST SP 800-53, AC-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• include procedures for creating, enabling, modifying, disabling, and removing emergency and temporary accounts; • are suitably designed and properly implemented based on risk; and • reasonably assure that emergency and temporary access to information systems and information system resources is appropriately controlled and protected. Obtain an understanding of the entity's processes and methods to log and monitor emergency and temporary access to the information systems and information system resources relevant to the significant business processes through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Observe appropriate personnel as they obtain access to the information systems and information system resources relevant to the significant business processes using emergency or temporary accounts. Consider whether the processes and methods observed to control emergency and temporary access are consistent with those the entity has documented. Inspect available documentation for a selection of instances in which emergency or temporary accounts were used during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures. Consider the	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	completeness and accuracy of the documentation obtained, including any logs of the use of emergency or temporary accounts, when performing control tests. Determine whether emergency and temporary access to the information systems and information system resources relevant to the significant business processes is appropriately controlled. Note: Temporary and emergency accounts are intended for short-term use. Entities establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Entities establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes.	
AC.02.03.07 Access to shared file systems is appropriately restricted.	Obtain an understanding of the entity's processes and methods to restrict access to shared file systems relevant to the significant business processes through • inquiry of appropriate personnel, including network and system administrators, and • inspection of relevant documentation, such as policies and procedures for managing access to shared file systems. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to restrict access to shared file systems relevant to the significant business processes. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that access to shared file systems relevant to the significant business processes is appropriately restricted. Observe appropriate personnel as they obtain access to the shared file systems relevant to the significant business processes. Consider	NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	whether the processes and methods observed to restrict access to shared file systems are consistent with those the entity has documented. Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software to determine whether access to shared file systems relevant to the significant business processes is appropriately restricted to authorized personnel. Inspect available documentation for a selection of instances in which access to shared file systems relevant to the significant business processes was modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures. Consider the completeness and accuracy of the documentation obtained, including any logs of changes to access control parameters, when performing control tests. Obtain an understanding of the entity's processes and methods to log and monitor access to the shared file systems, as well as changes to access control parameters, relevant to the significant business processes through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether access to shared file systems relevant to the significant business processes is appropriately restricted.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.02.03.08 Access to systems and system resources is reviewed periodically for continuing appropriateness.	Obtain an understanding of the entity's processes and methods for periodically reviewing access to the information systems and information system resources relevant to the significant business processes through • inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; • inspection of relevant policies and procedures for access authorization, account management, and periodic access recertification; and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which access to the information systems and information system resources relevant to the significant business processes was reviewed during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for access authorization, account management, and periodic access recertification. Consider the completeness and accuracy of the documentation obtained, including any system-generated listings of accounts, when performing control tests. Determine whether the processes for periodically reviewing access to the information systems and information system resources relevant to the significant business processes are designed, implemented, and operating effectively to reasonably assure that system access is appropriate.	NIST SP 800-53, AC-2
AC.02.03.09 Access control parameters are set to apply access control decisions and enforce access as authorized.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes	NIST SP 800-53, AC-3 NIST SP 800-53, AC-24 NIST SP 800-53, AC-25

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	employ to apply access control decisions and enforce access as authorized through • inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and • inspection of relevant documentation, such as policies and procedures for managing access control software, as well as implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to apply access control decisions and enforce access as authorized. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems; • are suitably designed and properly implemented based on risk; and • reasonably assure that access control parameters are properly set to apply access control decisions and enforce access as authorized. For each of relevant information systems, identify the directory names for files, data sets, libraries, and other information system resources critical to achieving information security or information processing objectives. For example, information system resources may include files used or relied upon by operating systems. Inspect the access control parameters for such information system resources, found in applicable access control lists, system configuration files, and reports produced using access control software (e.g., reports detailing access rules applicable to specific data sets or resources and reports detailing privileges granted to specific users or accounts that provide access to	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	data sets, libraries, and other information system resources). Consider whether the access control parameters are appropriate and consistent with access authorization decisions. Consider whether standard naming conventions are established and used effectively. Inspect available documentation for a selection of instances in which access control parameters applicable to information systems or information system resources relevant to the significant business processes were modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for managing access control software. Consider the completeness and accuracy of the documentation obtained, including any system-generated access control lists or system configuration files, when performing control tests. Obtain an understanding of the entity's processes and methods to log and monitor changes to access control parameters through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether access control parameters applicable to information systems and information system resources relevant to the significant business processes are properly set to apply access control decisions and enforce access as authorized. Note: Access control parameters are set to apply access control decisions to data sets, libraries, and other information system	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	resources. Standard naming conventions are generally established and used as a basis for controlling access to information system resources. Standard naming conventions support effective configuration management identification and control of production files and programs versus test files and programs.	
AC.02.03.10 The system is configured to provide only those functions and services that are necessary to support entity operations through, for example, • installing only required functions and services based on least functionality, • restricting access to required functions and services based on least privilege, • monitoring the use of functions and services, and • employing appropriate tools and technologies to identify and prevent the use of prohibited functions and services. *Related controls: CM.01.04.01 and CM.03.01.01*	Obtain an understanding of the entity's processes and methods for the information systems relevant to the significant business processes to reasonably assure that system functions and services are limited to those necessary to support entity operations through • inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and • inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and other documentation identifying the functions and services each information system is configured to provide. Inspect documentation demonstrating the design and implementation of the entity's processes and methods for relevant information systems to reasonably assure that system functions and services are limited to those necessary to support entity operations. Consider whether such processes and methods • include policies and procedures for installing only required functions and services based on least functionality, • include policies and procedures for restricting access to required functions and services based on least privilege, • address monitoring the use of functions and services, • employ appropriate tools and technologies to identify and prevent the use of prohibited functions and services, • are suitably designed and properly implemented based on risk, and	NIST SP 800-53, CM-7 NIST SP 800-53, SC-41

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• reasonably assure that system functions and services are limited to those that are necessary to support entity operations. Determine whether relevant information systems are properly configured to provide only those functions and services necessary to support entity operations.	
AC.02.03.11 The system prohibits remote activation of collaborative computing devices and applications and provides an explicit indication of use of such devices and applications to local users.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to prohibit remote activation of collaborative computing devices and applications through • inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and • inspection of relevant documentation, such as policies and procedures for managing collaborative computing devices and applications, as well as implemented configuration settings, found in applicable system configuration files. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to prohibit remote activation of collaborative computing devices and applications. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that the information systems prohibit remote activation of collaborative computing devices and applications. Observe appropriate personnel as they use collaborative computing devices and applications. Determine whether the system provides an explicit indication of use of such devices and applications to the local user.	NIST SP 800-53, SC-15

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether relevant information systems prohibit remote activation of collaborative computing devices. Note: Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.	
AC.02.04 Access privileges restrict access to information system resources to authorized individuals for authorized purposes.		
AC.02.04.01 The use of privileged accounts is restricted to individuals or processes with a legitimate need for privileged access to system resources for the purposes of accomplishing valid business functions. *Related controls: AC.02.03.02 and AC.02.03.05*	Obtain an understanding of the entity's processes and methods for the information systems relevant to the significant business processes to reasonably assure that the use of privileged accounts is appropriately restricted through • inquiry of appropriate personnel, including privileged users, network and system administrators, information resource owners, and authorizing officials, and • inspection of relevant documentation, such as relevant policies and procedures for access authorization and account management, system security and privacy plans, and other documentation identifying privileged users and the access they are authorized to have. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to reasonably assure that the use of privileged accounts is appropriately restricted. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems; • include entity-level policies governing the use of privileged accounts;	NIST SP 800-53, AC-2 NIST SP 800-53, AC-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• identify (preferably within the entity-level policies) the specific functions or tasks that individuals may perform while using privileged accounts; • maintain a complete listing of individuals who are authorized to use privileged accounts, which is shared with authorizing officials and other IT management personnel; • are suitably designed and properly implemented based on risk; and • reasonably assure that privileged access is limited to individuals or processes with a valid business purpose. Inspect available documentation for a selection of privileged accounts that were created, enabled, or modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for account management. Inspect system-generated listings of privileged accounts to determine whether the access privileges associated with such accounts are consistent with the access privileges defined and documented for privileged users or processes. Consider the completeness and accuracy of the documentation obtained, including any system-generated listings, when performing control tests. Determine whether the use of privileged accounts is restricted to individuals or processes with a legitimate need for privileged access to information system resources to accomplish valid business functions.	
AC.02.04.02 The use of privileged accounts is appropriately logged and adequately monitored.	Obtain an understanding of the entity's processes and methods to log and monitor the use of privileged accounts through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and	NIST SP 800-53, AC-2 NIST SP 800-53, AU-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to log and monitor the use of privileged accounts. Consider whether such processes and methods • adequately address the components of the information systems relevant to the significant business processes, including related operating systems and data management systems; • are suitably designed and properly implemented based on risk; • reasonably assure that reports that log management software produces and entity management reviews are complete and accurate; and • reasonably assure that the entity takes appropriate action to identify and address any access anomalies. Observe the entity's processes and methods to log and monitor the use of privileged accounts and inspect relevant reports that log management software produces and entity management reviews. Consider the completeness and accuracy of these reports when performing control tests. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether the use of privileged accounts is appropriately logged and adequately monitored.	
AC.02.04.03 Logical access to maintenance tools and utilities is appropriately controlled and logged and adequately monitored.	Obtain an understanding of the entity's processes and methods to control, log, and monitor logical access to maintenance tools and	NIST SP 800-53, AC-2 NIST SP 800-53, MA-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	utilities applicable to the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including network and system administrators, information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to control, log, and monitor logical access to maintenance tools and utilities applicable to relevant information systems. Consider whether such processes and methods • adequately address the components of the information systems, including related operating systems and data management systems; • are suitably designed and properly implemented based on risk; • reasonably assure that logical access to maintenance tools and utilities applicable to relevant information systems is appropriately controlled and logged; • reasonably assure that reports that log management software produces and entity management reviews are complete and accurate; and • reasonably assure that entity management takes appropriate action to identify and address any access anomalies. Observe appropriate personnel as they obtain logical access to maintenance tools and utilities applicable to relevant information	NIST SP 800-53, MA-3 NIST SP 800-53, MA-4 NIST SP 800-53, MA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	systems. Consider whether the processes and methods for controlling logical access are consistent with those documented by the entity. Observe the entity's processes and methods to log and monitor logical access to maintenance tools and utilities applicable to relevant information systems and inspect relevant reports that log management software produces and entity management reviews. Consider the completeness and accuracy of these reports when performing control tests. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether logical access to maintenance tools and utilities applicable to relevant information systems is appropriately controlled and logged and adequately monitored.	
AC.02.04.04 Authenticators and authentication services and directories are appropriately controlled and encrypted when appropriate.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to control logical access to authenticators and authentication services and directories through • inquiry of appropriate personnel, including authorizing officials, system developers, and network and system administrators, and • inspection of relevant documentation, such as policies and procedures for managing authenticators and authentication services and directories, as well as implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to control logical access to authenticators and authentication services and directories. Consider whether such processes and methods	NIST SP 800-53, AC-2 NIST SP 800-53, IA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• adequately address the components of the information systems, including related operating systems and data management systems; • employ encryption techniques when appropriate based on risk; • are suitably designed and properly implemented based on risk; and • reasonably assure that access to authenticators and authentication services and directories is restricted to authorized individuals for authorized purposes. Obtain an understanding of the entity's processes and methods to log and monitor logical access to authenticators and authentication services and directories applicable to relevant information systems and their components through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether authenticators and authentication services and directories applicable to relevant information systems and their components are appropriately controlled and encrypted when appropriate.	
AC.02.04.05 Mobile code is appropriately controlled.	Obtain an understanding of the entity's processes and methods to control mobile code through	NIST SP 800-53, SC-18

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to control mobile code. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that mobile code is appropriately controlled. Determine whether mobile code is appropriately controlled. Note: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system.	NIST SP 800-53, SC-43
AC.02.04.06 The system establishes an isolated, trusted communications path between the user and trusted components of the system, including entity-defined security functions of the system.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to establish an isolated, trusted communications path between the user and trusted components of the information system through • inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to establish an isolated, trusted communications path between the user and trusted components of the information system. Consider whether such processes and methods • identify and adequately address the trusted components of the information systems; • are suitably designed and properly implemented based on risk; and	NIST SP 800-53, SC-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• reasonably assure that an isolated, trusted communications path between the user and trusted components of the information system is established. Determine that the information systems establish an isolated, trusted communications path between the user and trusted components of the systems relevant to the significant business processes, including entity-defined security functions. Note: Entities employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users, including during system log-ons.	
AC.03 Management designs and implements control activities to appropriately protect data in response to risks.		
AC.03.01 Media controls are appropriately selected and employed based on risk.		
AC.03.01.01 Access to printed and digital media containing data removed from the system is limited to authorized individuals for authorized purposes.	Obtain an understanding of the entity's processes and methods to limit access to printed and digital media containing data removed from the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including users, information resource owners, and authorizing officials, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to limit access to printed and digital media containing data removed from relevant information systems. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that only authorized users with a valid business purpose have access to printed and digital media containing data removed from the information systems.	NIST SP 800-53, MP-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether access to printed and digital media containing data removed from relevant information systems is appropriately limited to authorized individuals for authorized purposes. Note: Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Nondigital media includes paper and microfilm.	
AC.03.01.02 The system marks output and associates security and privacy attributes with internal data in storage, process, and transmission as appropriate based on risk.	Obtain an understanding of the processes and methods that information systems relevant to the significant business processes employ to mark output and associate attributes with internal data in storage, process, and transmission through • inquiry of appropriate personnel, including system developers, users, information resource owners, and authorizing officials, and • inspection of relevant documentation. Inspect documentation, such as relevant system output reports and exports of relevant database schemas, demonstrating the design and implementation of the processes and methods that relevant information systems employ to mark output and associate attributes with internal data in storage, process, and transmission. Consider whether such processes and methods • are suitably designed and properly implemented based on risk; • employ standard practices for marking output, including the use of standard naming conventions; • employ standard practices for associating security and privacy attributes to internal data, including the labeling of data; and • reasonably assure that associated security and privacy attributes are not modified when information is exchanged between information systems and their components.	NIST SP 800-53, AC-16 NIST SP 800-53, MP-3 NIST SP 800-53, SC-16

