# Federal Information System Controls Audit Manual (FISCAM)

June 2026

GAO-26-108633

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

The *Federal Information System Controls Audit Manual* (FISCAM) presents a methodology for assessing information system controls of federal entities in accordance with professional standards. It consists of the audit methodology, controls framework, and three appendixes.

The U.S. Government Accountability Office (GAO) and Council of the Inspectors General on Integrity and Efficiency (CIGIE) worked jointly on this revision resulting in the first-ever GAO/CIGIE FISCAM—marking a major milestone in partnership and a shared commitment to strengthening and clarifying audit guidance.

This revision supersedes the September 2024 revision and is effective for engagements beginning with fiscal year and calendar year 2026 audits of federal entity financial statements. The 2026 revision of FISCAM is effective for attestation engagements and performance audits beginning on or after October 1, 2026.[1] The changes in this update are primarily based on the 2025 revision of the *Standards for Internal Control in the Federal Government*[2] and the 2026 revision of volumes 1 and 2 of the *Financial Audit Manual*.[3] Users should also consider any other relevant standards and guidance.

GAO and CIGIE distributed a limited exposure draft of this revision to staff from various offices of inspector general and independent public accounting firms that perform federal agency financial statement audits. All comments we received were considered in the final FISCAM.

Should you need additional information, please visit https://www.gao.gov/fiscam or contact us at fiscam@gao.gov.

Kristen A. Kociolek
Managing Director
Financial Management and Assurance
U.S. Government Accountability Office

Jennifer L. Fain
Chair, Audit Committee
Council of the Inspectors General on
Integrity and Efficiency

[1]GAO, *Federal Information System Controls Audit Manual*, GAO-24-107026 (Washington, D.C.: September 2024).
[2]GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 2025).
[3]GAO and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual*, vol. 1, GAO-26-108577 (Washington, D.C.: June 2026) and *Financial Audit Manual*, vol. 2, GAO-26-107706 (Washington, D.C.: June 2026).

## GAO

### Financial Management and Assurance

Dawn B. Simpson, Director

Nicole Burkart, Assistant Director

Rebecca L. Perkins, Auditor in Charge

Kristen A. Kociolek, Managing Director

### Applied Research and Methods

Robert F. Dacey, Chief Accountant

### Information Technology and Cybersecurity

Vijay A. D'Souza, Director

Wayne Emilien, Assistant Director

## CIGIE

### Offices of Inspectors General

Phillip Faller, U.S. Department of Defense

Beverly Farley, U.S. Department of Health and Human Services

Branco Garcia, Commodity Futures Trading Commission

Khalid Hasan, Board of Governors of the Federal Reserve System

Kelly McFadden, U.S. Department of Justice

Samantha Tigert, U.S. Department of Health and Human Services

Patrick Wunderlich, U.S. Small Business Administration

## Summary of Significant Changes

This summary lists significant changes from the September 2024 revision of FISCAM.

| Change description | Section or paragraph reference |
|---|---|
| Updated table of contents, headers, and footers to match formatting in FAM. | Throughout |
| Removed lists of figures and tables to match formatting in FAM. | Contents |
| Added abbreviation for PII. | Abbreviations |
| Updated figures 2, 4, and 6 to reflect changes to terms and definitions. | 100<br>200 |
| Updated the overview of the FISCAM methodology to reflect changes in section 200. | 110.11 |
| Replaced “detailed audit plan” with “detailed test plan” to provide clarity. Added “detailed test plan” to the terms defined in the glossary. | 100<br>200<br>300<br>500<br>600A |
| Clarified the relationship between the FISCAM framework and NIST’s frameworks related to cybersecurity and privacy. | 140.12 |
| Clarified the requirement for obtaining evidence of qualifications and independence when using the work of others. | 220.10 |
| Updated requirements and guidance for understanding the entity's IT environment (formerly IT operations), including guidance on identifying sources of information, such as previous audits, attestation engagements, and other studies, related to the engagement objectives, evaluating corrective actions to address findings and recommendations, and understanding inherent risk factors related to the IT environment (the latter two previously included in section 260). | 230 |
| Updated guidance related to the five components of internal control based on the Green Book 2025 revision. | 240.02 |
| Clarified the relationship between the information security management program and the entity’s operational objectives. | 240.03 |
| Removed requirements and guidance for determining the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest. | 240.05<br>270<br>600B |
| Updated guidance related to principles 8, 10, and 13 based on the Green Book 2025 revision. | 240.06<br>530.02<br>Table 1<br>Table 10 |
| Clarified the effect of information technology on internal control for financial statement audits. | 240.08 |
| Updated guidance to align with FAM 2026 for identifying significant business process applications and significant manual processes, | 250.05 |

| | |
|---|---|
| assessing inherent risk, and documenting control activities that address identified risks of material misstatement for financial statement audits. | |
| Updated requirements and guidance to align with FAM 2026 for assessing IS control risk on a preliminary basis, including moving the discussion of inherent risk factors and results of previous audits to section 230; adding the term IS control risk factors; and removing the term IS risk factors. | 260.03 |
| Clarified the relationship between the risks arising from the use of information technology for financial statement audits and IS control risk factors. | 260.06 |
| Updated guidance to align with FAM 2026 for considering whether to implement a tiered approach to evaluating the effectiveness of IS controls. | 320.08 |
| Clarified requirement for documentation related to automated audit tools. | 350.09 |
| Revised definitions, primarily to align with Green Book 2025 and FAM 2026 revisions, for access controls, accuracy, business process, business process controls, completeness, control activities, entity risk assessment, fraud, general controls, indirect general controls, information security management program, information system, information system risk factor, internal control, physical access control, service organization, user control. Added definitions for detailed test plan, information technology environment, and security configuration checklist. Replaced term security objectives with term information security objectives. Removed definition for financial management systems. | 600A |
| Updated the FISCAM assessment completion checklist to reflect changes to requirements. | 600B |
| Clarified purpose and instructions for the FISCAM security management questionnaire. | 600C |

# CONTENTS

## Contents of FISCAM

Section 100 Introduction
- Overview of FISCAM 110
- Fundamental IS Control Concepts 120
- Applicable Auditing and Attestation Standards and Requirements 130
- Applicable Criteria 140

Section 200 Planning Phase
- Overview of the Planning Phase 210
- Perform Preliminary Engagement Activities 220
- Understand the Entity's IT Environment 230
- Understand the Entity's Information Security Management Program 240
- Define the Scope of the IS Controls Assessment 250
- Assess IS Control Risk on a Preliminary Basis 260
- Identify Relevant General Control Objectives 270
- Prepare Planning Phase Documentation 280

Section 300 Testing Phase
- Overview of the Testing Phase 310
- Identify Relevant IS Controls 320
- Determine the Nature, Timing, and Extent of IS Control Tests 330
- Perform IS Control Tests and Evaluate the Results, Including the Significance of IS Control Deficiencies 340
- Prepare Testing Phase Documentation 350

Section 400 Reporting Phase
- Overview of the Reporting Phase 410
- Determine Compliance with FISCAM 420
- Draft Report 430
- Prepare Reporting Phase Documentation 440

Section 500 FISCAM Framework
- Overview of the FISCAM Framework 510
- FISCAM Framework for Business Process Controls 520
- FISCAM Framework for Security Management 530
- FISCAM Framework for Access Controls 540f
- FISCAM Framework for Segregation of Duties 550
- FISCAM Framework for Configuration Management 560

FISCAM Framework for Contingency Planning 570

Section 600 Appendixes

Glossary 600A

FISCAM Assessment Completion Checklist 600B

FISCAM Security Management Questionnaire 600C

## Abbreviations

| | |
|---|---|
| AC | access controls |
| AICPA | American Institute of Certified Public Accountants |
| AT-C | AICPA's *Standards for Attestation Engagements [Clarified]* |
| BP | business process |
| CIGIE | Council of the Inspectors General on Integrity and Efficiency |
| CONOPS | concept of operations |
| CM | configuration management |
| CP | contingency planning |
| 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 Standard |
| FISCAM | *Federal Information System Controls Audit Manual* |
| FISMA | Federal Information Security Modernization Act of 2014 and the Federal Information Security Management Act of 2002 |
| FMFIA | Federal Managers' Financial Integrity Act of 1982 |
| GAGAS | generally accepted government auditing standards |
| Green Book | *Standards for Internal Control in the Federal Government* |
| IS | information system |
| ISCM | information security continuous monitoring |
| IT | information technology |
| NIST | National Institute of Standards and Technology |
| NSS | national security system |
| OMB | Office of Management and Budget |
| PII | personally identifiable information |
| PKI | public key infrastructure |
| SD | segregation of duties |
| SM | security management |

| | |
|---|---|
| SCE | specific control evaluation |
| SP | Special Publication |
| STIG | Security Technical Implementation Guide |
| SRS | simple random selection |
| SYS | systematic random selection |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

# SECTION 100

## Introduction

## 110 Overview of FISCAM

110.01 This section provides an overview of the *Federal Information System Controls Audit Manual* (FISCAM). It describes FISCAM's purpose and applicability, sections and overall objectives, methodology, and framework. This section also contains other information about the manual's technology neutrality and future revisions.