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether relevant information systems appropriately mark output and associate attributes with internal data in storage, process, and transmission. Note: The association of attributes to subjects and objects by an information system is referred to as binding and includes setting the attribute value and the attribute type. Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of personally identifiable information, and identification of personal information within data objects. Entities can define the types of attributes needed for information systems to support mission or business functions. Labeling refers to the association of attributes with the subjects and objects represented by the internal data structures within information systems. This facilitates system-based enforcement of information security and privacy policies. A related term to labeling is marking. Marking refers to the association of attributes with objects in a human-readable form displayed on system output. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies.	
AC.03.01.03 The collection, transport, and delivery of system media are appropriately controlled.	Obtain an understanding of the entity's processes and methods for controlling the collection, transport, and delivery of system media associated with the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation. Observe the entity's processes and methods for controlling the collection, transport, and delivery of system media associated with relevant information systems.	NIST SP 800-53, MP-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect available documentation for a selection of instances in which system media associated with relevant information systems was collected, transported, or delivered during the audit period. Determine whether the collection, transport, and delivery of system media associated with relevant information systems is appropriately controlled.	
AC.03.01.04 System media is securely stored according to its sensitivity until destroyed or sanitized.	Obtain an understanding of the entity's processes and methods for storing system media associated with the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation. Observe the entity's processes and methods for storing system media associated with relevant information systems. Consider whether the processes and methods adequately address the sensitivity of data contained within such media and legal and entity information retention requirements. Determine whether system media associated with relevant information systems is securely stored according to its sensitivity until destroyed or sanitized.	NIST SP 800-53, MP-4
AC.03.01.05 Approved equipment, techniques, and procedures are implemented to sanitize and dispose of data, documentation, tools, or system components according to sensitivity.	Obtain an understanding of the entity's processes and methods for sanitizing and disposing of data, documentation, tools, or system components associated with the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation. Observe the entity's processes and methods for sanitizing and disposing of data, documentation, tools, or system components associated with relevant information systems. Consider whether the processes and methods adequately address the approved equipment, techniques, and procedures to be used based on the type of digital	NIST SP 800-53, MP-6 NIST SP 800-53, MP-8 NIST SP 800-53, SR-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	media, as well as the sensitivity of data contained within such media. Consider whether processes and methods adequately address sanitizing data, documentation, tools, or system components before disposal or release or reuse outside of the entity Inspect a selection of recently sanitized digital media and determine whether such have been properly sanitized. Inspect a selection of disposal records data, documentation, tools, or system components and determine whether such have been properly disposed of. Determine whether the approved equipment, techniques, and procedures for sanitizing and disposing of data, documentation, tools, or system components associated with relevant information systems are appropriate based on the sensitivity of data.	
AC.03.02 Cryptographic controls are appropriately selected and employed based on risk.		
AC.03.02.01 Cryptographic tools are implemented to protect the integrity and confidentiality of data and software when appropriate.	Obtain an understanding of any entity-level policies or procedures governing the selection and use of cryptographic tools through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of cryptographic tools selected for use in connection with relevant information systems and their components. Consider whether the cryptographic tools • are appropriate for their intended use, • were selected in accordance with the entity's policies and procedures, and • are suitably designed and properly implemented based on risk.	NIST SP 800-53, SC-13 NIST SP 800-53, SC-28

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the cryptographic tools selected for use in connection with relevant information systems and their components are properly implemented to protect the integrity of data and software, as applicable.	
AC.03.02.02 Encryption techniques are implemented to protect data communications when appropriate. *Related control: BP.05.03.03*	Obtain an understanding of any entity-level policies or procedures governing the selection and use of encryption techniques through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of encryption techniques selected for use in connection with relevant information systems and their components, including related operating systems and data management systems. Consider whether the encryption techniques • are appropriate for their intended use, • were selected in accordance with the entity's policies and procedures, and • are suitably designed and properly implemented based on risk. Determine whether the encryption techniques selected for use in connection with relevant information systems and their components are properly implemented to protect data communications, as applicable.	NIST SP 800-53, SC-8
AC.03.02.03 Appropriate mechanisms are employed for authentication to cryptographic modules.	Inspect documentation demonstrating the design and implementation of mechanisms employed for authentication to cryptographic modules applicable to the information systems relevant to the significant business processes. Consider whether the authentication mechanisms • are appropriate and	NIST SP 800-53, IA-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk. Determine whether appropriate mechanisms are properly employed for authentication to cryptographic modules applicable to relevant information systems. Note: Authentication mechanisms are hardware- or software-based mechanisms that force users to prove their identities before accessing information.	
AC.03.02.04 Processes for establishing and managing cryptographic keys are performed when cryptology is employed within the system.	Obtain an understanding of the entity's processes and methods to establish and manage cryptographic keys applicable to the information systems relevant to the significant business processes through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed in connection with cryptographic key generation distribution, storage, access, and destruction. Determine whether the cryptographic key establishment and management processes applicable to relevant information systems are designed, implemented, and operating effectively.	NIST SP 800-53, SC-12
AC.04 Management designs and implements control activities to appropriately restrict physical access to facilities, information systems, and information system resources to authorized individuals for authorized purposes.		
AC.04.01 Physical access controls are appropriately selected and employed based on risk.		
AC.04.01.01 Physical and environmental hazards to facilities where systems and system components reside are assessed and	Obtain an understanding of the entity-level process for assessing physical and environmental hazards to the facilities where information	NIST SP 800-53, PE-23

Illustrative control activities	Illustrative audit procedures	Relevant criteria
included as part of the entity-level risk management strategy for information security and privacy risks. *Related control: SM.04.01.01*	systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the entity-level risk management strategy for information security and privacy risks. Determine whether physical and environmental hazards to the facilities where information systems and information system resources relevant to the significant business processes reside are appropriately assessed and included as part of the entity-level risk management strategy. Note: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation.	
AC.04.01.02 System components are positioned within the facility to mitigate the risk of unauthorized access and minimize potential damage from physical and environmental hazards.	Obtain an understanding of the position of system components comprising the information systems relevant to the significant business processes within applicable facilities through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the position of system components within the applicable facilities. Inspect a diagram of the physical layout of the facilities where relevant information systems and information system resources reside. Identify sensitive areas housing critical system components or concentrations of system resources (e.g., data centers and server rooms). Perform walk-throughs of the facilities where relevant information systems and information system resources reside. Identify the position of system components comprising relevant information systems within the facilities. Consider whether nonessential support entities residing	NIST SP 800-53, PE-18 NIST SP 800-53, PE-19 NIST SP 800-53, PE-21

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	at the facilities are colocated with the system components. See AC.04.01.06 for considerations related to physical access controls. Determine whether system components comprising relevant information systems are positioned within applicable facilities to mitigate the risk of unauthorized access and minimize potential damage from physical and environmental hazards. Note: Entities consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to entity communications. When possible, system components should not be colocated with nonessential support entities (e.g., cafeterias, day cares, bank branches, etc.).	
AC.04.01.03 A list of individuals with authorized access to facilities where systems reside is developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating a list of individuals with authorized access to facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the list of individuals with authorized access to these facilities. Consider whether the list • has been recently reviewed and updated, as appropriate; • has been approved by appropriate senior official(s); and • is adequate to clearly identify individuals with authorized access and the individuals authorizing the access. Inspect the authorized access list and a list of recently separated personnel to verify whether the names of recently separated personnel remained on the authorized access list after their separation dates. Consider the completeness and accuracy of the documentation	NIST SP 800-53, PE-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	obtained, including any system-generated listings of recently separated personnel. Determine whether the list of individuals with authorized access to the facilities where information systems and information system resources relevant to the significant business processes reside has been appropriately documented, periodically reviewed and updated, and properly approved. Note: Individuals with authorized access to facilities may include employees, contractors, and others who routinely need access to facilities where systems reside.	
AC.04.01.04 Physical access authorization credentials are issued to individuals who are authorized to access facilities where systems reside. *Related control: AC.02.02.01*	Obtain an understanding of the entity's process and methods for issuing physical access authorizations credentials through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures. Inspect available documentation for a selection of individuals for whom physical access authorization credentials were issued during the audit period. Observe practices for safeguarding unissued physical access authorization credentials. Determine whether physical access authorization credentials are properly issued to individuals who are authorized to access facilities where systems reside. Note: Physical access authorization credentials include ID badges, identification cards, and smart cards.	NIST SP 800-53, MA-5 NIST SP 800-53, PE-2
AC.04.01.05 Visitors are required to present acceptable identification and may need to comply with certain background screening requirements before accessing facilities where systems reside. Visitors may also need	Obtain an understanding of any entity-level policies or procedures governing visitor access to the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel and	NIST SP 800-53, MA-5 NIST SP 800-53, PE-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
to be escorted by individuals with authorized access to facilities where systems reside.	• inspection of relevant policies and procedures for managing visitor access to applicable facilities. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of individuals who visited the facilities where information systems and information system resources relevant to the significant business processes reside during the audit period. Consider whether • the visitor screening activities performed, including any background screening requirements completed prior to a visitor accessing the facilities, are appropriate based on risk; • the conditions or circumstances requiring visitors to be escorted are consistently applied and appropriate based on risk; and • the maintenance of records associated with visitor access to the facilities is sufficient to demonstrate the performance of applicable control activities associated with a visitor's access. Observe entries to and exits from facilities where information systems and information system resources relevant to the significant business processes reside during and after normal business hours. Determine whether the control activities associated with visitor access to the facilities where relevant information systems and information system resources reside are designed, implemented, and operating effectively to appropriately restrict physical access to facilities to authorized individuals for authorized purposes.	
AC.04.01.06 Physical access authorizations are enforced at entity-defined entry and exit points, as well as interior access points relevant to sensitive areas, for facilities where systems reside through the selection and	Obtain an understanding of the physical access controls employed by the entity for the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel,	NIST SP 800-53, PE-3 NIST SP 800-53, PE-8 NIST SP 800-53, PE-16

Illustrative control activities	Illustrative audit procedures	Relevant criteria
employment of physical access controls based on risk, including • guards and guard posts; • physical access devices and barriers; • physical access logs, including visitor access records, used in conjunction with lists of individuals with authorized access; • requirements for individuals to carry or display ID badges (including visitor badges); and • physical perimeter security checks, patrols, and inspections.	• inspection of relevant documentation, and • observation of the entity's use of physical access controls. Inspect a diagram of the physical layout of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify key facility entry and exit points, as well as key interior access points for sensitive areas housing critical system components or concentrations of system resources (e.g., data centers and server rooms). Perform walk-throughs of the facilities where relevant information systems and information system resources reside. Identify the physical access controls employed by the entity for each of the key facility entry and exit points, as well as key interior access points. Consider whether the selection and employment of physical access controls at each of the key access points is appropriate based on risk. Determine whether the physical access controls at each of the key access points are designed, implemented, and operating effectively. Observe practices for safeguarding physical access devices, such as keys and combinations, applicable to the key access points. Determine whether physical access authorizations are adequately enforced at entity-defined entry and exit points, as well as interior access points relevant to sensitive areas, for the facilities where relevant information systems and information system resources reside. Note: Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical barriers include doors, gates, fences, bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers. Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and the names and organizations of individuals visited.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.04.01.07 Physical access is monitored at entity-defined entry and exit points, as well as interior access points relevant to sensitive areas, for facilities where systems reside through the selection and employment of physical access monitoring controls based on risk, including • guards and guard posts, • video surveillance equipment, and • physical intrusion alarms.	Obtain an understanding of the physical access monitoring controls employed by the entity for the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the entity's use of physical access monitoring controls. Inspect a diagram of the physical layout of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify key facility entry and exit points, as well as key interior access points relevant to sensitive areas housing critical system components or concentrations of system resources (e.g., data centers and server rooms). Perform walk-throughs of the facilities where relevant information systems and information system resources reside. Identify the physical access monitoring controls employed by the entity for each of the key facility entry and exit points, as well as key interior access points. Consider whether the selection and employment of physical access monitoring controls at each of the key access points are appropriate based on risk. Determine whether the physical access monitoring controls at each of the key access points are designed, implemented, and operating effectively. Determine whether physical access is adequately monitored at key entry and exit points, as well as key interior access points relevant to sensitive areas, for the facilities where relevant information systems and information system resources reside. Note: Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors.	NIST SP 800-53, PE-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
AC.04.01.08 Physical access to facilities where systems reside, as well as to sensitive areas within such facilities, is appropriately logged and adequately monitored.	Obtain an understanding of the entity's processes and methods to log and monitor physical access to the facilities where information systems and information system resources relevant to the significant business processes reside, including physical access to sensitive areas housing critical system components or concentrations of system resources within such facilities, through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to log and monitor physical access to the facilities where information systems and information system resources relevant to the significant business processes reside, including physical access to sensitive areas housing critical system components or concentrations of system resources within such facilities. Consider whether such processes and methods • are suitably designed and properly implemented based on risk, • reasonably assure that reports that log management software produces and entity management reviews are complete and accurate, and • reasonably assure that the entity takes appropriate action to identify and address any physical access anomalies. Observe the entity's processes and methods to log and monitor physical access to the facilities where relevant information systems and information system resources reside, including physical access to sensitive areas housing critical system components or concentrations	NIST SP 800-53, PE-6 NIST SP 800-53, PE-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	of system resources within such facilities. Consider the completeness and accuracy of the reports that log management software produces and entity management reviews when performing control tests. Inspect reports produced by log management software. Compare physical access log entries in the reports to authorized access lists or visitor access records, as appropriate. Observe entries to and exits from facilities where relevant information systems and information system resources reside, including sensitive areas housing critical system components or concentrations of system resources within such facilities. Consider whether reports that log management software produces are properly updated as authorized personnel or visitors enter and exit facilities where systems reside, as well as sensitive areas within such facilities. See AC.05.01 and AC.05.02 for additional control activities and audit procedures related to logging and monitoring. Determine whether physical access to facilities where relevant information systems and information system resources reside, including physical access to sensitive areas housing critical system components or concentrations of system resources within such facilities, is appropriately logged and adequately monitored. Note: Reviewing reports that log management software produces detailing physical access log entries can help identify suspicious activity, anomalous events, or potential threats. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.	
AC.04.01.09 Physical access to system distribution and transmission lines is appropriately controlled.	Obtain an understanding of the security controls employed by the entity to control physical access to system distribution and transmission lines within the facilities where information systems and information system resources relevant to the significant business processes reside through	NIST SP 800-53, PE-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the entity's use of security controls applicable to system distribution and transmission lines. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify the security controls employed by the entity to control physical access to system distribution and transmission lines. Consider whether the selection and employment of security controls are appropriate based on risk. Determine whether the entity's security controls for controlling physical access to system distribution and transmission lines are designed, implemented, and operating effectively. Determine whether physical access to system distribution and transmission lines is appropriately controlled. Note: Security controls are applied to system distribution and transmission lines to prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls of physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.	
AC.04.01.10 Physical access to system output devices is appropriately controlled.	Obtain an understanding of the entity's processes and methods to control physical access to system output devices within the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the entity's processes and methods for controlling physical access to system output devices.	NIST SP 800-53, PE-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify the controls employed by the entity to manage physical access to system output devices. Consider whether the selection and employment of such controls are appropriate based on risk. Determine whether the entity's controls for managing physical access to system output devices are designed, implemented, and operating effectively. Determine whether physical access to system output devices is appropriately controlled. Note: Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers. Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and limiting access to authorized individuals only, placing output devices in locations that authorized personnel can monitor, installing monitor or screen filters, and using headphones.	
AC.04.01.11 Physical access to power equipment and cabling is appropriately controlled.	Obtain an understanding of the entity's processes and methods to control physical access to power equipment and cabling for the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the entity's processes and methods for controlling physical access to power equipment and cabling. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify the controls employed by the entity to manage physical access to power equipment and cabling. Consider whether the selection and employment of such controls are appropriate based on risk. Determine whether the entity's controls to	NIST SP 800-53, PE-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	manage physical access to power equipment and cabling are designed, implemented, and operating effectively. Determine whether physical access to power equipment and cabling is appropriately controlled. Note: Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, as well as generators and power cabling outside of buildings.	
AC.05 Management designs and implements detective control activities to appropriately monitor logical and physical access in response to risks.		
AC.05.01 Incidents are properly identified and logged.		
AC.05.01.01 An intrusion detection system, including appropriate placement of intrusion-detection sensors and incident thresholds, is implemented to detect attacks and indicators of potential attacks, as well as unauthorized local, network, or remote connections.	Obtain an understanding of the design of the entity's intrusion detection system through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's intrusion detection tools and software, and • inspection of relevant documentation, such as network maps, policies and procedures for logging, monitoring, and managing the entity's intrusion detection tools and software, and reports or alerts that intrusion detection software produces and entity management reviews. Inspect documentation demonstrating the design and implementation of the entity's intrusion detection system. Consider whether the entity's intrusion detection system • adequately addresses the information systems and information system resources relevant to the significant business processes; • adequately addresses the components of relevant information systems; • adequately addresses the placement of intrusion-detection sensors and incident thresholds;	NIST SP 800-53, SI-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• is suitably designed and properly implemented based on risk; • reasonably assures that reports or alerts produced by intrusion detection software and reviewed by entity management are complete and accurate; and • reasonably assures that appropriate information is provided to entity management to facilitate action in response to attacks or indicators of potential attacks, as well as unauthorized local, network, or remote connections. Determine whether the intrusion detection system is designed, implemented, and operating effectively to detect attacks and indicators of potential attacks, as well as unauthorized local, network, or remote connections.	
AC.05.01.02 A process is established to periodically identify and select event types for logging based on risk. *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, and BP.06.05.03*	Obtain an understanding of any entity-level policies or procedures governing the identification and selection of event types for logging at the software, platform, or infrastructure system sublevels through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to the information systems and information system resources relevant to the significant business processes, including related operating systems and data management systems. Information system resources relevant to the significant business processes also include files, data sets, libraries, and other information system resources critical to achieving information security or information processing objectives. Consider whether the following event types have been selected for logging:	NIST SP 800-53, AU-2 NIST SP 800-53, SA-20

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• remote access (dial-up or broadband) to the information systems and information system resources relevant to the significant business process (see AC.01.01.04); • wireless access to entity networks, network components, information systems, and information system components (see AC.01.01.05); • consecutive attempts to log on with invalid passwords within a certain period (see AC.02.01.11); • concurrent sessions (see AC.02.02.05); • emergency and temporary access to information systems and information system resources (see AC.02.03.06); • access to shared file systems (see AC.02.03.07); • access control parameters (see AC.02.03.09); • the use of privileged accounts (see AC.02.04.02); • logical access to maintenance tools and utilities (see AC.02.04.03); • logical access to authenticators and authentication services and directories (see AC.02.04.05); and • physical access to facilities where systems reside, as well as sensitive areas within such facilities (see AC.04.01.08). Consider whether the event types selected for logging that are applicable to the information systems and information system resources relevant to the significant business processes, including related operating systems and data management systems, are adequate to support appropriate incident response. Determine whether the process established to periodically identify and select event types for logging is designed, implemented, and operating effectively and appropriate based on risk. Note: An event is an observable occurrence. The types of events that require logging are those events that are significant and relevant to the	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	security of information systems and the privacy of individuals. Event types include password changes, failed log-ons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, entities consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the information system.	
AC.05.01.03 All event types selected for logging are logged. *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, and BP.06.05.03*	Obtain an understanding of the entity's processes and methods to reasonably assure that all event types selected for logging are logged through • inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and entity management reviews. Inspect audit records for the event types selected for logging that are applicable to the information systems and information system resources relevant to the significant business processes, including related operating systems and data management systems. Consider the completeness and accuracy of the documentation obtained, including any reports that log management software produces and entity management reviews. Determine whether all event types selected for logging that are applicable to relevant information systems and information system resources are appropriately logged.	NIST SP 800-53, AU-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Audit records can be generated from many different information system components. The event types that the entity selects for logging are those for which audit records are to be generated. The event types selected for logging may be a subset of all event types for which the information system is capable of generating audit records.	
AC.05.01.04 Audit records contain appropriate information for effective review, including sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and any identities associated with the event. *Related control: AC.05.01.02 and AC.05.01.03*	Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Determine whether the audit records contain appropriate information for effective review, including sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and any identities associated with the event. Note: Audit record content that may be necessary to support the auditing function includes event descriptions, time stamps, source and destination addresses, user or process identifiers, success or fail indications, and file names involved. Time stamps generated by the system include date and time. Entities may define different time granularities for different system components. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds).	NIST SP 800-53, AU-3 NIST SP 800-53, AU-8 NIST SP 800-53, SC-45
AC.05.01.05 Audit log storage capacity is allocated to meet audit log retention requirements. In the event of an audit logging process failure, including deficient audit log storage capacity, the system alerts appropriate personnel and personnel take timely, appropriate action.	Obtain an understanding of the entity's processes and methods to reasonably assure that audit log storage capacity is allocated to meet log retention requirements through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log	NIST SP 800-53, AU-4 NIST SP 800-53, AU-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related controls: AC.05.01.02 and AC.05.01.03	management tools and software, as well as implemented configuration settings, found in applicable system configuration files. Inspect implemented storage parameters evidenced by applicable system configuration files and reports produced by log management software to determine whether the allocation of audit log storage capacity is adequate to meet audit log retention requirements. Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Consider whether all required audit records associated with such events are available for inspection. If applicable, inspect available documentation for any instances in which an audit logging process failure occurred during the audit period and determine whether such instances were identified and appropriately resolved on a timely basis. Determine whether audit log storage capacity is allocated to meet audit log retention requirements and whether appropriate action is taken on a timely basis in the event of an audit logging process failure.	
AC.05.01.06 Audit records and audit logging tools are protected from unauthorized access, modification, and deletion. In the event of unauthorized access, modification, or deletion of audit information, the system alerts appropriate personnel and personnel take timely, appropriate action. *Related controls: SD.01.01.01, AC.05.01.02, and AC.05.01.03*	Obtain an understanding of the entity's processes and methods to reasonably assure that audit records and audit logging tools are protected from unauthorized access, modification, and deletion through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as implemented access control parameters.	NIST SP 800-53, AU-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software and log management software to determine whether access to audit records and audit logging tools is appropriately restricted to authorized personnel. Consider whether security administrators who administer access controls also have the ability to access, modify, or delete corresponding audit records or change configuration settings for applicable audit logging tools. Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Consider whether all required audit records associated with such events are available for inspection. If applicable, inspect available documentation for any instances in which unauthorized access, modification, or deletion of audit information occurred and determine whether such instances were identified and appropriately resolved on a timely basis. Determine whether audit records and audit logging tools are protected from unauthorized access, modification, and deletion and whether appropriate action is taken on a timely basis in the event of unauthorized access, modification, or deletion of audit information. Note: Audit information includes all information needed to successfully audit information system activity, such as audit records, audit log settings, reports log management software produces, and personally identifiable information included in such reports. Log management tools and software are those programs and devices used to conduct information system audit and logging activities.	
AC.05.01.07 Audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet legal and entity information retention requirements.	Obtain an understanding of the entity's processes and methods to reasonably assure that audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet legal and regulatory requirements and entity policies on information retention through	NIST SP 800-53, AU-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related controls: AC.05.01.02 and AC.05.01.03	• inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and • inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as implemented configuration settings, found in applicable system configuration files. Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Consider whether all required audit records associated with such events are available for inspection. Determine whether audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet legal and regulatory requirements and entity policies on information retention.	
AC.05.01.08 A process is established for session auditing based on risk.	Obtain an understanding of the entity's process and methods for session auditing through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether such processes and methods • adequately define the situations for which session auditing may be employed, • adequately address the use of personally identifiable information, and • are suitably designed and properly implemented based on risk.	NIST SP 800-53, AU-14

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether the process established for session auditing is designed, implemented, and operating effectively and appropriately based on risk. Note: Session audits can include monitoring keystrokes, tracking websites visited, and recording information and file transfers.	
AC.05.02 Incidents are properly analyzed, and appropriate actions are taken.		
AC.05.02.01 Audit records are regularly reviewed and analyzed for indications of inappropriate or unusual activity, and audit records that indicate suspicious activity or suspected violations are reported and investigated. *Related controls: AC.05.01.02 and AC.05.01.03*	Obtain an understanding of the entity's processes and methods for regularly reviewing and analyzing audit records through • inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; • inspection of relevant policies and procedures for logging, monitoring, and managing log management tools and software; • observation of the processes for regularly reviewing and analyzing audit records; and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Consider whether the actions taken to review and analyze such records, as well as report and investigate suspicious activity or suspected violations, are appropriate for identifying and following up on indications of inappropriate, unusual, or suspicious activity and suspected violations. Consider whether such actions were performed in accordance with the entity's policies and procedures for logging, monitoring, and managing log management tools and software.	NIST SP 800-53, AC-2 NIST SP 800-53, AU-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Consider the completeness and accuracy of the documentation obtained, including any reports that log management software produces, when performing control tests. Determine whether audit records are regularly reviewed and analyzed for indications of inappropriate or unusual activity, and whether audit records that indicate suspicious activity or suspected violations are reported and investigated.	
AC.05.02.02 Investigation results are reported to appropriate personnel, and disciplinary actions are taken when necessary. *Related control: AC.05.02.01*	Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Consider whether any investigation results, as applicable, were reported to appropriate personnel. Consider whether any disciplinary actions taken, as applicable, were appropriate. Determine whether investigation results are reported to appropriate personnel and disciplinary actions are taken when necessary.	NIST SP 800-53, AU-6 NIST SP 800-53, PS-8
AC.05.02.03 Audit records are collected, summarized, and reported in a manner that facilitates review and analysis. Logs with different content and formats are converted to a single standard format with consistent data field representations without altering the original audit records. *Related controls: AC.05.01.02, AC.05.01.03, and AC.05.01.04*	Inspect available audit records for a selection of events that occurred during the audit period applicable to the information systems and information system resources relevant to the significant business processes. Determine whether audit records are collected, summarized, and reported in a manner that facilitates review and analysis. Determine whether logs with different content and formats are converted to a single standard format with consistent data field representations without altering the original audit records.	NIST SP 800-53, AU-7
AC.05.02.04 External and internal security alerts, advisories, and directives are identified and promptly issued to appropriate personnel, who take appropriate action. *Related control: SM.01.05.02*	Obtain an understanding of any entity-level policies or procedures governing the identification and issuance of external and internal security alerts, advisories, and directives through • inquiry of appropriate personnel and • inspection of relevant policies and procedures.	NIST SP 800-53, SI-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of any entity-level policies or procedures governing the identification and issuance of external and internal security alerts, advisories, and directives. Consider whether appropriate action is taken in response to the issuance of external and internal security alerts, advisories, and directives. Determine whether external and internal security alerts, advisories, and directives are identified and promptly issued to appropriate personnel, who take appropriate action.	
AC.05.02.05 A coordinated, cross-entity approach to sharing incident information is implemented. *Related control: SM.03.02.01*	Obtain an understanding of the entity's approach for sharing incident information through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect available documentation demonstrating the implementation of the entity's approach for sharing incident information. Consider whether the entity's approach is appropriately coordinated within and across applicable entity units, including external entities when appropriate. Determine whether a coordinated, cross-entity approach to sharing incident information is implemented. Note: When systems or services of external entities are used, the audit logging capability necessitates a coordinated, cross-entity approach. Entities should consider including processes for coordinating incident information requirements and protection of incident information in information exchange agreements.	NIST SP 800-53, AU-16
AC.05.02.06 Information spills and data losses are identified, isolated, and resolved by appropriate personnel.	Obtain an understanding of the entity's processes and methods to identify, isolate, and resolve information spills and data losses through	NIST SP 800-53, AU-13 NIST SP 800-53, IR-9 NIST SP 800-53, SI-20

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel, including incident response team members, and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to identify, isolate, and resolve information spills and data losses. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that incidents involving information spills and data losses are properly analyzed and appropriate actions are taken. Determine whether information spills and data losses are properly identified, isolated, and resolved by appropriate personnel. Note: Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. Data loss is the unauthorized disclosure of proprietary, sensitive, or classified information through data theft (or exfiltration) and data leakage.	

FISCAM Framework for Segregation of Duties

Table 11. FISCAM framework for segregation of duties.

Illustrative control activities	Illustrative audit procedures	Relevant criteria
SD.01 Management designs and implements control activities 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.01.01.01 Identify, document, and periodically review and update incompatible duties within and across business process (i.e., system user) functions that should not be performed by the same organizational unit or individual. Such duties may include • preparation of data for input into the system, • approval of data for input into the system, • data input, • research and resolution of input data validation errors that the system identified, • research and resolution of data processing errors that the system identified, • reconciliation of interfaced data, and • verification of output data. *Related controls: BP.04.01.02, BP.04.03.07, BP.04.06.02, BP.05.01.02, BP.05.06.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, BP.06.03.05, SM.01.02.03, and SM.02.01.03*	Obtain an understanding of the entity's processes and methods for identifying, documenting, and periodically reviewing and updating incompatible duties within and across business process functions through • inquiry of appropriate personnel and • inspection of relevant documentation. Inquire of appropriate personnel and inspect documentation to determine whether incompatible duties within and across business process functions have been properly identified and adequately documented. In determining whether incompatible duties have been properly identified, consider whether the following are true: • Any business process functions (e.g., billing, cash receipts, purchasing, cash disbursements, and payroll) significant to the engagement objectives are identified as incompatible with other business process functions. • Any specific duties performed by information system users within or across business process functions significant to the engagement objectives are identified as incompatible with other duties. Incompatible duties include initiating and approving transactions and maintaining records and custody of assets. In determining whether incompatible duties have been adequately documented, consider whether incompatible duties have been clearly identified and the rationale for such identification sufficiently explained	NIST SP 800-53, AC-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	to promote a shared understanding of risks among affected organizational units and individuals. Inspect documentation and inquire of appropriate personnel to determine whether documented incompatible duties are periodically reviewed by appropriate personnel and properly updated to reflect changes in the entity's organizational structure, operations, or use of information technology. Consider whether incompatible duties documentation has been recently reviewed and updated. Note: Business process functions comprise the tasks necessary to perform, record, and report on the results of the entity's mission-related operations. Incompatible duties within and across business process functions are documented in position descriptions and policies and procedures. Incompatible duties are also documented within segregation of duties matrices, which may be developed at the entity-level, organizational unit, business process function, and system levels. Segregation of duties matrices facilitate the entity's communication and further identification of incompatible duties.	
SD.01.01.02 Identify, document, and periodically review and update incompatible duties within and across IT management (i.e., system support) functions that should not be performed by the same organizational unit or individual. Such duties may include • information security management, • IT asset management, • system or application design, • system or application programming, • system or application maintenance, • quality assurance testing, • change authorization,	Obtain an understanding of the entity's processes and methods for identifying, documenting, and periodically reviewing and updating incompatible duties within and across IT management functions through • inquiry of appropriate personnel and • inspection of relevant documentation. Inquire of appropriate personnel and inspect documentation to determine whether incompatible duties within and across IT management functions have been properly identified and adequately documented. In determining whether incompatible duties have been properly identified, consider whether the following are true: Any incompatible duties within and across IT management functions are identified. Incompatible duties within and across IT management functions include authorizing, programming, testing, and implementing	NIST SP 800-53, AC-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
• code migration, • configuration auditing, • media management, • production control and scheduling, • application administration, • database administration; • operating system administration, • system administration, • network administration, • security administration, • log management, and • log monitoring. *Related controls: BP.04.03.07, BP.06.03.05, SM.01.02.03, and SM.02.01.03*	changes to relevant information systems and their components, as well as maintaining records and custody of IT assets. For example: • Programmers should not have the ability to migrate code into the production environment and should not have access to production software or data. • Security administrators who administer access controls should not also administer changes to network components, applications, databases, operating systems, or other system resources or components. • Database administrators should not be involved in any IT management functions beyond the duties of database administration. • Security, network, application, database, operating system, and other system administrators should not be responsible for maintaining the entity's log management tools and software or reviewing reports that log management software produces. In determining whether incompatible duties have been adequately documented, consider whether incompatible duties have been clearly identified and the rationale for such identification sufficiently explained to promote a shared understanding of risks among affected organizational units and individuals. Inspect documentation and inquire of appropriate personnel to determine whether documented incompatible duties are periodically reviewed by appropriate personnel and properly updated to reflect changes in the entity's organizational structure, operations, or use of information technology. Consider whether incompatible duties documentation has been recently reviewed and updated. Note: IT management functions comprise the tasks necessary to develop, maintain, and secure the information systems that support the entity's business process functions. Incompatible duties within and across IT management functions are documented in position descriptions and policies and procedures. Incompatible duties are also	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	documented within segregation of duties matrices, which may be developed at the entity-level, organizational unit, IT management function, and system level. Segregation of duties matrices facilitate the entity's communication and further identification of incompatible duties.	
SD.01.02 Incompatible duties are appropriately segregated when possible.		
SD.01.02.01 Segregation of business process (i.e., system user) functions and IT management (i.e., system support) functions, as well as any identified incompatible duties within and across such functions, is enforced by logical and physical access controls.	Obtain an understanding of the entity's processes and methods for employing logical and physical access controls to segregate identified incompatible duties relevant to the significant business processes and areas of audit interest through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of personnel performing business process and IT management functions. Through inquiry, inspection, and observation, identify and assess the adequacy of logical and physical access controls employed to enforce the segregation of identified incompatible duties relevant to the significant business processes. See applicable illustrative control activities and audit procedures within AC.02 and AC.04. Determine whether the segregation of identified incompatible duties relevant to the significant business processes is appropriately enforced by logical and physical access controls. Note: System user functions and system support functions should be segregated whenever possible. For example, information system users should not have the ability to change application code or information system functionality. Additionally, information system users should not have administrative access to the underlying components of such systems, including related operating systems and data management systems. However, only information system	NIST SP 800-53, AC-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	users—not IT management personnel—should have the ability to initiate transactions and authorize changes to transaction data.	
SD.01.02.02 The information system prohibits authorized users from performing incompatible duties within and across the business process functions that the system supports. *Related controls: AC.02.03.01, AC.02.03.02, AC.02.03.05, AC.02.03.09, AC.02.03.10, BP.04.03.07, BP.06.03.05, and CM.02.04.01*[	Obtain an understanding of the processes and methods that the relevant information system employs to prohibit authorized users from performing incompatible duties relevant to the significant business processes through • inquiry of appropriate personnel; • inspection of relevant documentation, including policies and procedures for the significant business processes; and • observation of personnel performing significant business processes. Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system's processes and methods. Consider whether the access privileges or roles assigned to information system users are appropriate to prohibit authorized users from performing incompatible duties. Through inquiry, inspection, and observation, identify and assess the adequacy of configuration management controls enforcing the system's processes and methods. Consider whether workflows or processing routines are appropriately designed and under configuration control to prohibit authorized users from bypassing or overriding segregation of duties controls. Determine whether the system's processes and methods are designed, implemented, and operating effectively to prohibit authorized users from performing incompatible duties relevant to the significant business processes.	NIST SP 800-53, AC-5
SD.01.02.03 The information system prohibits authorized users from performing IT management functions.	Obtain an understanding of the system's processes and methods to prohibit authorized users from performing IT management functions relevant to the significant business processes through • inquiry of appropriate personnel;	NIST SP 800-53, AC-5 NIST SP 800-53, SC-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant documentation, including policies and procedures for the significant business processes; and • observation of personnel performing significant business processes. Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system's processes and methods. Consider whether user functions, including user interface services, are appropriately segregated from IT management functions. Determine whether the system's processes and methods are designed, implemented, and operating effectively to prohibit authorized users from performing IT management functions relevant to the significant business processes. Note: Business process functions comprise the tasks necessary to perform, record, and report on the results of the entity's mission-related operations. These functions include the procedures by which transactions are initiated, recorded, processed, and reported, as well as the procedures by which transaction processing errors are detected and corrected. IT management functions comprise the tasks necessary to develop, maintain, and secure the information systems that support the entity's business process functions. They typically require access to privileged accounts. Preventing the presentation of IT management functions to nonprivileged users at interfaces ensures that administration options, including administrator privileges, are not available to the general user population.	
SD.01.02.04 The information system prohibits IT management personnel from performing business process functions.	Obtain an understanding of the processes and methods that the information system employs to prohibit IT management personnel from performing business process functions relevant to the significant business processes through • inquiry of appropriate personnel;	NIST SP 800-53, AC-5 NIST SP 800-53, SC-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inspection of relevant documentation, including policies and procedures for the significant business processes; and • observation of personnel performing significant business processes. Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system's processes and methods. Consider whether security administrators who administer access controls are prohibited from performing business process functions. Determine whether the system's processes and methods are designed, implemented, and operating effectively to prohibit IT management personnel from performing business process functions relevant to the significant business processes.	
SD.01.02.05 The information system isolates security functions from nonsecurity functions. *Related controls: AC.02.03.05 and AC.02.04.01*	Obtain an understanding of the processes and methods that the information system employs to isolate security functions from nonsecurity functions through • inquiry of appropriate personnel; • inspection of relevant documentation, including policies and procedures for security functions; and • observation of IT management personnel performing security functions. Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system's processes and methods. Consider whether the information system adequately restricts access to security functions through the use of appropriate access control mechanisms and by implementing least privilege capabilities. Determine whether the system's processes and methods are designed, implemented, and operating effectively to isolate security functions from nonsecurity functions relevant to the significant business processes.	NIST SP 800-53, AC-5 NIST SP 800-53, AC-6 NIST SP 800-53, SC-3 NIST SP 800-53, SC-39