### Purpose and Applicability

110.02 FISCAM presents a methodology for assessing information system (IS) controls. **IS controls** are those internal controls that depend on information system processing—processing performed by information systems using information technology. IS controls include user controls, application controls, and general controls (section 120). This manual uses "IS controls assessment" to refer to the auditor's assessment of IS controls using FISCAM.

110.03 The purpose of the IS controls assessment is to evaluate the design, implementation, and operating effectiveness of IS controls to the extent necessary to achieve the engagement objectives.[4]

- Design is assessed by determining whether an IS control individually, or in combination with other controls, can achieve a control objective and address the related risk.
- Implementation is assessed by determining if an IS control exists and has been placed into operation.
- Operating effectiveness is assessed by determining whether an IS control individually, or in combination with other controls, is operating effectively to achieve a control objective and address the related risk, considering among other things, whether it was applied at relevant times during the audit period, the consistency with which it was applied, and by whom or by what means it was applied.

110.04 The FISCAM methodology is designed to be applied to a wide variety of IS controls assessments that are performed as part of a federal financial audit, attestation engagement, or performance audit. FISCAM is intended to be used in conjunction with the *Financial Audit Manual* (FAM) for federal financial statement audits.[5] FISCAM may also be used for attestation engagements and performance audits when the engagement objectives include assessing the effectiveness of IS controls, similar to an assessment performed for federal financial statement audits. For example, FISCAM may be used to support an engagement team's conclusions regarding the reliability of information that information systems produce that is intended to materially support findings, conclusions, or recommendations for any

[4]Engagement objectives relate to the overall objectives of a federal financial audit, attestation engagement, or performance audit.

[5]GAO and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual*, vol. 1, GAO-26-108577 (Washington, D.C.: June 2026); *Financial Audit Manual*, vol. 2, GAO-26-107706 (Washington, D.C.: June 2026); and *Financial Audit Manual*, vol. 3, GAO-25-107707 (Washington, D.C.: August 2025).

engagement type. Additionally, FISCAM may be used to assess IS controls over compliance requirements and financial reporting in connection with a single audit.[6]

110.05 In contrast, GAO's Cybersecurity Program Audit Guide can be used to conduct performance audits that evaluate key components of an agency's cybersecurity program.[7] Additionally, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Federal Chief Information Officers and Chief Information Security Officers (CISO) councils have developed an evaluation guide[8] for inspectors general to use for annual evaluations performed under the Federal Information Security Modernization Act of 2014 (FISMA).[9] See FISCAM 140.05, 140.07, and 140.13-14 for additional information on FISMA.

110.06 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.[10] 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, "auditor" refers to either (1) an IS controls auditor or (2) another auditor working in consultation with or under the supervision of an IS controls auditor.

## Sections and Overall Objectives

110.07 FISCAM is organized into the following six sections:

- **Section 100 Introduction**. Section 100 introduces FISCAM by providing an overview of the manual, explaining fundamental IS control concepts, identifying applicable audit and attestation standards for auditors, and identifying applicable criteria based on management requirements. Section 100 does not include auditor requirements.
- **Section 200 Planning Phase**. Section 200 includes auditor requirements for planning the IS controls assessment. The overall objective of the planning phase is to determine an effective and efficient plan for obtaining sufficient, appropriate evidence of the design, implementation, and operating effectiveness of IS controls.
- **Section 300 Testing Phase**. Section 300 includes auditor requirements for testing IS controls. The overall objective of the testing phase is to determine

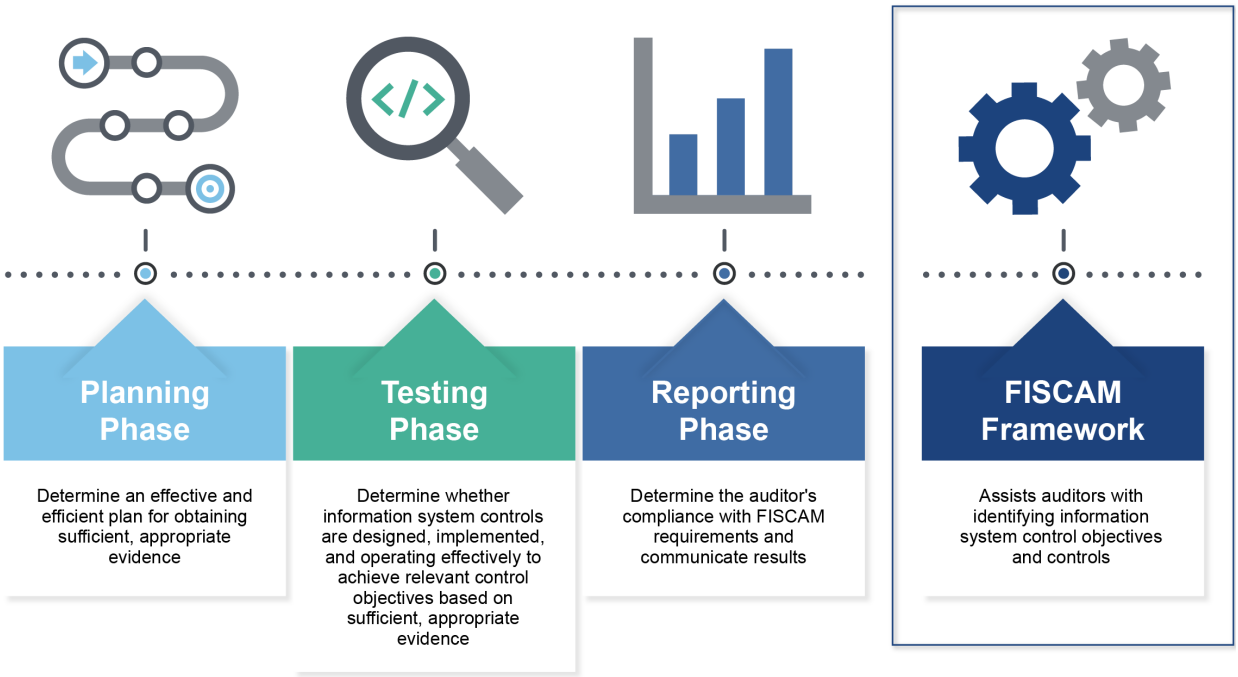
[6]"Single audit" refers to certain audits of nonfederal recipients of federal awards, conducted under the federal Single Audit Act, which is codified at 31 U.S.C. §§ 7501–7506. The Office of Management and Budget (OMB) has issued implementing single audit guidance in subpart F of its Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance), which is reprinted in 2 C.F.R. part 200.
[7]GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: September 2023).
[8]Council of the Inspectors General on Integrity and Efficiency, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*, version 1.0 (Washington, D.C.: May 2025).
[9]Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (*codified, as amended, at* 44 U.S.C. §§ 3551–3559).
[10]In the context of FISCAM, nonfederal entities include state, local, territorial, and tribal governments; nonprofit organizations; and for-profit organizations.

whether IS controls are designed, implemented, and operating effectively to achieve relevant control objectives based on sufficient, appropriate evidence.

- **Section 400 Reporting Phase**. Section 400 includes auditor requirements for reporting the results of the engagement. The overall objectives of the reporting phase are to determine the auditor's compliance with FISCAM requirements and to communicate the results of the information system controls assessment.
- **Section 500 FISCAM Framework**. Section 500 presents an objectives-based control framework—the FISCAM Framework—to assist the auditor in identifying information system control objectives and controls. Section 500 does not include auditor requirements.
- **Section 600 Appendixes**. Section 600 includes three appendixes that contain supplementary information to assist the auditor in applying the FISCAM methodology. Appendix 600A, FISCAM Glossary, defines the terms used throughout FISCAM. Appendix 600B, FISCAM Assessment Completion Checklist, is designed to assist auditors in determining whether they have complied with FISCAM requirements. Appendix 600C, FISCAM Security Management Questionnaire, is designed to assist auditors in determining whether the entity's information security management program is suitably designed, properly implemented, and operating effectively.

Sections 200 through 400 make up the FISCAM methodology and section 500 contains the FISCAM Framework (see fig. 1), which is integral to the FISCAM methodology.

**Figure 1: Overall Objectives of the Federal Information System Controls Audit Manual (FISCAM) Methodology and Framework**




Source: GAO (data and icons). | GAO-26-108633

## FISCAM Methodology

110.08 The FISCAM methodology is designed to enable the auditor to develop the scope of the IS controls assessment during the planning phase. **Scope** is the boundary of the IS controls assessment and is directly tied to the engagement objectives.

110.09 Developing the scope of the IS controls assessment begins with the auditor obtaining an understanding of the engagement objectives—the subject matter and performance aspects to be evaluated and reported on, based on evidence obtained and assessed against criteria. With this understanding, the auditor identifies and obtains an understanding of the business processes and business process controls that are significant to the engagement objectives (section 250). Business processes involve transforming inputs into outputs through a series of transactions, activities, and events to achieve the entity's objectives that are significant to the engagement objectives (e.g., financial reporting). Business process controls are the structure, policies, and procedures that operate over individual transactions; activities across business processes; and events between information systems relevant to the business process.