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Security functions are isolated from nonsecurity functions using an isolation boundary composed of partitions and domains within an information system. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform security functions. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities.	
SD.01.03 Alternative control activities are implemented to mitigate risks resulting from incompatible duties that cannot be segregated.		
SD.01.03.01 Organizations with limited resources to segregate incompatible duties implement alternative control activities, such as the supervisory review of tasks or the subsequent monitoring of relevant audit records. *Related controls: BP.04.03.07 and BP.06.03.05* *Related critical element:* AC.05	Obtain an understanding of the entity's processes and methods for (1) approving exceptions to segregation of duties requirements and (2) designing and implementing alternative control activities to mitigate risks resulting from incompatible duties that cannot be segregated through • inquiry of appropriate personnel and • inspection of relevant documentation. Inquire of appropriate personnel to obtain an understanding of any approved exceptions to segregation of duties requirements. Inspect documentation for any approved exceptions to segregation of duties requirements relevant to the significant business processes and areas of audit interest. Consider whether the documentation for any such exceptions • has been recently reviewed and updated; • describes the current status of any mitigating factors or compensating controls cited as part of the entity's approval of the exception; • accurately describes the impact of the exception on business process and IT management functions, as well as information systems and common controls available for inheritance, to enable senior management and authorizing officials to assess risk and determine whether the mitigating factors or	NIST SP 800-53, AC-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	compensating controls sufficiently reduce risk to an acceptable level; and • demonstrates that the exception was properly approved in accordance with the entity's procedures. Obtain an understanding of any compensating controls or alternative control activities cited as part of the entity's approval of relevant exceptions through • inquiry of appropriate personnel; • inspection of relevant documentation, including policies and procedures; and • observation of the entity's application of compensating controls. Determine whether the compensating controls or alternative control activities are designed, implemented, and operating effectively to mitigate the risks associated with incompatible duties that cannot be separated. Determine whether entity management appropriately considered and accepted any residual risks associated with exceptions to segregation of duties requirements.	

FISCAM Framework for Configuration Management

Table 12. FISCAM framework for configuration management.

Illustrative control activities	Illustrative audit procedures	Relevant criteria
CM.01 Management designs and implements control activities 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.01.01.01 System-level configuration management plans are developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level configuration management plans through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect the system-level configuration management plans for each of the information systems relevant to the significant business processes. Consider whether the plans • identify roles and responsibilities; • incorporate or reference current entity-level configuration management policies and procedures; • define configuration items for the information system and place such items under configuration management; • establish a process for identifying configuration items throughout the system development life cycle; • establish processes for managing the configuration of these items for the information system and monitoring implemented configuration settings against baseline configurations; • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); • include required information in accordance with authoritative criteria; and	NIST SP 800-53, CM-2 NIST SP 800-53, CM-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are adequate to address configuration management activities applicable to the information system, including any changes to the baseline configuration of the system. Determine whether the system-level configuration management plans for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, consider whether the system-level configuration management plans for relevant information systems have been implemented. Note: Configuration management plans satisfy the requirements in entity-level configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities. The plans are generated during the development and acquisition stages of the system development life cycle. The plans describe how to advance changes through change management processes; update implemented configuration settings and baseline configuration settings; maintain information system component inventories; control development, test, and operational environments; and maintain system documentation.	
CM.01.01.02 Management selects, tests, and implements configuration settings that optimize the security features of the system and minimize available processes and services consistent with operational requirements and management's baseline configuration. *Related control: CM.01.01.03*	Obtain an understanding of the entity's processes and methods for selecting, testing, and implementing configuration settings for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for selecting, testing, and implementing configuration settings for information systems and information system components.	NIST SP 800-53, CM-6 NIST SP 800-53, CM-7 NIST SP 800-53, SA-4 NIST SP 800-53, SA-8 NIST SP 800-53, SA-23 NIST SP 800-53, SC-25 NIST SP 800-53, SC-29 NIST SP 800-53, SC-34

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the implemented configuration settings for a selection of configuration items for relevant information systems. Consider whether the implemented configuration settings • optimize the system's security features; • minimize available processes and services consistent with operational requirements; • align with entity-level requirements, including any entity-defined common secure configurations; and • are consistent with the corresponding baseline configuration settings. Determine whether the implemented configuration settings for the configuration items selected have been properly selected, tested, and implemented. Throughout the engagement, consider whether the implemented configuration settings for the relevant information systems are appropriate for optimizing the systems' security features and minimizing available processes and services consistent with operational requirements. Note: Deploying information system components with minimal functionality reduces the need to secure every end point and may reduce the exposure of information, systems, and services to attacks. It may be necessary to enhance or augment the security features of an information system or component that supports critical or essential mission and business functions to maximize the trustworthiness of the resource. Data execution prevention controls can be implemented to protect the information system from adversaries that launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited.	NIST SP 800-53, SC-51 NIST SP 800-53, SI-14 NIST SP 800-53, SI-16 NIST SP 800-53, SI-21

Illustrative control activities	Illustrative audit procedures	Relevant criteria
CM.01.01.03 Baseline configurations of systems are developed, documented, and periodically reviewed and updated. *Related control: CM.01.01.02*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating baseline configurations of systems through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for maintaining baseline configurations of systems. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the baseline configurations for the information systems relevant to the significant business processes. Consider whether the baseline configurations • are under configuration control; • are adequate to serve as a basis for future builds, releases, or changes to the information systems; • are based on documented configuration change decisions and reflect the existing enterprise architecture; • include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture; • have been recently reviewed and updated, as appropriate; and • have been approved by the appropriate senior official(s). Determine whether the baseline configurations for the relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, consider whether the baseline configurations for relevant information systems have been properly maintained.	NIST SP 800-53, CM-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Baseline configurations for information systems and information system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Automated mechanisms that help entities maintain consistent baseline configurations for systems include configuration management tools; hardware, software, and firmware inventory tools; and network management tools. Automated tools can be used at the entity, system, or business process levels and applied to workstations, servers, notebook computers, network components, or mobile devices.	
CM.01.01.04 System documentation for administrators and users is developed, documented, and periodically reviewed and updated. *Related controls: SM.02.02.03, SM.02.03.03, and AC.02.03.03*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system documentation for administrators and users through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for maintaining system documentation. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the system documentation for administrators and users of the information systems relevant to the significant business processes. Consider whether the documentation • is appropriately protected commensurate with the security categorization of the information system; • accurately describes for administrators the secure configuration, installation, and operation of the information system and their components, as well as the effective use and maintenance of security and privacy mechanisms and any known vulnerabilities associated with administrative functions;	NIST SP 800-53, SA-4 NIST SP 800-53, SA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• accurately describes for users any user-accessible security and privacy mechanisms and their use, as well as user responsibilities for maintaining the security of the system and the privacy of individuals; • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); • includes required information in accordance with authoritative criteria; and • has been distributed to appropriate personnel. Determine whether system documentation for administrators and users of relevant information systems has been appropriately documented, periodically reviewed and updated, and properly approved. Note: Entities may require different levels of detail in the documentation for the design and implementation of controls in information systems, information system components, or information system services. The levels of detail are based on mission and business function requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. System documentation helps personnel understand the implementation and operation of controls. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, program or software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system. When adequate documentation cannot be obtained from manufacturers or suppliers of information systems, information system components, or information system services, entities may need to recreate the documentation relevant to the implementation or operation of the controls.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
CM.01.02 An inventory of information system components is developed and maintained.		
CM.01.02.01 An inventory of system components is developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating inventories of information system components through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for maintaining information system component inventories. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the inventories of components for relevant information systems. Consider whether each inventory • accurately reflects the information system; • includes records for all components for the information system; • does not include duplicate records for any components; • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); and • includes required information in accordance with authoritative criteria and in sufficient detail to promote accountability for information system components. Reconcile inventory records to any listings of information system components included in other information system documentation, such as information security and privacy plans, baseline configurations, or other system documentation. For a selection of inventory records, perform audit procedures to verify the accuracy and validity of the records. When verifying the accuracy and validity of inventory records related to hardware, consider whether the associated hardware components are appropriately marked to	NIST SP 800-53, CM-2 NIST SP 800-53, CM-8 NIST SP 800-53, PE-22

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	identify the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component. Determine whether the inventories of components for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved. Note: An information system component is a discrete identifiable IT asset that represents a building block of a system and may include hardware, software, and firmware. Entities may choose to implement centralized information system component inventories that include components for all entity information systems. In such situations, entities ensure that the inventories include system-specific information required for component accountability. Information system component inventories are subject to configuration management policies and procedures, and changes to inventory records generally require an appropriate senior official's approval. Identifying individuals who are responsible and accountable for administering information system components ensures that the assigned components are properly administered and that entity personnel can contact those individuals if some action is required. System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.	
CM.01.02.02 Unauthorized system components are detected and appropriately addressed on a timely basis.	Obtain an understanding of the entity's processes and methods for detecting and addressing unauthorized information system components through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for monitoring the baseline configurations for information systems.	NIST SP 800-53, CM-2 NIST SP 800-53, CM-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Observe appropriate personnel as they perform procedures for detecting and addressing unauthorized information system components. Obtain an understanding of any automated tools the entity uses to facilitate the detection of unauthorized information system components. If automated tools are used, perform appropriate audit procedures to assess whether such tools are properly configured and appropriately employed to detect unauthorized system components and alert appropriate personnel. Inspect available documentation for a selection of instances in which the entity detected unauthorized information system components. Consider whether appropriate actions were taken to address these components on a timely basis. Determine whether unauthorized system components are detected and appropriately addressed on a timely basis. Note: Entities can improve the accuracy, completeness, and consistency of information system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. Monitoring for unauthorized information system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to entity systems contributes to providing adequate security. Entities may combine information system component inventory and baseline configuration monitoring activities.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
CM.01.02.03 Counterfeit system components are detected and appropriately addressed on a timely basis. *Related control: CM.03.03.02*	Obtain an understanding of the entity's processes and methods for detecting and addressing counterfeit information system components through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for determining the authenticity of information system components prior to installation. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Observe appropriate personnel as they perform procedures for detecting and addressing counterfeit information system components. Inspect available documentation for a selection of instances in which the entity detected counterfeit information system components. Consider whether appropriate actions were taken to address these components on a timely basis. Determine whether counterfeit information system components are detected and appropriately addressed on a timely basis. Note: Sources of counterfeit information system components include manufacturers, developers, vendors, and contractors. Entities develop policies and procedures to detect, address, and report counterfeit information system components.	NIST SP 800-53, SR-9 NIST SP 800-53, SR-10 NIST SP 800-53, SR-11
CM.01.03 Configuration items for information systems are identified and placed under configuration management.		
CM.01.03.01 The types of configuration items for information systems are clearly defined.	Inspect the system-level configuration management plans for each of the information systems relevant to the significant business processes, as applicable. Determine whether the types of configuration items for relevant information systems are clearly defined. Note: In order to properly identify configuration items, it is important that the entity define the configuration items for entity information	NIST SP 800-53, CM-2 NIST SP 800-53, CM-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	systems. A configuration item is an information system component or an aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process. Configuration items are the information system components, such as the hardware, software, firmware, and documentation that are placed under configuration management.	
CM.01.03.02 Configuration items for information systems are identified and placed under configuration management.	Obtain an understanding of the entity's processes and methods to identify configuration items for information systems and place these items identified under configuration management through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for identifying configuration items and managing the configuration of configuration items. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to identify configuration items for information systems and place the items identified under configuration management. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that configuration items for information systems are properly identified and placed under configuration management. Inspect listings of configuration items for the information systems relevant to the significant business processes. Determine whether configuration items for relevant information systems are properly identified and placed under configuration management.	NIST SP 800-53, CM-2 NIST SP 800-53, CM-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Note: Configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.	
CM.01.04 Baseline configuration settings are developed and documented for configuration items.		
CM.01.04.01 Baseline configuration settings are developed, documented, and periodically reviewed and updated. *Related control: CM.02.03.01*	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating baseline configuration settings for configuration items through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for establishing baseline configuration settings for information systems and information system components that align with entity-level requirements. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the baseline configuration settings for a selection of configuration items for the information systems relevant to the significant business processes. Consider whether these settings • reflect the most restrictive mode consistent with operational requirements; • align with entity-level requirements, including any entity-defined common secure configurations; • have been recently reviewed and updated, as appropriate;	NIST SP 800-53, CM-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• have been approved by the appropriate senior official(s); and • are consistent with implemented configuration settings. Determine whether the baseline configuration settings for the configuration items selected have been appropriately documented, periodically reviewed and updated, and properly approved. Throughout the engagement, consider whether the baseline configuration settings for the configuration items for relevant information systems have been properly maintained. Note: Entities establish entity-level configuration settings and subsequently determine specific configuration settings for the items that make up information systems and information system components. The established settings become part of the configuration baseline for the system. Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for IT products and platforms. They also provide instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including IT product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.	
CM.02 Management designs and implements control activities 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.02.01.01 Entity-level and system-level processes for formally authorizing, testing, and approving planned changes to	Obtain an understanding of the entity and system-level processes and methods employed by the entity for formally authorizing,	NIST SP 800-53, CM-3 NIST SP 800-53, SA-10 NIST SP 800-53, SA-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
information systems and information system components are established and implemented. *Related controls: SM.01.04.01 and CM.03.02.01*	testing, and approving planned changes to information systems and information system components through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity and system-level processes. Consider whether the processes • identify roles and responsibilities; • are integrated with the entity's system development life cycle processes; • address each type of change to information systems and information system components that is configuration controlled and subject to the entity and system-level processes, as applicable; • specify the processes and methods employed for authorizing, testing, and approving planned changes to information systems and information system components, as well as retaining records of such actions for subsequent review and monitoring; • specify the processes and methods for updating baseline configuration documentation as part of the change management process; • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and	NIST SP 800-53, SA-15 NIST SP 800-53, SA-17

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are adequate to facilitate and document controlled modifications to hardware, firmware, and software components of entity information systems. Inspect a selection of changes to configuration items for each of the information systems relevant to the significant business processes. Determine whether the entity and system-level processes for formally authorizing, testing, and approving planned changes to information systems and information system components are effectively designed and implemented to reasonably assure that changes to configuration items are appropriately controlled. Note: Changes to information systems include modifications to hardware, software, or firmware components as well as to configuration settings. Processes and methods for managing changes to information systems and information system components include establishing configuration control boards or change advisory boards that review and approve proposed changes to configuration items.	
CM.02.01.02 Management authorizes proposed changes to software for development. *Related control: BP.04.07.01*	Obtain an understanding of the entity's processes and methods for considering proposed changes to software for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. Inspect available documentation for any changes to software for the information systems relevant to the significant business processes that were implemented (or are expected to be implemented) during the audit period. Consider whether the documentation • demonstrates that proposed changes are considered and authorized prior to development and • facilitates tracing of source code to the design specifications and functional requirements associated with authorized changes.	NIST SP 800-53, SA-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether management has authorized proposed changes to software for relevant information systems for development.	
CM.02.01.03 Security and privacy impact analyses are conducted and the results are documented, approved, and disseminated prior to the implementation of planned changes.	Obtain an understanding of the entity's processes and methods for conducting security and privacy impact analyses and documenting, approving, and disseminated results through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect any security or privacy impact analyses conducted in connection with planned changes to the information systems relevant to the significant business processes. Consider whether such analyses • have been appropriately documented, approved and disseminated and • are appropriately considered as part of the processes for formally authorizing, testing, and approving planned changes to information systems and information system components. Determine whether security and privacy impact analyses are properly conducted and the results are appropriately documented, approved, and disseminated prior to the implementation of planned changes. Note: Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to	NIST SP 800-53, CM-4 NIST SP 800-53, RA-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required. A privacy impact assessment analyzes how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks.	
CM.02.01.04 Planned changes to information systems and information system components, including authorized changes to software, are properly tested, and flaws identified through testing are appropriately remediated.	Obtain an understanding of the entity's processes and methods for testing planned changes to information systems and information system components, including authorized changes to software, for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. Inspect available documentation for any changes to the information systems relevant to the significant business processes that were implemented (or are expected to be implemented) during the audit period. Consider whether the documentation • provides sufficient evidence of the approval, execution, and review of test plans and results, as appropriate; • demonstrates that a comprehensive set of test transactions and data was developed and used in testing to represent the various activities and conditions that are likely to be encountered in the production environment; • clearly presents the results of testing, including any flaws identified; • identifies the necessary resources, planned actions, and time frames for flaw remediation; and	NIST SP 800-53, SA-11

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• demonstrates that planned changes to information systems and information system components, including authorized changes to software, are only implemented into the production environment by authorized personnel after management approval. Inspect available documentation for flaw remediation. Consider whether all flaws identified through testing are remediated or tracked for remediation. Determine whether planned changes to information systems and information system components, including authorized changes to software, are properly tested. Determine whether flaws identified through testing are appropriately remediated. Note: Unit testing, integration testing, and regression testing, as well as security and privacy control assessments, are generally performed. Manual code reviews, as well as static code analysis and dynamic code analysis, may also be performed to assess changes to custom software for business process applications. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risks to entities. Entities can minimize such risks by developing and using a comprehensive set of test transactions and data during the development and testing of changes to information systems, information system components, and information system services.	
CM.02.01.05 Management employs appropriate tools and software to support the entity's system development and configuration management processes.	Obtain an understanding of the tools and software employed by the entity to support the system development and configuration management processes applicable to the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's system development and configuration management tools and software, and • inspection of relevant documentation, such as policies and procedures for using and managing the entity's system	NIST SP 800-53, SA-15

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	development and configuration management tools and software, as well as implemented configuration settings, found in system configuration files for the tools and software employed. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the implemented configuration settings for the system development and configuration management tools and software employed in connection with relevant information systems and their components. Consider whether the implemented configuration settings are appropriate. Determine whether management properly employs appropriate tools and software to support the entity's system development and configuration management processes applicable to relevant information systems. Note: System development and configuration management tools and software are often employed to produce audit trails of program or software changes; maintain version control of hardware descriptions, source code, and object code; track version numbers on operating systems, applications, programs, and software implemented; log and monitor changes to information system components; remove previous versions of software or firmware components of information systems from the production environment; maintain the composition of open source and proprietary source code, including the current version; securely archive copies of previous versions; and control concurrent updates to information system components.	
CM.02.02 Emergency changes to configuration items are documented, analyzed, and reviewed.		
CM.02.02.01 Entity-level and system-level processes for documenting, analyzing, and reviewing emergency changes to information	Obtain an understanding of the entity-level and system-level processes and methods employed by the entity for documenting,	NIST SP 800-53, CM-3 NIST SP 800-53, SA-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
systems and information system components are established and implemented. *Related controls: SM.01.04.01 and CM.03.02.01*	analyzing, and reviewing emergency changes to information systems and information system components through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity and system-level processes. Consider whether the processes • identify roles and responsibilities; • are integrated with the entity's system development life cycle processes; • define emergency changes and address each type of change to information systems and information system components that is subject to the entity and system-level processes for implementing emergency changes, as applicable; • specify the processes and methods employed for documenting and analyzing emergency changes to information systems and information system components and retaining records of such changes for subsequent review and monitoring; • specify the processes and methods for updating baseline configuration documentation as part of the change management process; • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and	NIST SP 800-53, SA-11 NIST SP 800-53, SA-15 NIST SP 800-53, SA-17

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are adequate to facilitate and document controlled modifications to hardware, firmware, and software components of entity information systems in emergency situations where formal authorization, testing, and approval procedures are not feasible. Inspect a selection of emergency changes to configuration items for each of the information systems relevant to the significant business processes. Determine whether the entity and system-level processes for documenting, analyzing, and reviewing emergency changes to information systems and information system components are effectively designed and implemented to reasonably assure that emergency changes to configuration items are appropriately controlled. Note: Making emergency changes often involves using sensitive system utilities or methods that grant much broader access than would normally be needed. It is important that such access is strictly controlled and that its use is promptly reviewed. Shortly after an emergency change is made, the usual configuration management controls are applied retroactively. The change is subjected to the same review, testing, and approval processes that apply to scheduled changes. In addition, data center management or security administrators periodically review logs of emergency changes and related documentation to determine whether all such changes have been tested and have received final approval.	
CM.02.03 Information systems and information system components are routinely monitored for deviations from baseline configuration settings and unauthorized changes.		
CM.02.03.01 Deviations from baseline configuration settings are properly identified and appropriately addressed on a timely basis.	Obtain an understanding of the entity's processes and methods for identifying and addressing deviations from baseline configuration settings through • inquiry of appropriate personnel and	NIST SP 800-53, CM-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
Related control: CM.01.04.01	• inspection of relevant documentation, such as comparing policies and procedures for monitoring implemented configuration settings for information systems and information system components against baseline configuration settings, including any such settings derived from entity-defined common secure configurations. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Observe appropriate personnel as they perform procedures for identifying and addressing deviations from baseline configuration settings. Obtain an understanding of any automated tools the entity uses to facilitate compliance with baseline configuration settings, including those derived from common secure configurations. If automated tools are used, perform appropriate audit procedures to assess whether such tools are properly configured and appropriately employed to identify deviations from baseline configuration settings and alert appropriate personnel. Inspect available documentation for a selection of deviations that the entity identified. Consider whether appropriate actions were taken to address the deviations on a timely basis. Such actions may include • changing implemented configuration settings for configuration items through a formal configuration management process, • addressing the deviation through the entity's process for managing plans of action and milestones to document and communicate the actions necessary to fully address the deviation, or • approving the deviation and accepting the risk associated with it.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect implemented configuration settings for a selection of configuration items for the information systems relevant to the significant business processes. Consider whether the implemented settings align with the baseline configuration settings for the configuration items. Determine whether deviations from baseline configuration settings are properly identified and appropriately addressed on a timely basis. Note: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. IT products for which configuration settings can be defined include servers, workstations, operating systems, mobile devices, input and output devices, protocols, and applications. Common secure configurations include the United States Government Configuration Baseline and security technical implementation guides. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method for uniquely identifying, tracking, and controlling configuration settings.	
CM.02.03.02 The correct operation of security and privacy functions provided by systems or system components is periodically verified, and appropriate action is taken when anomalies are identified.	Obtain an understanding of the entity's processes and methods for periodically verifying security and privacy functions, which relevant information systems provide, are operating correctly through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for verifying security and privacy functions provided by information systems and information system components, as well as addressing any anomalies identified through security and privacy function verification. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.	NIST SP 800-53, SI-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Observe appropriate personnel as they perform procedures for verifying the correct operation of security and privacy functions provided by relevant information systems and their components. Consider whether such procedures address transitional states for information systems and information system components, including system startup, restart, shutdown, and abort. Obtain an understanding of any automated tools the entity uses to facilitate security and privacy function verification. If automated tools are used, perform appropriate audit procedures to assess whether such tools are properly configured and appropriately employed to identify anomalies. Determine whether the correct operation of security and privacy functions that systems or their components provide is periodically verified and appropriate action is taken when anomalies are identified.	
CM.02.03.03 Management employs integrity verification tools to detect unauthorized changes to systems and system components. *Related controls: BP.04.07.03 and BP.06.06.05*	Obtain an understanding of the entity's processes and methods for detecting unauthorized changes to systems and system components through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's integrity verification tools, and • inspection of relevant documentation, such as policies and procedures for using and managing the entity's integrity verification tools, as well as implemented configuration settings, found in system configuration files for the tools employed. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for a selection of instances in which management reviewed the output of the entity's integrity verification tools employed in connection with relevant information	NIST SP 800-53, SI-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	systems and their components. Consider whether appropriate personnel properly reviewed such output and took appropriate, timely action to address any unauthorized changes detected. Inspect the implemented configuration settings for the integrity verification tools employed in connection with relevant information systems and their components. Consider whether the implemented configuration settings are appropriate for detecting unauthorized changes to systems and system components. Determine whether management properly employs integrity verification tools to detect unauthorized changes to systems and their components. Note: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.	
CM.02.04 Logical access controls relevant to configuration management are selected and employed based on risk.		
CM.02.04.01 The development, test, integration, and production environments are sufficiently separated and appropriately controlled.	Obtain an understanding of the entity's processes and methods to separate and control access to the development, test, integration, and production environments for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system design documentation, system security and privacy plans, and system-level configuration management plans. Inspect documentation demonstrating the design and implementation of the entity's processes and methods to separate and control access to the development, test, integration, and production environments for relevant information systems. Consider whether such processes and methods	NIST SP 800-53, SA-3 NIST SP 800-53, SC-32 NIST SP 800-53, SC-49 NIST SP 800-53, SC-50

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are suitably designed and properly implemented based on risk; • facilitate segregation of duties for program development and implementation, including the movement of programs between environments; and • reasonably assure that the development, test, integration, and production environments are sufficiently separated and appropriately controlled. Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports that access control software produces to determine whether access to the development, test, integration, and production environments for relevant information systems is appropriately restricted to authorized personnel. Determine whether the development, test, integration, and production environments for relevant information systems are sufficiently separated and appropriately controlled. Note: Information system preproduction environments (i.e., development, test, and integration) are protected commensurate with risk throughout the system development life cycle for the information system, information system component, or system service.	
CM.02.04.02 Source code repositories and program libraries are sufficiently separated and appropriately controlled.	Obtain an understanding of the entity's processes and methods to separate and control access to source code repositories and program libraries for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation, such as system design documentation, system security and privacy plans, and system-level configuration management plans.	NIST SP 800-53, CM-5 NIST SP 800-53, SA-8 NIST SP 800-53, SA-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect documentation demonstrating the design and implementation of the entity's processes and methods to separate and control access to source code repositories and program libraries for relevant information systems. Consider whether such processes and methods • are suitably designed and properly implemented based on risk and • reasonably assure that source code repositories and program libraries are sufficiently separated and appropriately controlled. Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports that access control software produces to determine whether access to source code repositories and program libraries for relevant information systems is appropriately restricted to authorized personnel. Determine whether source code repositories and program libraries for relevant information systems are sufficiently separated and appropriately controlled. Note: Source code is a set of computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator. Source code is written by a programmer in a programming language that humans can read and understand. Source code is ultimately translated into object code, which a computer can read. Programs, or computer programs, are complete sets of ordered instructions that a computer executes to perform a specific operation or task.	
CM.02.04.03 Logical access to the tools and software that support the entity's system development and configuration management processes is appropriately controlled.	Obtain an understanding of the entity's processes and methods to control logical access to the entity's system development and configuration management tools and software through	NIST SP 800-53, CM-5 NIST SP 800-53, SA-3