110.10 The understanding of significant business processes and business process controls assists the auditor with identifying the entity's information systems to include in the scope of the IS controls assessment based on their significance to the engagement objectives (areas of audit interest). In the context of FISCAM, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

110.11 The auditor continues to scope the IS controls assessment by assessing IS control risk on a preliminary basis (section 260). IS control risk, as defined by FISCAM, is the likelihood that conditions or events related to the areas of audit interest (1) could significantly affect the entity's ability to achieve its information processing objectives (completeness, accuracy, and validity), and (2) will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls. In assessing IS control risk, the auditor considers the extent to which IS controls are likely to mitigate risk factors to achieve relevant control objectives. The auditor assesses the level of IS control risk for each area of audit interest based on the auditor's understanding of inherent risk factors (section 230), IS control risk factors (section 260), and fraud risk factors (section 260). The auditor also considers information gathered to evaluate whether the entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant to the engagement objectives (section 230).

110.12 The auditor is then able to identify control objectives pertaining to the areas of audit interest that are necessary to achieve the engagement objectives (relevant control objectives). The preliminary IS control risk assessment and the FISCAM Framework assist the auditor with identifying relevant control objectives for each area of audit interest (section 270). See paragraphs 110.17 through 110.20 for discussion of the FISCAM Framework.

110.13 Based on the scope of the IS controls assessment, the auditor develops the approach during the testing phase. **Approach** is the nature, timing, and extent of audit procedures applied to the significant business processes and areas of audit interest based on the relevant control objectives and the relevant IS controls. **Relevant IS controls** are the user, application, and general controls that are

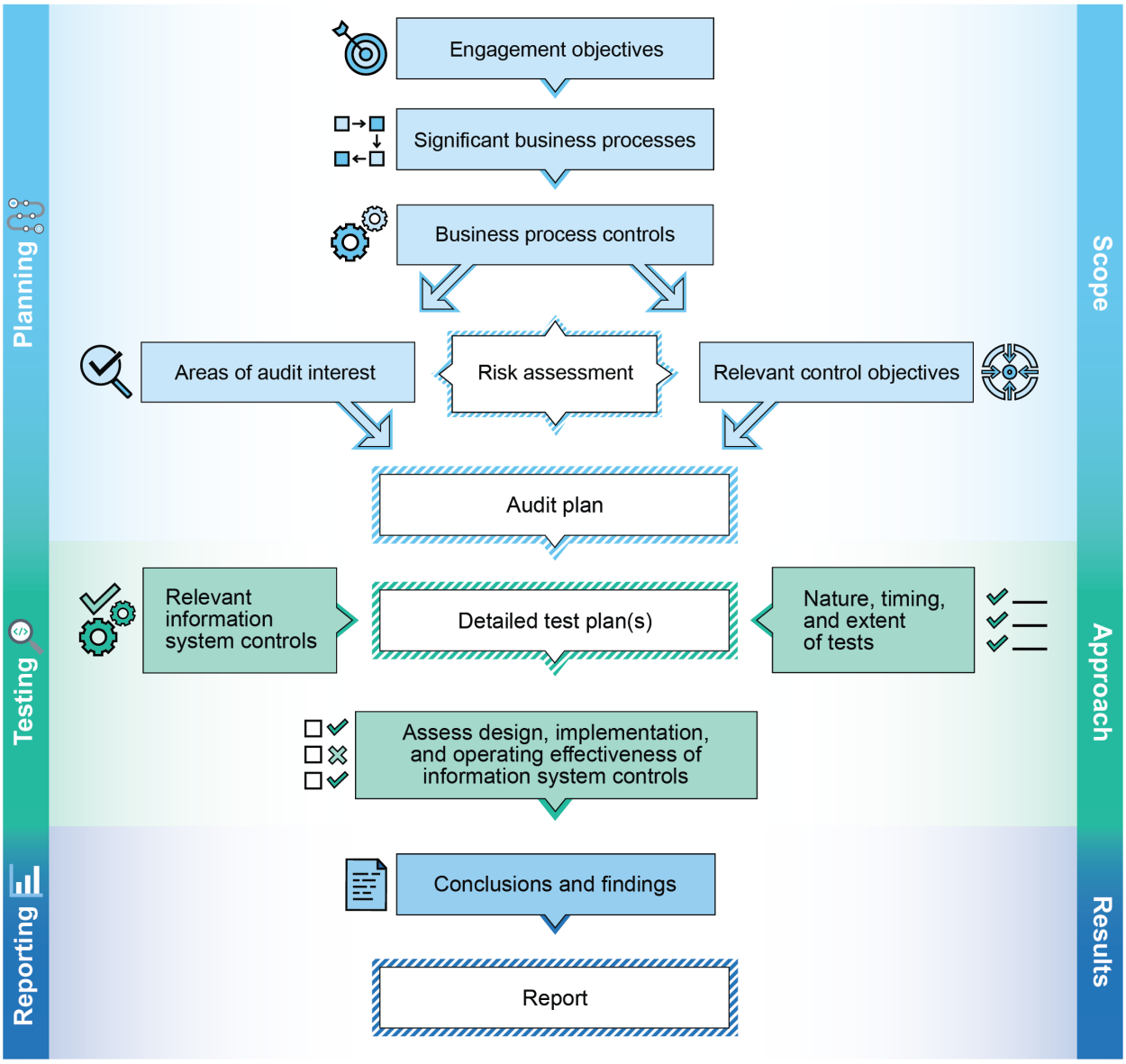
necessary to achieve the relevant control objectives; that are suitably designed; and that the auditor plans to test for implementation and operating effectiveness.

110.14 The auditor develops planned audit procedures and documents them in the audit plan. **Planned audit procedures** are the specific steps auditors plan to perform to address the engagement objectives. This includes the procedures necessary to determine the nature, timing, and extent of IS control tests for the relevant IS controls (sections 320 and 330). The auditor completes a detailed test plan for each area of audit interest.

110.15 The auditor assesses the design, implementation, and operating effectiveness of relevant IS controls based on the tests performed and determines whether they achieve the relevant control objectives (section 340). The auditor arrives at conclusions based on the evidence obtained. The auditor develops findings to the extent necessary to assist management in understanding the need for taking corrective action. See paragraphs 430.11 and 430.12 for further discussion of developing the elements of a finding (i.e., criteria, condition, cause, and effect). The auditor then issues a report to communicate the results. The content of the report depends on the engagement objectives (section 430).

110.16 This high-level process for performing an IS controls assessment using the FISCAM methodology is depicted in figure 2.

**Figure 2: The Federal Information System Controls Audit Manual Methodology**



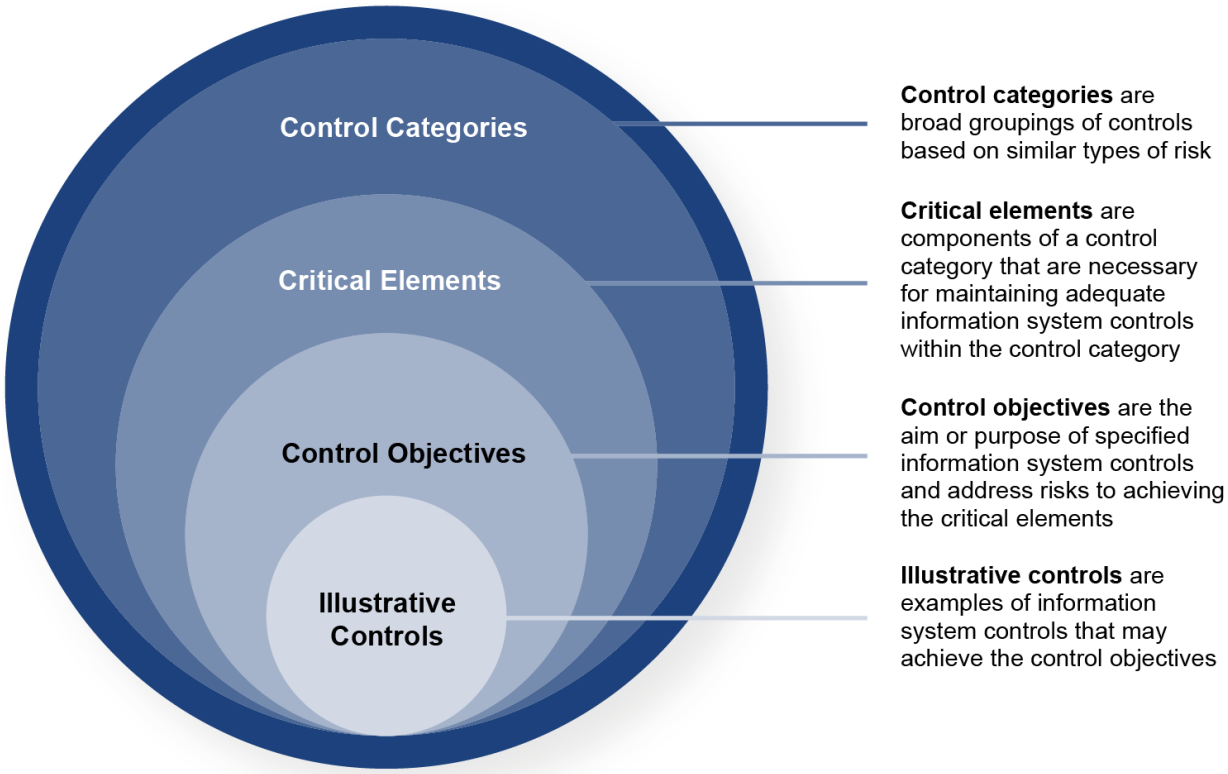

Source: GAO (data and icons). | GAO-26-108633

## FISCAM Framework

110.17 The FISCAM Framework presents control categories, critical elements, control objectives, and illustrative controls in a hierarchical structure to facilitate the auditor's planning, testing, and reporting procedures (shown in fig. 3). **Control categories** are broad groupings of information system controls based on similar types of risk. Control categories consist of the following: business process controls, security management, access controls, configuration management, segregation of duties, and contingency planning. **Critical elements** are components of a control category that are necessary for maintaining adequate information system controls within the control category. **Control objectives** are the aim or purpose of specified information

system controls and address risks to achieving the critical elements. **Illustrative controls** are examples of information system controls that may achieve the control objectives. The FISCAM Framework includes illustrative controls for each control objective within the critical elements of the control categories.