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• inquiry of appropriate personnel, including IT management personnel responsible for the entity's system development and configuration management tools and software, and • inspection of relevant documentation, such as policies and procedures for the entity's system development and configuration management processes. Inspect implemented access control parameters evidenced by applicable access control lists or system configuration files for the entity's system development and configuration management tools. Determine whether logical access to the tools and software that support the entity's system development and configuration management processes is appropriately controlled.	
CM.03 Management designs and implements control activities to protect information systems and information system components from vulnerabilities, flaws, and threats.		
CM.03.01 Vulnerability monitoring is routinely conducted.		
CM.03.01.01 Entity-level and system-level processes for vulnerability monitoring and scanning are established and implemented. *Related controls: SM.04.01.01, SM.04.01.02, and SM.06.01.01*	Obtain an understanding of the entity-level and system-level processes and methods employed by the entity for conducting vulnerability monitoring and scanning for relevant information systems and their components through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity and system-level processes. Consider whether the processes • identify roles and responsibilities;	NIST SP 800-53, RA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are integrated with the entity-level risk management strategy, as well as the entity and system-level continuous monitoring strategies, as applicable; • specify the processes and methods employed for vulnerability monitoring and scanning and for analyzing results from vulnerability monitoring and vulnerability scan results; • specify the processes and methods for sharing information obtained from the vulnerability monitoring and scanning processes with appropriate personnel to help eliminate similar control deficiencies and vulnerabilities in other information systems; • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and • are adequate to facilitate the proper identification and timely remediation of control deficiencies and vulnerabilities. Determine whether the entity and system-level processes for vulnerability monitoring and scanning for relevant information systems and their components are designed, implemented, and operating effectively. Note: Entities establish required vulnerability monitoring and scanning processes for information system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, and sensors), networked printers, scanners, and copiers—are not overlooked. Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include using continuous	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	vulnerability monitoring tools that employ instrumentation to continuously analyze information system components. Instrumentation-based tools may improve accuracy and may be run throughout an entity without scanning.	
CM.03.01.02 Management employs appropriate tools and software to support the entity's vulnerability monitoring and scanning processes.	Obtain an understanding of the tools and software employed by the entity to support the vulnerability monitoring and scanning processes applicable to the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including IT management personnel responsible for the entity's vulnerability monitoring and scanning tools and software, and • inspection of relevant documentation, such as policies and procedures for using and managing the entity's vulnerability monitoring and scanning tools and software, as well as implemented configuration settings, found in system configuration files for the tools and software employed. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the implemented configuration settings for the vulnerability monitoring and scanning tools and software employed in connection with relevant information systems and their components. Consider whether the implemented configuration settings are appropriate. Determine whether management properly employs appropriate tools and software to support the entity's vulnerability monitoring and scanning processes applicable to relevant information systems. Note: The capability to readily update vulnerability monitoring tools and software as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not overlooked. Properly maintaining and updating vulnerability monitoring tools and software also helps to	NIST SP 800-53, RA-5

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	ensure that potential vulnerabilities in information systems and information system components are identified and addressed as quickly as possible. Vulnerability monitoring tools and software that facilitate interoperability include tools that are SCAP-validated. Entities may employ scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures naming convention and that use the Open Vulnerability Assessment Language to determine the presence of vulnerabilities. Entities may also employ scanning tools that express vulnerability impact using the Common Vulnerability Scoring System. Sources for vulnerability information include the Common Weakness Enumeration listing and the National Vulnerability Database.	
CM.03.02 Critical updates and patches for information systems are implemented and unsupported information system components are replaced on a timely basis.		
CM.03.02.01 Entity-level and system-level processes for flaw remediation, including patch management, are established and implemented. *Related controls: CM.02.01.01, CM.02.02.01, SM.04.01.01, SM.04.01.02, and SM.06.01.01*	Obtain an understanding of the entity-level and system-level processes and methods employed by the entity for flaw remediation, including patch management, for relevant information systems and their components through • inquiry of appropriate personnel, • inspection of relevant policies and procedures, and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity and system-level processes. Consider whether the processes • identify roles and responsibilities;	NIST SP 800-53, SI-2

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are integrated with the entity-level risk management strategy, as well as the entity and system-level continuous monitoring strategies, as applicable; • are incorporated into the entity's configuration management processes, including the entity and system-level processes for managing planned and emergency changes to information systems and information system components; • specify the processes and methods employed for timely flaw remediation, including patch management; • have been recently reviewed and updated, as appropriate; • have been approved by the appropriate senior official(s); and • are adequate to facilitate the proper identification and timely remediation of control deficiencies and vulnerabilities. Inspect a selection of vendor-recommended patches and compare to those installed on relevant information systems. Consider whether all available patches have been installed and conduct follow-up with management on any exceptions. Determine whether the entity and system-level processes for flaw remediation, including patch management, for relevant information systems and their components are designed, implemented, and operating effectively. Note: The need to remediate system flaws applies to all types of software and firmware. Entities identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to appropriate personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures.	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. The time periods for flaw remediation may vary based on a variety of risk factors, including the security categorization of the information system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission or business functions that the information system supports, or the threat environment. Some types of flaw remediation may require more testing than others. Entities determine the nature and extent of testing needed for the specific type of flaw remediation activity under consideration. In making this determination, entities consider the types of changes that are configuration controlled and subject to the entity and system-level processes for managing planned and emergency changes to information systems and information system components. In some situations, entities may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates.	
CM.03.02.02 Unsupported system components are replaced, or alternative sources for continued support are identified and employed.	Obtain an understanding of the entity's processes and methods for replacing unsupported system components or identifying and employing alternative sources for continued support for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. Inspect the inventory of information system components for relevant information systems, as well as listings of configuration items for such systems. Identify any information system components that have reached, or are approaching, end-of-life and are not, or will no longer be, supported by the developer, vendor, or manufacturer.	NIST SP 800-53, SA-22

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Consider whether such components are scheduled for replacement or supported by other means through alternative sources. Determine whether unsupported system components are replaced or alternative sources for continued support are identified and employed on a timely basis. Note: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.	
CM.03.03 Information systems and information system components are protected from spam and malicious code.		
CM.03.03.01 Spam and malicious code protection mechanisms are selected and employed based on risk.	Obtain an understanding of any entity-level policies or procedures governing the selection of spam and malicious code protection mechanisms through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of spam and malicious code protection mechanisms selected for use in connection with relevant information systems and their components. Determine whether the spam and malicious code protection mechanisms selected for use in connection with relevant	NIST SP 800-53, SC-35 NIST SP 800-53, SI-3 NIST SP 800-53, SI-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	information systems and their components are appropriate based on risk. Note: Spam is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as image steganography. Spam and malicious code protection mechanisms are implemented at system entry and exit points, which include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices.	
CM.03.03.02 Management prevents the installation of software and firmware components lacking recognized and approved digital signature certificates. *Related control: CM.01.02.03*	Obtain an understanding of any entity-level policies or procedures governing the use of signed information system components through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Consider whether the policies and procedures • identify roles and responsibilities; • are incorporated into or referenced by the entity's configuration management processes, including the entity-level and system-level processes for managing planned and emergency changes to information systems and information system components; • specify the processes and methods employed to validate that software and firmware components have been digitally signed using a certificate that the entity recognized and approved prior to installation;	NIST SP 800-53, CM-14

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• have been recently reviewed and updated; • have been approved by the appropriate senior officials; and • are adequate to prevent unsigned software and firmware components from being installed. Inspect a selection of software and firmware components for the information systems relevant to the significant business processes. Consider whether such components are signed with an entity-approved certificate. Determine whether management adequately prevents the installation of software and firmware components lacking recognized and approved digital signature certificates for relevant information systems. Note: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input and output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures are methods of code authentication.	

FISCAM Framework for Contingency Planning

Table 13. FISCAM framework for contingency planning.

Illustrative control activities	Illustrative audit procedures	Relevant criteria
CP.01 Management designs and implements control activities 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.01.01.01 Management performs criticality analyses for systems, system components, and system services.	Obtain an understanding of management's process for conducting and documenting criticality analyses through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the results of criticality analyses performed for the information systems, information system components, and information system services relevant to the significant business processes. Consider whether management's assumptions based on its analyses are reasonable and whether such assumptions are appropriately documented. Additionally, consider whether criticality analyses are updated when significant changes are made to the corresponding systems, system components, or system services. Determine whether the criticality analyses for the information systems, information system components, and information system services relevant to the significant business processes were properly performed and appropriately documented. Note: Criticality analyses may also be performed for business process applications. Large or complex information systems supporting multiple mission and business functions may include multiple business process applications. System engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes identification of	NIST SP 800-53, RA-9 NIST SP 800-53, SA-20

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	organizational missions a system supports; decomposition into the specific functions to perform those missions; and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system. For critical system components that cannot be trusted due to specific threats to and vulnerabilities in those components for which there are no viable security controls to adequately mitigate risk, reimplementation or custom development of such components may reduce potential attacks by adversaries.	
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.01.02.01 System-level contingency plans are developed, documented, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level contingency plans through • inquiry of appropriate personnel and • inspection of relevant documentation, such as policies and procedures for developing contingency plans. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect the contingency plans for each of the information systems relevant to the significant business processes, as applicable. Consider whether the plans • identify critical or essential mission and business functions, as applicable, and associated contingency requirements, including how critical or essential mission and business functions will be maintained in the event of a system disruption, compromise, or failure;	NIST SP 800-53, CP-2 NIST SP 800-53, CP-10 NIST SP 800-53, CP-12 NIST SP 800-53, SC-24

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• are based on current information and reflect current conditions, including contingency roles, responsibilities, and assigned individuals with contact information; • have been recently reviewed and updated; • have been approved by the appropriate senior officials; • are integrated with the risk management and system development life cycle processes; • are appropriately aligned with other organizational plans, including the critical infrastructure and key resources protection plan, as well as business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, insider threat implementation plans, data breach response plans, cyber-incident response plans, breach response plans, and occupant emergency plans, as applicable; • address information system interdependencies; • include required information in accordance with authoritative criteria; • identify and allocate appropriate resources to support achieving continuity of operations and prioritize recovery and reconstitution procedures; • provide for the failure and timely recovery and reconstitution of the information system and system components to a known state; • adequately consider whether alternate processing and storage sites (both internal and external to the entity) can be relied on for continuity or operations without compromising security concerns; and • are adequate to address eventual, full system restoration and implementation of alternative mission or business processes	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	without deterioration of the controls originally planned and implemented. Determine whether the contingency plans for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved. Note: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design, as systems can be designed for redundancy, to provide backup capabilities, and for resilience. Additionally, for systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation.	
CP.01.02.02 A critical infrastructure and key resources protection plan is developed, documented, disseminated, and periodically reviewed and updated.	Obtain an understanding of the entity's processes and methods for developing, documenting, disseminating, and periodically reviewing and updating the critical infrastructure and key resources protection plan through • inquiry of appropriate personnel and • inspection of relevant entity documentation. Inspect the critical infrastructure and key resources protection plan. Consider whether the plan • has been recently reviewed and updated, as appropriate; • has been approved by the appropriate senior official(s); • includes required information in accordance with authoritative criteria;	NIST SP 800-53, PM-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• is consistent with applicable statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, and guidelines; • provides an overview of the entity's protection strategies based on management's prioritization of critical or essential mission and business functions and management's determination of the criticality of information systems, information system components, and information system services; • considers the risks and potential impacts of a system disruption, compromise, or failure on the performance of critical or essential mission and business functions; and • addresses the information systems and information system resources relevant to the significant business processes. Determine whether the crucial infrastructure and key resources protection plan has been appropriately developed, documented, disseminated, and periodically reviewed and updated. Note: The development of contingency plans is coordinated with the critical infrastructure and key resources protection plan, as well as with other organizational plans, such as business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, insider threat implementation plans, data breach response plans, cyber-incident response plans, breach response plans, and occupant emergency plans.	
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.01.03.01. Management establishes, documents, and periodically reviews and updates contingency training that incorporates lessons learned from contingency plan testing or actual system	Obtain an understanding of the entity's processes and methods for establishing, documenting, and periodically reviewing and updating contingency training through	NIST SP 800-53, CP-2 NIST SP 800-53, CP-3 NIST SP 800-53, SI-17

Illustrative control activities	Illustrative audit procedures	Relevant criteria
disruptions into contingency training techniques. Management monitors the completion status of applicable mandatory training courses for information system users.	• inquiry of appropriate personnel, including any senior officials responsible for contingency training, and • inspection of relevant documentation. Inspect documentation for contingency training for each of the information systems relevant to the significant business processes, as applicable. Consider whether • training course materials are consistent with information system user roles and responsibilities and the content has been reviewed and updated when required because of system changes and at an appropriate frequency; • lessons learned from contingency plan testing or actual system disruptions are incorporated into course materials and training techniques; • mandatory training courses are identified and communicated to information system users as a condition for system access, as applicable; and • management monitors and maintains records of the completion status of applicable mandatory training courses for information system users. Determine whether contingency training for relevant information systems is effectively designed, appropriately documented, and periodically reviewed and updated, and whether user attendance and completion are monitored. Note: Actions addressed in contingency plans, and for which training may be required, include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. Additionally, fail-safe procedures may be required when certain failure conditions occur and training on such procedures may be beneficial. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps	

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.	
CP.01.04 Information system contingency plans are periodically tested to determine their effectiveness and the entity's readiness to execute them.		
CP.01.04.01 Contingency plans are periodically tested under conditions that simulate a system disruption.	Obtain an understanding of the entity's processes for periodically testing the contingency plans for the information systems relevant to the significant business processes through • inquiry of appropriate personnel, including users and authorizing officials; • inspection of relevant policies and procedures for contingency plan testing; and • inspection of other relevant documentation demonstrating the design and implementation of the processes. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect available documentation for any instances in which the contingency plans for relevant information systems were tested during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures for contingency plan testing. Determine whether the processes for periodically testing the contingency plans for relevant information systems are designed, implemented, and operating effectively to reasonably assure that contingency plans are effective and the entity is ready to execute such plans. Note: Methods for testing contingency plans to determine their effectiveness and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full	NIST SP 800-53, CP-4

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans.	
CP.01.04.02 Contingency plan test results are documented, reviewed by management, and used to inform updates to the system-level contingency plans. *Related control: CP.03.01.01*	Inspect contingency plan test results documented for the information systems relevant to the significant business processes. Determine whether contingency plan test results, including any necessary corrective actions, have been documented, reviewed by management, and appropriately considered as part of the process for updating the contingency plans for relevant information systems.	NIST SP 800-53, CP-2 NIST SP 800-53, CP-4
CP.02 Management designs and implements control activities to prevent or minimize system disruption and potential damage to facilities, information systems, and information system resources due to natural disasters, structural failures, hostile attacks, or errors.		
CP.02.01 Environmental controls are appropriately selected and employed based on risk.		
CP.02.01.01 Management maintains and monitors temperature, humidity, and other environmental factors for facilities where systems reside through the selection and employment of climate controls based on risk.	Obtain an understanding of the climate controls employed by the entity for the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel; • inspection of relevant documentation; and • observation of the entity's use of climate controls to maintain and monitor temperature, humidity, and other environmental factors. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify the climate controls employed by the entity. Consider whether the selection and employment of climate controls to maintain and monitor temperature, humidity, and other environmental factors are appropriate based on risk. Determine whether management adequately maintains and monitors temperature, humidity, and other environmental factors through the selection and employment of climate controls for the facilities where	NIST SP 800-53, PE-14

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	relevant information systems and information system resources reside. Note: Insufficient climate controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support critical or essential mission and business functions.	
CP.02.01.02 Master shutoff or isolation valves are accessible, functional, and known to appropriate personnel to protect facilities, information systems, and information system resources from water damage.	Obtain an understanding of any master shutoff or isolation valves employed by the entity for the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the location of any master shutoff or isolation valves within the facilities. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify any master shutoff or isolation valves employed by the entity. Consider whether the location of such valves would facilitate timely access during an emergency to prevent or minimize water damage to information system resources. Determine whether the master shutoff or isolation valves identified are accessible, functional, and known to appropriate personnel to adequately protect facilities, information systems, and information system resources from water damage. Note: Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.	NIST SP 800-53, PE-15
CP.02.01.03 Emergency shutoff switches are accessible, functional, and known to appropriate personnel to provide the	Obtain an understanding of any emergency shutoff switches employed by the entity for the facilities where information systems and	NIST SP 800-53, PE-10