**Figure 3: Components of the Federal Information System Controls Audit Manual Framework**




Source: GAO. | GAO-26-108633

110.18 The components of the FISCAM Framework are presented in table format and include a four-tiered alphanumeric numbering scheme for referencing these components. See section 510 for further discussion of the table format and numbering scheme.

110.19 The FISCAM Framework's control categories are consistent with those included in generally accepted government auditing standards (GAGAS).[11] The FISCAM Framework's critical elements and control objectives are consistent with the principles and attributes included in the *Standards for Internal Control in the Federal Government* (Green Book).[12] Specifically, the critical elements and control objectives within the security management control category incorporate the Green Book principles and attributes associated with the control environment, risk assessment, information and communication, and monitoring components of internal control. The critical elements and control objectives within the remaining control categories incorporate the Green Book principles and attributes associated with the control

[11]GAO, *Government Auditing Standards: 2018 Revision*, GAO-21-368G (Washington, D.C.: July 2018, updated April 2021). Early implementation of this revision is permitted.
[12]GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 2025).

activities component of internal control. Additionally, the illustrative controls presented in the FISCAM Framework are consistent with management requirements for information security and privacy controls included in National Institute of Standards and Technology (NIST) Computer Security Resource Center publications—and specifically include the information security and privacy controls presented in NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*,[13] including the patch release.[14]Though the FISCAM Framework presents illustrative controls based on NIST SP 800-53, it is not intended to be used as criteria. See section 140 for further discussion of criteria. Considering the illustrative controls, the auditor identifies the entity's IS controls that may achieve the control objectives. The auditor is ultimately responsible for obtaining an understanding of information security and privacy controls designed and implemented by the entity in sufficient detail to assess IS control risk and design appropriate audit procedures.

110.20 Additionally, though the FISCAM Framework presents illustrative audit procedures for each illustrative control, it is not intended to be used as an audit plan (section 280). Rather, it is incumbent upon the auditor to prepare an audit plan, which includes a detailed test plan for each area of audit interest, that supports achieving the engagement objectives and is responsive to the auditor's assessment of IS control risk. 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 control objectives.

## Other Information

### Technology

110.21 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

110.22 IS control-related criteria change periodically. The auditor is responsible for monitoring and considering any changes to IS control criteria that may be applicable to the engagement.

[13]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).

[14]On November 7, 2023, NIST issued a patch release of SP 800-53 (Release 5.1.1) that includes one new information security control related to identification and authorization, which is published at https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IA-13.

## 120 Fundamental IS Control Concepts

120.01 This section describes fundamental IS control concepts used throughout FISCAM. It defines IS controls and describes IS control types, related organizational objectives, and related FISCAM control categories. The section also contains information about the levels at which these IS control types may be implemented.

### IS Control Types

120.02 **IS controls** are those internal controls that depend on information system processing— processing performed by information systems using information technology. Types of IS controls include the following:

- User controls – 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 actions established through policies and procedures that apply to all or a large segment of an entity's information systems.

### IS Control Types and Organizational Objectives

120.03 User and application controls are designed to achieve one or more of the following information processing objectives:

- Completeness – All transactions, events, and balances that should have been recorded have been properly recorded.[15]
- Accuracy – Data relating to transactions, events, and balances are properly and timely recorded.
- Validity – All recorded transactions and events actually occurred, are related to the entity, and were executed according to prescribed procedures. All recorded balances are appropriately supported and have been properly recorded.

Direct general controls apply to information systems used within the business process and directly support the effective operation of user and application controls. Direct general controls comprise controls to reasonably assure that

- business process applications are properly managed to achieve information processing objectives,
- system interfaces are properly managed to achieve information processing objectives, and
- data management systems are properly managed to achieve information processing objectives.

[15]Transactions and events occur over a period of time, while balances relate to a point in time (e.g., unliquidated obligations as of the end of the year).

When designed, implemented, and operating effectively, user, application, and direct general controls reasonably assure the completeness, accuracy, and validity of transactions, events, and data.

120.04 Indirect general controls, which apply to the information security management program and information systems, maintain a suitable environment to support the effective operation of user, application, and direct general controls. Indirect general controls are generally related to 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.[16] 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.

Weaknesses in indirect general controls can circumvent or impair the effectiveness of direct general controls and can result in unauthorized access to, modification of, and disclosure of sensitive data and programs and disruption of critical operations.

## IS Control Types and Implementation Levels

120.05 IS controls are applied at three levels: business process, system, and entity. Each level is described below.

- Business process level refers to the level at which user, application, and direct general controls relevant to specific business processes are implemented. These controls are specific to a business process and often correspond to information resources (i.e., data and information technology) employed by the business process—business process applications, process automation software, system-generated reports, system interfaces, and data management systems.
- System level refers to the level at which direct and indirect general controls relevant to an information system are implemented. These controls are specific to certain information systems and often correspond to one of three sublevels inherent in all information systems: infrastructure, platform, and software.
    - Infrastructure generally comprises the physical information system components necessary to run software and includes the computer and hardware devices used for information processing, data storage, and network communication. Infrastructure also includes the logical

[16]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.

information resources necessary to run multiple virtual machines on shared physical information system components.

- Platform generally comprises the logical information 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.

120.06 Entity level refers to the level at which indirect general controls relevant to the entire entity or component are implemented. These controls are broader than those applied at the system level and often correspond to the entity's information security management program or most of its information systems.

## IS Control Types and FISCAM Control Categories

120.07 The FISCAM Framework groups IS controls within six control categories based on their relevance to the business process. Those IS controls that are directly related to the business process (i.e., user, application, and direct general controls) are included in the **business process controls (BP) category**. This category relates to the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions; activities across business processes; and events between business process applications, their components, and other systems. Business process controls include direct general controls that support information processing objectives (completeness, accuracy, and validity). Without adequate business process controls, incomplete, inaccurate, or invalid data can be input intentionally or unintentionally by individuals, improperly processed by the information system, and improperly included in output.

120.08 Those IS controls that are indirectly related to the business process (i.e., indirect general controls) are included in the following:

- **Security management (SM)** category provides the foundation of a 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 managing risk, developing and implementing effective security policies, assigning and communicating 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 information resources (i.e., processes, data, and information technology) and disproportionately high expenditures for controls over low-risk resources.
- **Access controls (AC)**, also known as logical and physical access, category limits access or detects inappropriate access to information resources (e.g., data and information technology), thereby protecting these resources against unauthorized modification, loss, and disclosure. Logical access controls require users to authenticate themselves and limit the files and other information resources that authenticated users can access and the actions

that they can execute. Physical access controls involve restricting physical access to information resources and facilities. Inadequate access controls can result in unauthorized access to, modification of, or disclosure of sensitive data and programs and disruption of critical operations.

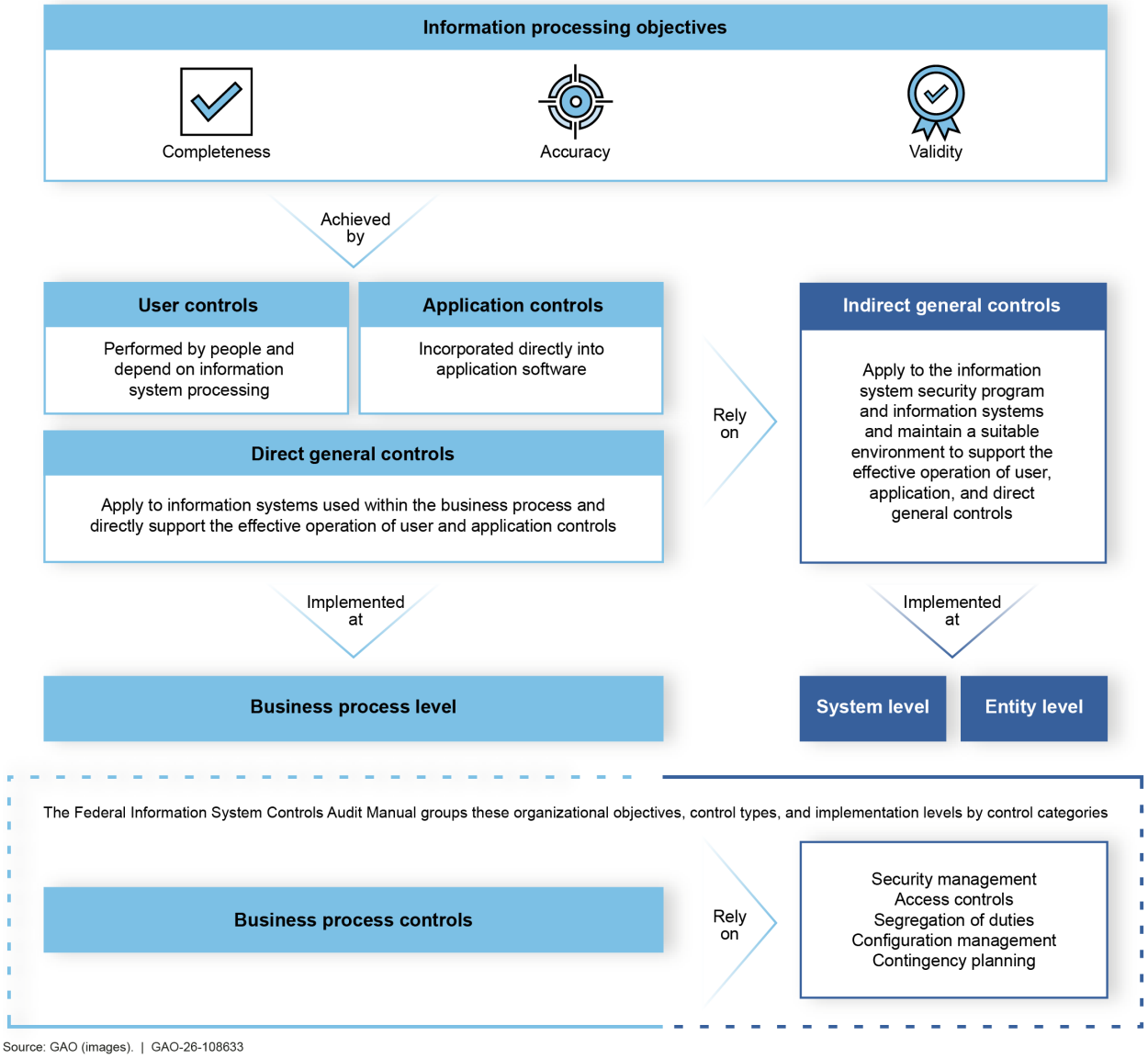
- **Segregation of duties (SD)** category relates to the policies, procedures, and an organizational structure for managing who can control key aspects of computer-related operations and thereby prevent unauthorized actions or access to assets or records. Segregation of duties involves segregating work responsibilities so that one individual does not control all critical stages of a process. 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. Without adequate segregation of duties, erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed.
- **Configuration management (CM)** category relates to identifying and managing operating and security features for information technology (e.g., hardware, software, firmware, equipment, media, and services) at a given point and systematically controlling 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 systems and provide reasonable assurance that systems are securely configured and operated as intended. 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. Configuration management also involves identifying vulnerabilities and applying platform and software updates to close security vulnerabilities and improve functionality.

  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. Without proper configuration management controls, there is a risk that security features could be inadvertently or deliberately omitted or turned off or that processing irregularities or malicious code could be introduced. Without effective configuration management, users do not have adequate assurance that the information system will work as intended and to the extent needed to support their operations.
- **Contingency planning (CP)** category provides 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 resources (i.e.,

people, processes, data, and information technology), protecting facilities, and minimizing the risk of unplanned interruptions. It also involves having a plan to recover and reconstitute information systems should system disruptions occur. Without adequate contingency planning controls, system disruptions, compromises, or failures causing lost or incorrectly processed data can result in financial losses, expensive recovery efforts, and inaccurate or incomplete information.

120.09 The relationship between fundamental IS control concepts discussed in this section is illustrated in figure 4.

**Figure 4: Fundamental Information System Control Concepts**




Source: GAO (images). | GAO-26-108633

## 130 Applicable Auditing and Attestation Standards and Requirements

130.01 In conducting the IS controls assessment in accordance with GAGAS (2018), the GAGAS requirements and guidance apply based on the type of engagement. The requirements and guidance in GAGAS (2018) chapters 1 through 6 apply to financial audits; GAGAS (2018) chapters 1 through 5 and 7 apply to attestation-level examination, review, and agreed-upon procedures engagements; and GAGAS (2018) chapters 1 through 5, 8, and 9 apply to performance audits.[17]

130.02 FISCAM incorporates by reference the GAGAS requirements presented in chapters 1 through 9—including the American Institute of Certified Public Accountants (AICPA) requirements that GAGAS (2018) incorporates by reference for federal financial audits and attestation-level examination, review, and agreed-upon procedures engagements. 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 (2018).

130.03 For federal financial audits, FISCAM is to be used in conjunction with the FAM.[18] The FAM includes references to the AICPA's *Auditing Standards [Clarified]* and *Standards for Attestation Engagements [Clarified]*. FISCAM refers to the FAM for additional requirements and guidance, as appropriate.

130.04 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).[19]

130.05 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.

[17]GAO-21-368G. References to this document are noted as "GAGAS (2018)" in the FISCAM. There is a 2024 revision to GAGAS that is effective for financial audits, attestation engagements, and reviews of financial statements for periods beginning on or after December 15, 2025, and for performance audits beginning on or after December 15, 2025.

[18]GAO-26-108577, GAO-26-107706, and GAO-24-107280.

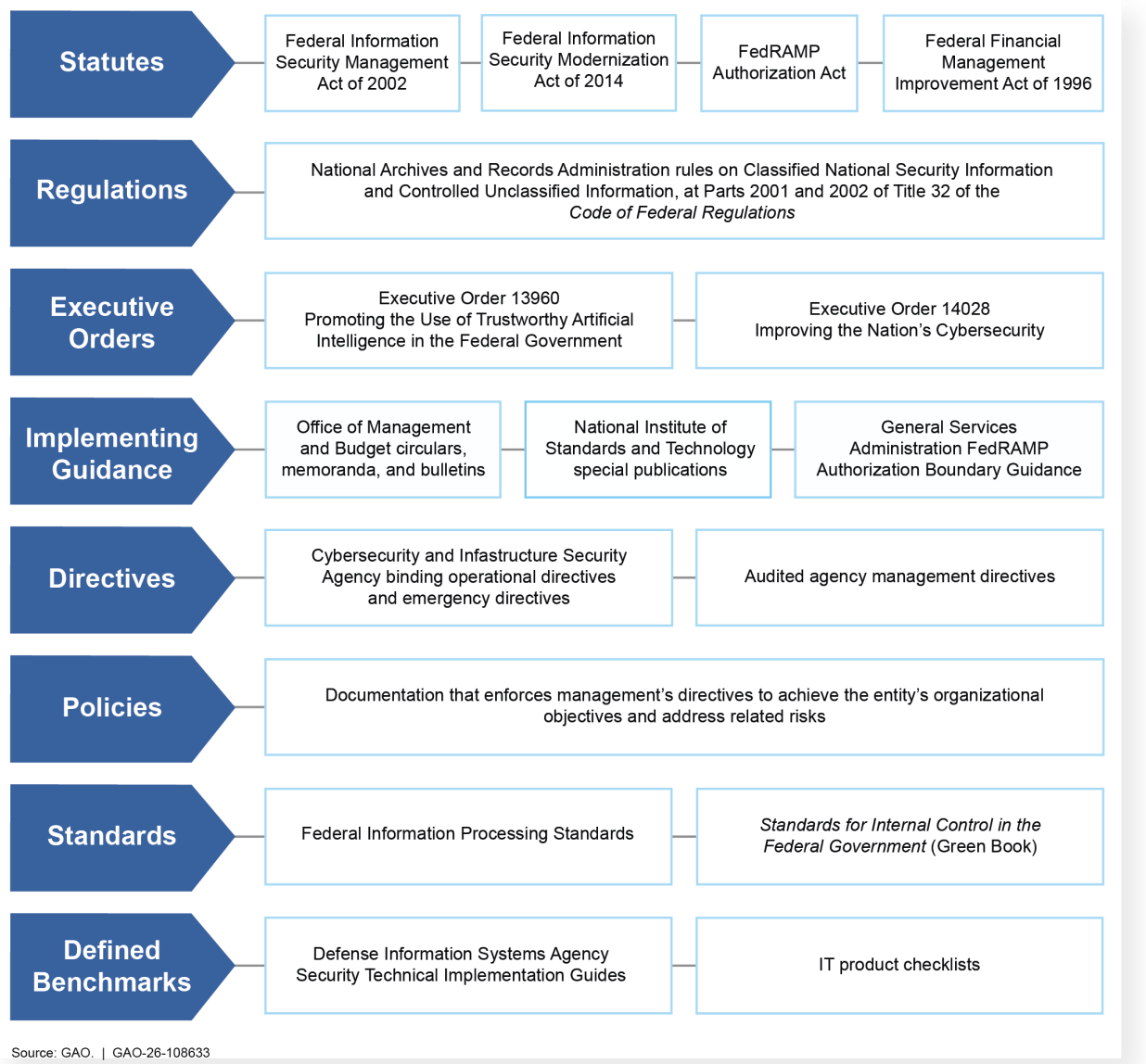
[19]ISACA, *IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit*, 4th ed. (Schaumburg, Ill.: 2020).