Illustrative control activities	Illustrative audit procedures	Relevant criteria
capability of shutting off power to facilities, information systems, and information systems resources in the event of an emergency. Access to emergency shutoff switches is appropriately controlled.	information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the location of any emergency shutoff switches within the facilities. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify any emergency shutoff switches employed by the entity. Consider whether the location of such switches would facilitate timely access during an emergency. Consider whether access to such switches is limited to authorized personnel. See also AC.04.01.11. Determine whether the emergency shutoff switches are accessible, functional, and known to appropriate personnel to provide the capability of shutting off power to facilities, information systems, and information systems resources in the event of an emergency. Determine whether access to emergency shutoff switches is appropriately controlled.	
CP.02.01.04 Management maintains and monitors fire detection and suppression systems for facilities where systems reside.	Obtain an understanding of the fire detection and suppression systems employed by the entity for the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel, • inspection of relevant documentation, and • observation of the entity's use of fire detection and suppression systems. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Identify the fire detection and suppression systems	NIST SP 800-53, PE-13

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	employed by the entity. Consider whether an independent power source supports the fire detection and suppression systems. Determine whether management adequately maintains and monitors fire detection and suppression systems for the facilities where relevant information systems and information system resources reside. Note: Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.	
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.02.02.01 Sufficiently separated alternate processing and storage sites are maintained to provide and support processing capabilities in the event that the primary processing or storage sites are unavailable.	Obtain an understanding of any alternate processing or storage sites employed by the entity for the information systems and information system resources relevant to the significant business processes through • inquiry of appropriate personnel; • inspection of relevant documentation, including any necessary agreements permitting the timely transfer and resumption of processing for critical or essential mission and business functions, as well as the storage and retrieval of system backup information, in the event that the primary processing or storage sites are unavailable; and • observations of alternate processing and storage sites. Perform walk-throughs of the alternate processing and storage sites where information systems and information system resources relevant to the significant business processes are duplicated or backed up to provide and support processing capabilities when the primary processing or storage sites are unavailable. Consider whether the equipment and supplies required to facilitate the timely transfer and resumption of processing are on hand or readily available. Consider	NIST SP 800-53, CP-6 NIST SP 800-53, CP-7 NIST SP 800-53, PE-17

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	whether the controls at the alternate processing and storage sites are equivalent or commensurate to those at the primary processing and storage sites. Determine whether sufficiently separated alternate processing and storage sites are maintained for the information systems and information system resources relevant to the significant business processes to provide and support processing capabilities in the event that the primary processing or storage sites are unavailable. Note: While distinct from alternate processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Alternate work sites include government facilities or the private residences of employees. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing and storage sites based on the types of threats that are of concern.	
CP.02.02.02 Alternate telecommunications services are established to permit the timely resumption of operations supporting critical or essential mission and business functions in the event that the primary telecommunications services are unavailable.	Obtain an understanding of any alternate telecommunications services employed by the entity for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect relevant telecommunications services contracts and agreements. Consider whether such contracts and agreements include provisions addressing availability requirements, including priority of service. Consider whether any physical infrastructure is shared between the primary and alternate telecommunications service providers, and if so, how risks relevant to a single point of failure resulting from a natural disaster, structural failure, hostile attack, or errors would be mitigated.	NIST SP 800-53, CP-8

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Determine whether alternate telecommunication services are available for relevant information systems.	
CP.02.02.03 Alternate security mechanisms for critical security functions are established to control access in the event that the primary security mechanisms are unavailable or compromised.	Obtain an understanding of any alternate security mechanisms employed by the entity for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant documentation. Inspect documentation demonstrating the design and implementation of any alternate security mechanisms employed by the entity for relevant information systems. Determine whether alternate security mechanisms for critical security functions are available and appropriate for the relevant information systems. Note: Given the cost and level of effort required to establish and maintain alternate security mechanisms, such mechanisms are generally only applied to critical security functions of information systems, information system components, or information system services.	NIST SP 800-53, CP-13 NIST SP 800-53, SI-13
CP.02.02.04 In the event of a loss of the primary power source, emergency lighting is activated and an uninterruptible power supply is available to provide temporary power while the alternate power source is started.	Obtain an understanding of the entity's use of emergency lighting and an uninterruptible power supply in the event of a loss of the primary power source at the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel and • inspection of relevant documentation. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Inspect the results of any recent tests of the entity's uninterruptible power supply. Consider whether the uninterruptible power supply	NIST SP 800-53, PE-11 NIST SP 800-53, PE-12

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	provided sufficient power to facilitate an orderly shutdown of the systems involved in the tests or to temporarily power the systems while the alternate power source was started. Determine whether, in the event of a loss of the primary power source at the facilities where relevant information systems and information system resources reside, emergency lighting is activated and an uninterruptible power supply is available and sufficient to provide temporary power while the alternate power source is started.	
CP.02.02.05 In the event of a loss of the primary power source, an alternate power supply, such as a backup generator, is available to be started.	Obtain an understanding of the entity's use of an alternate power supply in the event of a loss of the primary power source at the facilities where information systems and information system resources relevant to the significant business processes reside through • inquiry of appropriate personnel and • inspection of relevant documentation. Perform walk-throughs of the facilities where information systems and information system resources relevant to the significant business processes reside. Inspect the results of any recent tests of the entity's alternate power supply. Consider whether the alternate power supply provided sufficient power to support operations while the primary power source was unavailable. Determine whether, in the event of a loss of the primary power source at the facilities where relevant information systems and information system resources reside, an alternate power supply is available and sufficient to support operations.	NIST SP 800-53, PE-11
CP.02.02.06 Alternate communications mechanisms are established to support continuity of operations in the event of a system disruption.	Obtain an understanding of any alternate communications mechanisms employed by the entity to support continuity of operations in the event of a system disruption through • inquiry of appropriate personnel and • inspection of relevant documentation.	NIST SP 800-53, CP-11 NIST SP 800-53, SC-47

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect documentation demonstrating the design and implementation of any alternate communications protocols or alternate communications paths employed by the entity for the information systems relevant to the significant business processes. Determine whether alternate communications mechanisms are available and appropriate for relevant information systems. Note: Switching communications protocols may affect application software and operational aspects of systems. It is important for entities to assess the potential side effects of introducing alternate communications protocols prior to implementation. An incident, whether adversarial or nonadversarial, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident.	
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.02.03.01 System backups of data and software are conducted regularly consistent with risk.	Obtain an understanding of the entity's processes for conducting system backups through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of system-level contingency plans for each of the information systems relevant to the significant business processes, as applicable. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes for conducting system backups for relevant information systems. Consider whether • the frequency at which system backups are conducted is adequate,	NIST SP 800-53, CP-9

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• access to system backups is appropriately controlled, and • the retention periods for system backups are aligned with entity-level policies. See also AC.03.02.01 and AC.03.02.02. Inspect the results of any recent tests of the entity's system backups. Consider whether the confidentiality, integrity, and availability of system backups are adequately protected through reperformance of the entity's test procedures or independent analysis. Determine whether system backups of data and software for relevant information systems are properly conducted regularly consistent with risk.	
CP.02.03.02 System media containing backup data and software is properly maintained at alternate processing or storage sites.	Obtain an understanding of the entity's processes for transferring and maintaining system media containing backup data and software at alternate processing or storage sites through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of system-level contingency plans for each of the information systems relevant to the significant business processes, as applicable. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes for transferring and maintaining system media containing backup data and software for relevant information systems. Consider whether • the locations of the alternate processing or storage sites are appropriate to minimize disruption and • the methods used to transport, receive, and replace system backups permit them to be tracked throughout the process. See also AC.03.01.03, AC.03.01.04, and AC.03.01.05.	NIST SP 800-53, CP-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	Inspect the results of any recent tests of the entity's system backups. Consider whether the confidentiality, integrity, and availability of system backups are adequately protected through reperformance of the entity's test procedures or independent analysis. Consider whether such backups of software reflect the most recent version in use and are protected from modification. Determine whether system media containing backup data and software is properly maintained at alternate processing or storage sites.	
CP.02.04 Maintenance of information system components is properly performed on a timely basis to prevent or minimize system disruption.		
CP.02.04.01 Management maintains appropriate tools and resources for performing system component maintenance on a timely basis.	Obtain an understanding of the tools and resources that management employs to perform system component maintenance for the information systems relevant to the significant business processes through • inquiry of appropriate personnel; • inspection of relevant policies and procedures; and • inspection of maintenance contracts or service agreements with external entities, as applicable. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes for approving, controlling, and monitoring the use of system maintenance tools. Inspect documentation demonstrating the design and implementation of the entity's processes for obtaining maintenance support, as well as any spare parts or replacement hardware needed to perform system component maintenance on a timely basis. Consider whether • the entity has established a process for authorizing access for external personnel engaged to perform system component maintenance,	NIST SP 800-53, MA-3 NIST SP 800-53, MA-5 NIST SP 800-53, MA-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• maintenance contracts or service agreements include provisions to define timeliness and specify requirements for completing timely maintenance, • requirements for the performance of system component maintenance in accordance with vendor specifications are included in the entity's policies and procedures, and • the entity maintains an inventory of spare parts or replacement hardware for system components that support critical or essential mission and business functions. Inspect available documentation for a selection of system components to assess whether maintenance has been performed for such components in accordance with vendor specifications. Determine whether management maintains appropriate tools and resources for performing system component maintenance for relevant information systems on a timely basis.	
CP.02.04.02 Management schedules and performs system component maintenance in a manner that minimizes service outages and disruption of operations.	Obtain an understanding of the entity's processes and methods to schedule and perform system component maintenance for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes for scheduling and performing system component maintenance for relevant information systems. Consider whether • flexibility exists in operations, including processing for critical or essential mission and business functions, to accommodate	NIST SP 800-53, MA-6

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	regularly scheduled maintenance and a reasonable amount of unscheduled maintenance; • management has established goals for the availability of services and processing capabilities; • advance notice of regularly scheduled maintenance and timely communication of unscheduled maintenance is provided to system users, as well as others affected by or involved in such maintenance, to minimize the impact on operations; and • performance measures and compliance metrics are periodically evaluated and appropriately employed to measure the effectiveness or efficiency of system component maintenance. Determine whether management schedules and performs system component maintenance in a manner that minimizes service outages and disruption of operations.	
CP.02.04.03 Management performs system component maintenance in a controlled manner to prevent unexpected service outages and system disruptions.	Obtain an understanding of the entity's processes and methods to control system component maintenance for the information systems relevant to the significant business processes through • inquiry of appropriate personnel and • inspection of relevant policies and procedures. See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. Inspect documentation demonstrating the design and implementation of the entity's processes for controlling system component maintenance for relevant information systems. Consider whether • management reviews and approves maintenance activities, regardless of whether such activities are performed locally or remotely;	NIST SP 800-53, MA-2 NIST SP 800-53, MA-4 NIST SP 800-53, MA-5 NIST SP 800-53, MA-7

Illustrative control activities	Illustrative audit procedures	Relevant criteria
	• the removal of a system component from an entity facility for maintenance, repair, or replacement requires explicit approval from management; • affected, or potentially affected controls, are tested to determine whether such controls operate as intended following system component maintenance; • records, which provide evidence for all maintenance actions and approvals, are properly prepared and maintained; • the entity has implemented processes for approving, controlling, and monitoring the use of system maintenance tools and for periodically reviewing previously approved system maintenance tools for continuing appropriateness; • strong authentication methods and appropriate session-level controls are employed in connection with remote maintenance and diagnostic activities; • field maintenance is appropriately controlled; • entity personnel with adequate technical competence supervise or oversee the performance of maintenance activities; and • maintenance activities are appropriately logged and adequately monitored. Determine whether management performs system component maintenance for relevant information systems in a controlled manner.	

APPENDIX 500C

FISCAM ASSESSMENT COMPLETION CHECKLIST

Purpose

The *Federal Information System Controls Audit Manual* (FISCAM) assessment completion checklist includes the requirements for conducting an information system (IS) controls assessment based on generally accepted government auditing standards (GAGAS) and requirements prescribed by FISCAM. The FISCAM assessment completion checklist is intended to help auditors determine compliance with FISCAM. It does not include all procedures necessary to achieve the engagement objectives overall.

Instructions

The FISCAM assessment completion checklist contains detailed questions that are organized into four sections: planning, testing, reporting, and conclusions. A response to each question should be documented by either a "Yes," "No," or "N/A (not applicable) response in the "Response" column." For "Yes" responses, a reference to related audit documentation should be noted in the "Explanation and Reference" column. It is not necessary to create additional documentation to support a "Yes" response. For most questions, "No" responses indicate departures from FISCAM. All departures and their significance, including any effects on the auditor's report, should be explained in the "Explanation and Reference" column. An "N/A" response is appropriate when an item does not exist or exists but is considered insignificant to engagement objectives. All "N/A" responses should be explained in the "Explanation and Reference" column.

The auditor-in-charge, audit senior, or audit manager prepares and signs this checklist before the assessment completion date, which generally coincides with the date of the auditor's report. The assistant director and first partner (audit director) review and sign this checklist before the auditor's report date.

Engagement Information

Entity Name: _____ Job Code: _____

Preparation, Review, and Approval

Auditor's report date:	_____		
Auditor-in-Charge:	_____	Date Reviewed:	_____
Assistant Director:	_____	Date Reviewed:	_____
Audit Director:	_____	Date Reviewed:	_____