130.06 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 each term is intended.

## 140 Applicable Criteria

140.01 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 relevant provisions in statutes, regulations, executive orders, implementing guidance, directives, policies, contracts, grant agreements, standards, measures, expected performance, defined business practices, and defined benchmarks against which performance is compared or evaluated. Examples of selected criteria are provided in figure 5.

**Figure 5: Examples of Selected Criteria by Type**




Source: GAO. | GAO-26-108633

140.02 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

140.03 The Federal Managers' Financial Integrity Act of 1982 (FMFIA)[20] requires federal executive management to establish internal accounting and administrative controls consistent with internal control standards prescribed by the Comptroller General. Since 1983, these standards have been presented in the Green Book, which GAO has updated periodically.[21] The Green Book prescribes these standards and provides criteria for an effective system of internal control in federal entities. The Green Book applies to all entity 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.

140.04 The critical elements and control objectives included within the FISCAM Framework presented in section 500 are consistent with the principles and attributes included in the Green Book. See paragraph 110.19 for additional discussion.

## Office of Management and Budget Information and Guidance

140.05 Under FISMA,[22] OMB, in coordination with DHS, is responsible for overseeing civilian executive entity information security policies and practices based on standards that NIST develops and the Secretary of Commerce promulgates.[23] See paragraphs 140.13 and 140.14 for discussion of DHS. OMB uses circulars, bulletins, and memorandums to provide information and guidance, including areas applicable to information security. The following circulars provide guidance that establishes information security requirements for federal executive entities:

- OMB Circular No. A-123, *Management's Responsibility for Internal Control*, defines management's responsibilities for establishing, maintaining, and assessing internal control over operations, reporting, and compliance.[24]
- 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, IT

[20]31 U.S.C. § 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act.
[21]GAO-25-107721.
[22]Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (*codified, as amended, at* 44 U.S.C. §§ 3551–3559). 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). Several 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 that NIST develops and the Secretary of Commerce promulgates under 40 U.S.C. § 11331.
[23]NIST is established within the Department of Commerce as a science, engineering, technology, and measurement laboratory, and it 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.
[24]Office of Management and Budget, *Management's Responsibility for Internal Control*, OMB Circular No. A-123 (Washington, D.C.: March 10, 2026).

resources, and supporting infrastructure and services.[25] 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

140.06 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 SPs (e.g., 800 series guidelines) and, where appropriate and directed by OMB, NIST interagency or internal reports.[26] 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

140.07 FIPS are standards and guidelines for federal information systems (other than national security systems) that NIST develops when there are no acceptable industry standards or solutions for a particular government requirement. Under the Clinger-Cohen Act of 1996 (codified, as amended, at 40 U.S.C. § 11331), NIST issues FIPS after approval by the Secretary of Commerce. FISMA requires federal agencies to comply with applicable requirements for federal information systems, such as FIPS. The applicability section of each of the FIPS details when a standard is applicable and mandatory.

140.08 NIST developed and issued the following mandatory FIPS 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.[27] 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.[28] The minimum security requirements cover security-related areas that support protecting the confidentiality, integrity, and availability of federal information systems and the information that those systems process, store, and transmit.

[25]Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular No. A-130 (Washington, D.C.: July 15, 2016).
[26]OMB Circular No. A-130, Managing Information as a Strategic Resource, p. 18, app. I-4.
[27]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199 (Gaithersburg, Md.: March 2004).
[28]National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Gaithersburg, Md.: March 2006).

140.09 FIPS publications do not apply to national security systems.[29] The Committee on National Security Systems is responsible for providing system security guidance for national security systems.

## Special Publications

140.10 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 controls, assessing security controls, authorizing information systems, and monitoring the security and privacy posture of the information system and the organization.[30] 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 Organizations*, 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.[31] 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*.[32] 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

[29]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)." Several FISMA provisions, such as those codified as sections 3553 and 3554 of Title 44, U.S. Code, establish requirements related to standards and guidelines prescribed by the Secretary of Commerce under 40 U.S.C. § 11331, which specifically exclude national security systems.

[30]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).

[31]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, rev. 5 (Gaithersburg, Md.: September 2020).

[32]National Institute of Standards and Technology, *Control Baselines for Information Systems and Organizations*, SP 800-53B (Gaithersburg, Md.: December 2020).

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.[33] 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.
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, assists organizations in developing an ISCM strategy and implementing an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls.[34] The ISCM strategy and program support ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner.

140.11 The illustrative controls included within the FISCAM Framework address information security and privacy control requirements presented in NIST Computer Security Resource Center publications (e.g., FIPS and SPs) and specifically include the information security and privacy controls presented in NIST SP 800-53.

140.12 In addition to NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST provides frameworks to assist entities with identifying and managing risks specifically related to privacy and cybersecurity. While FISCAM does not discuss these frameworks, the information security and privacy controls included in NIST SP 800-53 address such risks. These controls are included in the FISCAM Framework. In addition, NIST provides various crosswalks between the frameworks and the controls.

## DHS Directives and Defense Information Systems Agency Security Technical Implementation Guides

140.13 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.[35] DHS's Cybersecurity and Infrastructure Security Agency 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

[33]National Institute of Standards and Technology, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, SP 800-70, rev. 5 (Gaithersburg, Md.: May 2026).
[34]National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, SP 800-137 (Gaithersburg, Md.: September 2011).
[35]See 44 U.S.C. § 3553(a)-(b), which sets out the authority and functions of the OMB Director and the Secretary of Homeland Security.

entities. These directives are published at https://www.cisa.gov/news-events/directives.

140.14 Under FISMA, (1) the Department of Defense (DOD) is responsible for overseeing noncivilian 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 is responsible for overseeing noncivilian 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.[36] 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.[37] DISA's STIGs provide implementation guidance for specific products and versions. They also contain all requirements flagged as applicable for a product that has been selected on a DOD control baseline.

## Management Policies and Procedures

140.15 Policies and procedures enforce management's directives to achieve the entity's objectives and address related risks. 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. For information systems, policies and procedures may be applied at the business process, system, and entity levels.

[36]See 44 U.S.C. § 3553(e), which sets out the authority of the Secretary of Defense in relation to DOD information systems and the Director of National Intelligence in relation to the intelligence community's information systems.
[37]DOD Instruction 8500.01, "Cybersecurity" (rev. Oct. 7, 2019).

# SECTION 200

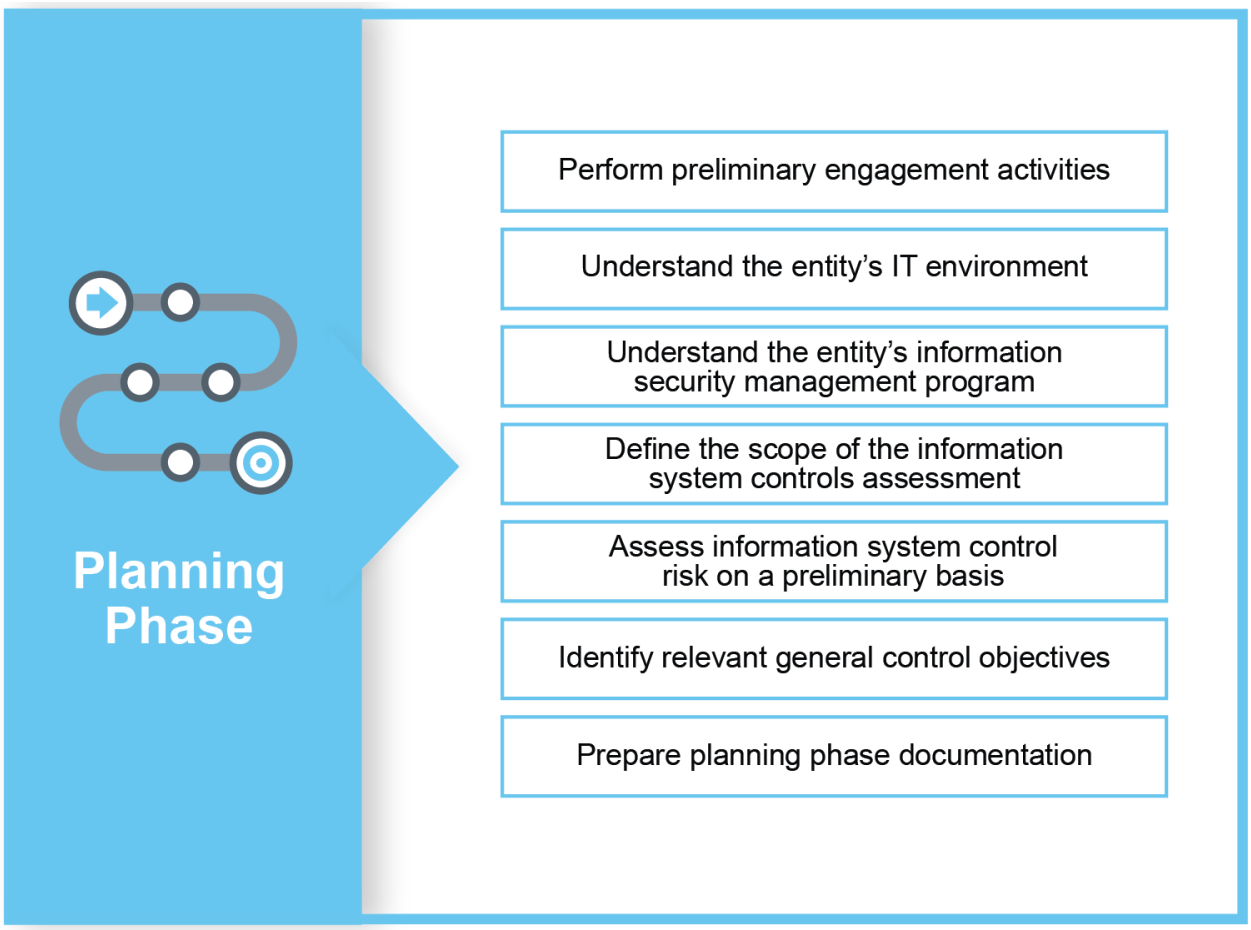
## Planning Phase

## 210 Overview of the Planning Phase

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

210.02 The engagement team meets this overall objective for planning the IS controls assessment by performing the planning activities in figure 6.

**Figure 6: Planning Phase Activities**




Source: GAO (data and icons). | GAO-26-108633

210.03 When performing the IS controls assessment, the nature and extent of planning activities vary 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.

210.04 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.

210.05 Planning activities are intended to be iterative, in that, as information is obtained throughout the engagement, it is evaluated for its potential effect on IS control risk. Adjustments to the IS controls assessment scope and approach may be necessary to address additional risk factors identified, regardless of the phase in which the information is obtained. For example, the auditor could obtain new information about a business process application during the testing phase that may have an effect on the auditor's risk assessment. The auditor considers and, as appropriate, adjusts the scope and approach of the IS controls assessment accordingly to obtain sufficient, appropriate evidence to support the engagement objectives.

210.06 During the planning phase, the concepts of significance and audit risk assist auditors in determining the scope (paragraph 110.08). **Significance** is the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Throughout this manual, the term significance is comparable to the term material—as used in the context of federal financial audits. Such factors include the magnitude of the matter in relation to the subject matter of the engagement, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the effect of the matter on the audited program or activity. **Audit risk** is the possibility that the auditor's findings, conclusions, recommendations, or assurance may be improper or incomplete. The underlying principle of these concepts is that the auditor is not required to spend resources on items of little importance, that is, those that would not affect the judgment or conduct of a reasonable user of the audit report, considering surrounding circumstances. Based on this principle, the auditor establishes the scope and approach of the IS controls assessment to exclude areas of the entity's operations that are not significant to the engagement objectives and therefore warrant little or no audit attention.

210.07 Professional judgment assists auditors when evaluating significance and audit risk to the engagement objectives. **Professional judgment** is the use of the auditor's professional knowledge, skills, and abilities, in good faith and with integrity, to diligently gather information and objectively evaluate the sufficiency and appropriateness of evidence. Professional judgment includes exercising reasonable care and professional skepticism.

## 220 Perform Preliminary Engagement Activities

220.01 For the IS controls assessment, preliminary engagement activities include assigning a combination of auditors and IT specialists to the engagement team who collectively possess the competence needed to address the engagement objectives and communicating the engagement terms with management, those charged with governance, and others. These activities are performed either at the beginning of or throughout an engagement and are distinct from audit procedures performed to address the engagement objectives.

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

### Assigning Auditors and IT Specialists

220.03 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 and perform their work. For the IS controls assessment, a broad range of knowledge, skills, and abilities may be needed to perform effective and efficient audit procedures.

220.04 The engagement team may include a combination of financial, performance, and IS controls auditors and IT specialists. IT specialists possess special knowledge or skills in the IT field that extend beyond the knowledge and skills normally possessed by those working in specialized fields of auditing. A combination of IS controls auditors and IT specialists with technical skills in areas such as networks, operating systems, data management systems, infrastructure applications, access control software, and application-specific technical knowledge may be needed to identify and assess general controls at the business process, system, and entity levels.

220.05 The audit organization considers the levels of proficiency needed for each role on the engagement when assigning auditors to the engagement. The following are references to roles at GAO; however, descriptions of proficiency levels in relation to the audit are included so that corresponding roles can be identified in other audit organizations.

- Nonsupervisory auditors plan or perform audit procedures characterized by low levels of ambiguity, complexity, and uncertainty. Nonsupervisory auditors assigned to the IS controls assessment require a basic level of proficiency in auditing and information technology to perform assigned audit work. This includes fundamental knowledge of or limited experience with auditing tasks (e.g., interviewing, gathering and documenting evidence, and communicating both orally and in writing) and information technology (e.g., networks, operating systems, data management systems, infrastructure applications, and access control software).
- Supervisory auditors plan or direct engagements and perform audit procedures characterized by moderate levels of ambiguity, complexity, and uncertainty. Supervisory auditors assigned to the IS controls assessment have an intermediate level of proficiency in auditing and information technology to perform or direct assigned audit work. This includes practical

application of auditing tasks and IT expertise to allow for proper review of audit documentation; assessment of the appropriateness and sufficiency of evidence; management of projects; and identification and assessment of general controls at the entity, system, and business process levels.

- Partners and directors plan, direct, or report on engagements and perform or review audit procedures characterized by high levels of ambiguity, complexity, and uncertainty. Partners and directors have an advanced level of proficiency in auditing and information technology to manage the quality of the engagement.

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

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

## Using the Work of Others

220.07 The engagement team may use the work of auditors and IT specialists outside of the audit organization to support findings or conclusions for the IS controls assessment. These other auditors and IT specialists may be part of an independent public accounting firm contracted by the audit organization, part of the entity's internal audit function, and IT specialists contracted by the audit organization. The work of others may provide useful information for planning and conducting the IS controls assessment.

220.08 The auditor should determine whether other auditors have completed or are completing IS controls work that is relevant to the engagement objectives. If such IS

controls work is being performed, the auditor should determine whether the scope, quality, and timing of the work can be relied on within the context of the current engagement objectives.

220.09 The auditor may determine that the audit organization will contract with other auditors or IT specialists to perform all or a portion of the IS controls assessment. The auditor's participation in the procurement process when the audit organization contracts for IT audit support services can be instrumental in determining the scope of such services, specifying minimum qualifications for the competence of contracted staff, and developing documentation requirements. The *Federal Information System Controls Audit Manual* (FISCAM) may be required to be used as a basis for the work to be performed.

220.10 If the auditor determines that the audit organization will use the work of other auditors, IT specialists, or both to perform all or a portion of the IS controls assessment, the auditor should, as applicable,

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

220.11 If the auditor determines that the work of the IT specialist is not adequate for the auditor's purposes, the auditor should agree with the IT specialist on the nature and extent of further work that the IT specialist is to perform or perform additional audit procedures appropriate to the circumstances.

220.12 For federal financial audits, the auditor should comply with requirements for using the work of others discussed in FAM 600, Using the Work of Others, as applicable.

## Communication of Engagement Information

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

- Communicating the scope and approach of the IS controls assessment. This may include (1) an overview of the engagement objectives, including how the IS controls assessment will support achieving such objectives, and (2) high-level information about the approach, including who will be performing the IS controls tests, the tools that will be employed, and any precautions the engagement team plans to take to mitigate the risk of service degradation or

interruption (for example, performing certain testing during nonpeak hours). However, it is important that the auditor not compromise the effectiveness of the IS controls assessment or the engagement. For example, communicating the nature and timing of detailed audit procedures may reduce the effectiveness of those procedures by making them too predictable.

- Identifying roles and responsibilities. This includes addressing the roles and responsibilities of key members of the engagement team, as well as management.
- Addressing logistical requirements. Logistical requirements may include on-site workspace arrangements and procedures for safeguarding sensitive information.

## 230 Understand the Entity's IT Environment

230.01 Once preliminary engagement activities have been performed, the auditor begins planning the IS controls assessment to address the engagement objectives by obtaining an understanding of the entity's IT environment. An entity's IT environment comprises the entity's IT operations and the IT applications and supporting IT infrastructure that the entity uses to support its operations and achieve strategic objectives. This enables the auditor to understand inherent risk factors related to the entity's IT environment and establishes a foundation for the auditor to assess IS control risk on a preliminary basis (section 260).

230.02 The auditor should obtain an understanding of the entity's IT environment sufficient to plan the engagement. Obtaining an understanding of the entity's IT environment includes consideration of

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

230.03 When planning the audit, the auditor should ask management to identify previous audits, attestation engagements, and other studies that directly relate to the engagement objectives. This would include weaknesses management identified through its monitoring controls (e.g., for federal entities, plans of action and milestones) that relate to the entity's IT environment. The auditor uses this information to assess IS control risk on a preliminary basis and determine the nature, timing, and extent of further audit procedures. The auditor should evaluate whether the entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant to the engagement objectives.