Checklist

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
Section 1: Planning Phase			
1. Did the audit organization assign auditors to conduct the engagement who, before beginning work on the engagement, collectively possessed the competence needed to address the engagement objectives and perform their work in accordance with GAGAS?	FISCAM, 220.03 GAGAS 2018, 4.02		
2. Did the auditor determine whether other auditors have conducted, or are conducting, audits that are relevant to the engagement objectives?	FISCAM, 220.06 GAGAS 2018, 8.80		
3. If the auditor used the work of other auditors, did the auditor • perform procedures that provided a sufficient basis for using the work; • obtain evidence concerning qualifications and independence of the other auditors; and • determine whether the scope, quality, and timing of the audit work performed by the other auditors can be relied on in the context of current engagement objectives?	FISCAM, 220.08 GAGAS 2018, 8.81		
4. If the engagement is a financial audit and the auditor used the work of other auditors, did the	FISCAM, 220.09		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
auditor comply with the requirements in FAM 600?			
5. If the auditor used the work of an IT specialist, did the auditor assess the qualifications, competence, and independence of the IT specialist?	FISCAM, 220.10 GAGAS 2018, 4.12, 8.82		
6. If the engagement is a financial audit and the auditor used the work of an IT specialist, did the auditor comply with the requirements in FAM 620?	FISCAM, 220.11		
7. Did the auditor obtain an understanding of the entity and its operations sufficient to plan the engagement?	FISCAM, 230.04		
8. Did the auditor identify and obtain an understanding of the significant business processes, using walk-throughs or alternative procedures, sufficient to identify areas of audit interest and business process controls?	FISCAM, 230.07, 230.08, 230.10		
9. Did the auditor appropriately identify areas of audit interest at the business process and system levels?	FISCAM, 240.06		
10. Did the auditor obtain a sufficient understanding of the business process controls designed to achieve information processing objectives (completeness, accuracy, and validity)?	FISCAM, 240.11		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
11. Did the auditor review available business process application documentation that explains the processing and flow of data within the application, as well as interfaces to other information systems and the design of the underlying data management systems?	FISCAM, 240.12		
12. Did the auditor appropriately identify user and application control objectives for each area of audit interest at the business process level using the FISCAM Framework (app. 500B, table 8)?	FISCAM, 240.13		
13. Did the auditor appropriately identify general control objectives for each area of audit interest at the business process level that are necessary to support the achievement of the engagement objectives using the FISCAM Framework (app. 500B, table 8)?	FISCAM, 240.14		
14. If external entities performed any business process controls on behalf of the entity that are intended to achieve the relevant business process control objectives, did the auditor obtain an understanding of such controls sufficient to assess risk and design further audit procedures in response to those risks?	FISCAM, 240.18, 240.19		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
15. Did the auditor obtain an understanding of the entity's information security management program sufficient (1) plan the IS controls work necessary to support the achievement of the engagement objectives and (2) 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 information system (IS) controls assessment?	FISCAM, 250.04		
16. Did the auditor obtain an understanding of the entity's information security management program using the FISCAM Framework (app. 500B, table 9)?	FISCAM, 250.04		
17. Did the auditor appropriately identify inherent and control risk factors relevant to the significant business processes and areas of audit interest?	FISCAM, 260.04		
18. Did the auditor appropriately assess and discuss the risk of fraud occurring that is significant to the engagement objectives?	FISCAM, 260.09 GAGAS 2018, 8.71		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
19. Did the auditor adequately evaluate whether the audited entity has taken appropriate corrective action to address previously reported findings and recommendations that are significant to the engagement objectives, including • asking entity management to identify previous engagements or other studies that directly relate to the objectives of the engagement, including whether related recommendations have been implemented, and • using this information to assess risk and determine the nature, extent, and timing of current audit work?	FISCAM, 260.15 GAGAS 2018, 6.11, 7.13, 8.30		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
20. Did the auditor adequately assess the level of IS risk for each of the areas of audit interest on a preliminary basis based on • the auditor's identification of inherent and control risk factors, including fraud risk factors, • the auditor's determination regarding the likelihood that conditions or events, related to the areas of audit interest, could affect the entity's ability to achieve its information processing or information security objectives, and • the impact that such conditions or events (e.g., significance or materiality) would have on the entity's achievement of information processing and information security objectives that are significant to the engagement objectives?	FISCAM, 260.17, 260.18		
21. Did the auditor appropriately involve senior members of the engagement team in • assessing IS risk and • determining the nature, extent, and timing of IS control tests in response to assessed risks?	FISCAM, 260.20, 260.22		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
22. Did the auditor appropriately • identify general control objectives for each area of audit interest at the system level that are necessary to support the achievement of the engagement objectives and • determine the likelihood that general control activities will effectively achieve the relevant general control objectives?	FISCAM, 270.04, 270.06		
23. Did the auditor use the FISCAM Framework (app. 500B, tables 9 through 13) to • identify general control objectives relevant to the areas of audit interest at the system level and • determine the likelihood that control activities will effectively achieve the relevant IS control objectives?	FISCAM, 270.07, 270.09, 270.11, 270.13, 270.15		
24. Did the auditor 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, approach, and methodology of the IS controls assessment?	FISCAM, 280.01 GAGAS 2018, 8.132		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
25. Did the auditor adequately prepare a written risk assessment, including • the inherent and control risk factors, including fraud risk factors, that significantly increase or decrease the auditor's assessed level of IS risk for each of the areas of audit interest • the likelihood that conditions or events related to the areas of audit interest that could significantly (or materially) affect the entity's ability to achieve its information processing or information security objectives could occur • the impact that such conditions or events would have on the entity's achievement of information processing and information security objectives that are significant to the engagement and • the compensating controls that mitigate the effects of identified inherent and control risk factors?	FISCAM, 280.02		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
26. Did the auditor adequately prepare and update a written audit plan, planning memo, subordinate test plans for each area of audit interest, and results memo that describe 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, • the identification of user, application, and general control objectives for each area of audit interest, as applicable, and • the auditor's basis for such scoping decisions?	FISCAM, 280.03, 280.04, 280.05, 350.03, 350.04, 350.05 GAGAS 2018, 8.03, 8.33		
Section 2: Testing Phase			
27. Did the auditor obtain sufficient, appropriate evidence to conclude on whether the relevant business process and general control objectives are achieved by the entity's user, application, and general control activities?	FISCAM, 320.02		
28. Did the auditor develop test plans to assist in obtaining sufficient, appropriate evidence to conclude on whether the entity's IS controls are designed, implemented, and operating effectively to achieve the IS control objectives relevant to the areas of audit interest?	FISCAM, 320.02		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
29. Did the auditor appropriately consider the extent to which control dependencies exist among user, application, and general control activities designed to achieve the relevant business process and general control objectives?	FISCAM, 320.03		
30. Did the auditor appropriately select the IS control activities that • are likely to achieve the relevant IS control objectives and • are most efficient for testing?	FISCAM, 320.04		
31. Did the auditor use the FISCAM Framework (app. 500B) to identify user, application, and general control activities by control objective?	FISCAM, 320.05		
32. In determining the nature of IS control tests to be performed for each selected IS control activity, did the auditor appropriately consider • the nature of the IS control activity; • the evidence available to demonstrate whether the IS control activity is designed, implemented, and operating effectively; and • the significance of the IS control activity to achieving the related IS control objective(s)?	FISCAM, 330.02, 330.07		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
33. Did the auditor perform IS control tests sufficient to conclude on the operating effectiveness of the selected user, application, and general controls that have been suitably designed and properly implemented?	FISCAM, 330.05		
34. If the auditor used information provided by entity officials as evidence, did the auditor perform audit procedures to assess the information's reliability?	FISCAM, 330.09 GAGAS 2018, 8.93		
35. If the auditor performed inquiries regarding the design, implementation, and operating effectiveness of IS control activities, did the auditor appropriately perform other audit procedures in combination with inquiry to obtain sufficient, appropriate evidence?	FISCAM, 330.10 GAGAS 2018, 8.94		
36. In determining the extent of IS control tests to be performed for each selected IS control activity, did the auditor appropriately consider • the nature of the IS control test, • the frequency at which the entity performs the IS control activity, • the significance of the IS control activity achieving the related IS control objective(s), and • the use of statistical sampling or nonstatistical selection methods for determining operating effectiveness?	FISCAM, 330.02, 330.13, 330.17		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
37. If the auditor used statistical sampling to identify items within a population for control testing, did the auditor appropriately define and determine • the objectives of the control test (including what constitutes a deviation), • the population (including the sampling unit and time frame), • the method of selecting the sample, and • sample design and resulting sample size?	FISCAM, 330.19, 330.20, 330.21		
38. If the auditor used statistical sampling to identify items within a population for control testing, did the team appropriately • use attribute sampling, • determine whether to stratify the population prior to sampling, and • determine a sample size sufficient to reduce sampling risk to an acceptably low level?	FISCAM, 330.18, 330.19, 330.22, 330.25		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
39. In determining the timing of IS control tests to be performed for each selected IS control activity, did the auditor appropriately consider • the type of evidence available to the auditor to demonstrate whether the IS control activity is designed, implemented, and operating effectively; • the nature of the IS control test; and • the significance of the IS control activity to achieving the related IS control objective(s)?	FISCAM, 330.29		
40. Did the auditor determine the nature, extent, and timing of IS control tests necessary to obtain sufficient, appropriate evidence to • determine the effectiveness of selected IS control activities and • conclude on whether the relevant IS control objectives are achieved by the selected IS controls?	FISCAM, 320.02, 330.02		
41. Did the auditor appropriately determine whether each selected IS control activity is • suitably designed to support achieving the related IS control objective(s), • properly implemented (placed in operation), and • operating effectively?	FISCAM, 330.03		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
42. If the auditor used automated audit tools, did the auditor adequately understand the following for each • what are the associated risks, • when to use the tool, • how to operate the tool, • how to analyze the data, and • how to interpret results?	FISCAM, 330.32		
43. If the auditor used automated audit tools, did the auditor perform a technical review of to verify • the use and operation of the automated audit tool is appropriate, • the results the tool produces are complete and accurate, and • that the conclusions are supported.	FISCAM, 330.33		
44. If the engagement is a financial audit and the auditor used a service organization report as evidence to support the effective design, implementation, and operation of IS control activities, did the auditor comply with the requirements in FAM section 640?	FISCAM, 330.38		
45. If the auditor used a service organization report as evidence to support the effective design, implementation, and operation of IS control activities, did the auditor determine whether the report provides sufficient, appropriate evidence about the design,	FISCAM, 330.37		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
implementation, and operating effectiveness of IS control activities by • assessing the adequacy of the standards under which the service auditor's report was issued; • evaluating whether the report is for a period that is appropriate for the auditor's purpose; • determining whether complementary user-entity controls that the service organization identified as relevant to the IS control activities performed by the service organization are designed, implemented, and operating effectively; • evaluating the adequacy of the time period covered by the service auditor's tests of the IS control activities performed by the service organization and the time elapsed since performance of such tests; and • evaluating whether the results of the service auditor's tests of the IS control activities the service organization performed, as described in the service auditor's report, provide sufficient, appropriate evidence to support the auditor's risk assessment?			

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
46. If the service organization report excluded the services that a subservice organization performed and those services are relevant to the auditor's assessment of IS controls, did the auditor adequately apply the same criteria in paragraph 330.36 to the services the subservice organization provided?	FISCAM, 330.41		
47. Did the auditor use suitable criteria to perform control tests of the selected IS control activities?	FISCAM, 340.02 GAGAS 2018, 8.07		
48. Did the auditor adequately evaluate the results of control tests to determine whether IS control activities are designed, implemented, and operating effectively to achieve the IS control objectives?	FISCAM, 340.03		
49. Did the auditor appropriately communicate identified control deviations to the entity in sufficient detail for management to consider whether there are additional factors or compensating controls that are relevant to the auditor's determination as to whether • a control deviation is an IS control deficiency and • the related IS control objective is achieved?	FISCAM, 340.04		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
50. Did the auditor appropriately determine whether there are specific compensating controls that could mitigate each potential IS control deficiency?	FISCAM, 340.05		
51. If compensating controls could adequately mitigate a potential deficiency and achieve the IS control objective, did the auditor obtain sufficient evidence that the compensating controls are designed, implemented, and operating effectively or that the other factors actually mitigate the potential deficiency?	FISCAM, 340.05		
52. For control deviations that were not resolved by additional evidence, did the auditor appropriately communicate to management, in writing and on a timely basis, the details of the IS control deficiencies identified?	FISCAM, 340.06 GAGAS 2018, 6.17, 7.19, and 8.116		
53. Did the auditor adequately evaluate and sufficiently document the significance of identified IS control deficiencies?	FISCAM, 340.07 GAGAS 2018, 8.54		
54. If the engagement is a financial audit, did the auditor comply with requirements for classifying control weaknesses as discussed in FAM section 580?	FISCAM, 340.08		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
55. Did the auditor adequately perform and sufficiently document an overall assessment of the collective evidence obtained throughout the IS controls assessment to support the auditor's findings and conclusions?	FISCAM, 340.09 GAGAS 2018, 8.108		
56. Did the auditor reassess, based on the audit procedures performed and the collective evidence obtained, the level of IS risk for each of the areas of audit interest?	FISCAM, 340.10		
57. Did the auditor determine whether the audit procedures performed throughout the IS controls assessment are adequate to reduce audit risk to an acceptably low level?	FISCAM, 340.11 GAGAS 2018, 8.109		
58. If the engagement is a financial audit, did the auditor determine whether the IS controls achieve the relevant IS control objectives and support a low assessed level of control risk for the auditor's overall assessment of internal control over financial reporting?	FISCAM, 340.12		
59. Did the auditor prepare testing phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand from the audit documentation the nature, timing, extent of audit procedures performed and the results of the IS controls assessment, including the significance of any IS control deficiencies identified?	FISCAM, 350.01 GAGAS 2018, 8.132		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
60. Before the report was issued, did the auditor adequately prepare audit documentation containing sufficient, appropriate evidence for the auditor's findings, conclusions, and recommendations, including • a completed, written audit plan reflecting the results of the audit procedures performed, • a written results memo describing the overall assessment of the collective evidence obtained, as well as the auditor's final determinations regarding IS risk and audit risk, and • subordinate test plans documenting the approach for testing controls for the relevant IS control objectives for each area of audit interest?	FISCAM, 350.02, 350.03, 350.04, 350.05 GAGAS 2018, 8.133, 8.134, 8.135		
61. If the auditor used statistical sampling to perform IS control tests, did the auditor prepare written sampling plans that include • the objectives of each test (including what constitutes a deviation), • the population (including sampling unit and time frame), • the method of selecting the sample, and • the sample design and resulting sample size?	FISCAM, 350.06		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
62. If the auditor used automated audit tools to perform IS control tests, did the auditor prepare relevant audit documentation in sufficient detail to enable a technical review by audit staff independent of the preparer to determine that • the use and operation of the automated audit tool is appropriate, • the results produced by the automated audit tool are complete and accurate, and • any conclusions are supported?	FISCAM, 350.07		
Section 3: Reporting Phase			
63. Did the auditor adequately determine whether it followed the FISCAM methodology?	FISCAM, 420.01		
64. For financial audit reports, did the auditor comply with the reporting requirements in FAM section 580?	FISCAM, 430.06 GAGAS 2018, 6.42		
65. For examination-level attestation engagements, did the auditor properly include in the examination report all internal control deficiencies, even those communicated early, that are considered to be significant deficiencies or material weaknesses that the auditor identified based on the engagement work performed?	FISCAM, 430.07 GAGAS 2018, 7.42		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
66. For performance audits, did the auditor properly include in the audit report • any deficiencies in internal control that are significant engagement objectives and based upon the audit work performed?	FISCAM, 430.08 GAGAS 2018, 9.29, 9.30		
67. If the auditor detected deficiencies in internal control that are not significant to the objectives of the performance audit but warrant the attention of those charged with governance, did the team either • include those deficiencies in the report, or • communicate those deficiencies in writing to audited entity officials and refer to that written communication in the audit report?	FISCAM, 430.09 GAGAS 2018, 9.31		
68. Did the auditor develop the elements of the findings to the extent necessary to assist management or oversight officials of the audited entity in understanding the need for taking corrective action?	FISCAM, 430.10 GAGAS 2018, 6.50, 7.48, 9.18		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
69. When presenting findings in the report, did the auditor • place findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the findings; • relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures to give the reader a basis for judging the prevalence and consequences of the findings; and • if the results cannot be projected, limit conclusions appropriately?	FISCAM, 430.12 GAGAS 2018, 6.51, 7.49, 9.21		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
70. Did the auditor • disclose significant facts relevant to the objectives of its work and known to the team that if not disclosed could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices; • report conclusions based on the engagement objectives and findings; • provide recommendations for corrective action for any sufficiently developed findings that are significant to the engagement objectives; • make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended; and • recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions?	FISCAM, 430.13, 430.14, 430.15 GAGAS 2018, 9.19, 9.23		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
71. For reports that contain, or may contain, information prohibited from public disclosure because of its confidential or sensitive nature, did the auditor appropriately • request that the source agency perform a classification, security, or sensitivity review of the draft report; • evaluate entity concerns and make appropriate report revisions or redactions, considering legal or regulatory requirements; • if information is excluded from a report, disclose in the report that certain information has been omitted and the circumstances that make the omission necessary; • if information is omitted from the report, evaluate whether this omission could distort the results or conceal improper or illegal practices and revise the report language as necessary to avoid report users drawing inappropriate conclusions from the information presented; and • determine whether public records laws could affect the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate?	FISCAM, 430.16, 430.17, 430.18, 430.19 GAGAS 2018 6.63, 6.64, 6.65, 7.61, 7.62, 7.63, 9.61, 9.62, 9.63		

Question	Paragraph reference(s) and related GAGAS requirement	Response (Yes, No, or N/A)	Explanation and Audit Documentation Reference
72. Did the auditor prepare reporting phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand the conclusions reached, including evidence that supports the auditor's conclusions?	FISCAM, 440.01 GAGAS 2018, 8.132		
73. Did the engagement team adequately document any departures from the FISCAM requirements and the impact on the engagement and on the auditors' conclusions?	FISCAM, 440.02 GAGAS 2018, 8.136		