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

- the results of previous audits, examinations, and other internal control assessments, including management reviews, relevant to the engagement objectives;
- entity policies and procedures;
- management officials;

- key personnel involved in IT operations;
- program managers (for programs significant to the engagement objectives);
- office of inspector general and internal audit managers;
- other members of the audit organization (concerning relevant completed, planned, or in-progress engagements involving the entity);
- personnel within the entity's or the audit organization's office of general counsel;
- personnel within the entity's or the audit organization's special investigations unit; and
- other relevant reports and articles issued by or about the entity, including
    - the entity's prior Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. § 3554(c)) or equivalent reports on IS controls;
    - the entity's annual performance and accountability report or equivalent reports on performance, including reports filed to comply with the Federal Financial Management Improvement Act of 1996 (FFMIA) and Federal Managers' Financial Integrity Act of 1982 (FMFIA);
    - other reports by management, the auditor, or others that contain information concerning IS controls that are relevant to the engagement objectives;
    - service organization reports, if available, for any operations, processes, or controls that service organizations perform on behalf of the entity;
    - GAO reports;
    - inspector general reports and internal audit reports (including those for performance audits and other reviews); and
    - consultant reports.

230.05 The auditor should obtain an understanding of inherent risk factors related to the entity's IT environment. A complex IT environment, or one that is undergoing significant change, may increase inherent risk. Additionally, the information technology the entity employs can introduce inherent risk factors. When understanding inherent risk factors related to the entity's IT environment, the auditor considers the following:

- Certain types of hardware and software in use may be more susceptible to threats than others. For example, altered or counterfeit hardware components could allow attackers to gain unauthorized access through backdoors and spyware. In addition, outdated, unpatched, or unsupported firmware, software, and information system components present greater inherent risk than those that are updated, patched, and supported by the developer, vendor, or manufacturer.

- The entity's use of new or emerging technology can increase the risk that secure configurations of corresponding information system components may not be well-developed or tested, or that IT personnel may not have the knowledge, skills, and abilities necessary to properly select and implement security controls over such technology.
- The consistency of the system-level security and privacy architectures with the entity's enterprise architecture, as well as the entity's mission and business strategies, can affect the design of information systems and related security controls.
- The complexity of the entity's IT operations, including the extent to which external parties perform IT operations, including information security and privacy functions, on behalf of the entity, can result in higher inherent risk.
- Custom-developed software programs may have higher inherent risk than commercial off-the-shelf products that have been thoroughly tested and are in general commercial use. Conversely, commercial off-the-shelf products may expose the entity to known and newly discovered software and firmware flaws that may enable malicious activity.
- The structure of the entity's networks and the configuration of network components affect the access paths into and out of the information systems relevant to the significant business processes. For example, factors increasing inherent risk include a significant number of internet access points that are not centrally controlled; networks that are not segmented to protect sensitive information and information systems; and a lack of tools and software that enhance network security, such as intrusion detection and prevention systems.
- Highly decentralized information systems, particularly web applications, add complexity and increase potential vulnerabilities.

230.06 The auditor may obtain an understanding of inherent risk factors related to the entity's IT environment through inquiries of appropriate personnel and the inspection of relevant reports and other documents.

## 240 Understand the Entity's Information Security Management Program

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

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

240.02 GAO's *Standards for Internal Control in the Federal Government* (Green Book) defines the principles for the five components of internal control related to the objectives that an entity strives to achieve.[38] The five components follow.

- Control environment. The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives.
- Entity risk assessment.[39] The identification and analysis of risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.
- Information and communication. The quality information management and other personnel communicate and use to support the internal control system.
- Monitoring. Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.
- Control activities. The actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels.

240.03 The entity's information security management program addresses relevant principles and attributes within each component of internal control necessary to achieve operational objectives related to information security (confidentiality, integrity, and

[38]GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 2025). The Green Book broadly classifies these objectives into three categories: operations, reporting, and compliance. Operations addresses the effectiveness and efficiency of operations. Reporting addresses the reliability of reporting for internal and external use. Compliance addresses compliance with applicable laws and regulations.
[39]Although the Green Book uses "risk assessment," FISCAM uses "entity risk assessment" to distinguish between the entity's risk assessment and the auditor's risk assessment.

availability) and privacy, which support the achievement of operational objectives related to information processing (completeness, accuracy, and validity).

240.04 The FISCAM Framework for Security Management (section 530) aligns with the Green Book principles and attributes for the control environment, entity risk assessment, information and communication, and monitoring components of internal control associated with the IS controls assessment. The other control categories of the FISCAM Framework (sections 520, 540, 550, 560, and 570) align with the Green Book principles and attributes for the control activities component.

240.05 The auditor should obtain an understanding of the entity's information security management program. By doing so, the auditor gains a preliminary understanding of how the entity identifies risks relevant to information technology and how it responds to them. This understanding provides the basis for the auditor's preliminary assessment of IS control risk. See section 260 for further discussion on assessing IS control risk on a preliminary basis.

240.06 Additionally, the auditor obtains an understanding of the entity's information security management program sufficient to assess the design and implementation of the control environment, entity risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment. In obtaining an understanding of the entity's information security management program, the auditor considers whether management demonstrates a commitment to integrity and ethical values, including whether there is an appropriate tone at the top. The auditor also considers whether management obtains, generates, and uses relevant, quality information to support the achievement of the entity's objectives related to information security (confidentiality, integrity, and availability), privacy, and information processing (completeness, accuracy, and validity).

240.07 The auditor should use the FISCAM Framework for Security Management to obtain an understanding of the entity's information security management program. The FISCAM Framework for Security Management presents critical elements, control objectives, illustrative controls, and audit procedures for security management general controls. Table 1 is an excerpt from the framework and presents the critical elements and control objectives relevant to an entity's information security management program.

240.08 For federal financial audits, FAM 260, Understand the Entity's Internal Control, requires the auditor to understand and evaluate the design and implementation of the five components of internal control relevant to the preparation of the financial statements. The entity's use of information technology affects the manner in which the information relevant to the preparation of the financial statements is processed, stored, and communicated. Therefore, it affects the manner in which the entity's internal control over financial reporting is designed and implemented. When evaluating the design of the five components of internal control and determining whether each has been implemented, the auditor obtains an understanding of the entity's information security management program to consider the effect of information technology on internal control.

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

| Critical elements | Control objectives |
|---|---|
| SM.01 Management establishes organizational structures, assigns and communicates responsibilities, and develops plans and processes to implement an information security management program for achieving the entity's information security and privacy objectives. | SM.01.01 Organizational structures are established to enable the entity to plan, execute, control, and assess the information security and privacy functions. |
| | SM.01.02 Responsibilities are assigned to senior management positions within the information security and privacy functions. |
| | SM.01.03 Planning documentation related to the entity's information security management program is developed and maintained. |
| | SM.01.04 System development life cycle processes that incorporate information security and privacy considerations are established. |
| | SM.01.05 An incident response program is established. |
| | SM.01.06 System-level and entity-level processes for implementing and operating the entity's information security management program are developed and maintained. |
| SM.02 Management demonstrates a commitment to recruit, develop, and retain individuals who are competent and suitable for their information security and privacy positions. | SM.02.01 Expectations of competence and suitability for key information security and privacy roles are established and communicated. |
| | SM.02.02 Screening activities are completed, and access agreements are signed prior to access authorization. |
| | SM.02.03 Information security and privacy training programs and other mechanisms are established to communicate responsibilities and expected behavior for information and information system usage. |
| | SM.02.04 Training activities are documented, monitored, retained, and evaluated. |
| | SM.02.05 Transfer and termination activities are completed on a timely basis. |
| SM.03 Management holds individuals and external parties accountable for | SM.03.01 Information security and privacy policies and procedures are enforced. |

| Critical elements | Control objectives |
|---|---|
| their internal control responsibilities related to the entity's information security management program. | SM.03.02 External parties are held accountable for their assigned internal control responsibilities related to the entity's information security and privacy objectives. |
| | SM.03.03 Complementary user-entity controls related to external parties are identified, implemented, and operating effectively. |
| SM.04 Management identifies, analyzes, and responds to risks, including those related to fraud and improper payments, 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 mitigate risks to achieving the entity's information security and privacy objectives to acceptable levels. | SM.05.01 Information security and privacy policies and procedures are developed and implemented. |
| | SM.05.02 Information systems are authorized to operate. |
| SM.06 Management establishes and performs monitoring activities to evaluate the effectiveness of the entity's information security management program. | SM.06.01 The effectiveness of information security and privacy controls is continually and periodically assessed. |
| SM.07 Management remediates identified internal control deficiencies related to the entity's information security management program on a timely basis. | SM.07.01 Information security and privacy control deficiencies and vulnerabilities are reported, evaluated, and remediated on a timely basis. |

Source: GAO. | GAO-26-108633

240.09 To effectively use the FISCAM Framework for Security Management to obtain an understanding of the entity's information security management program, the auditor considers the critical elements and control objectives in the context of the areas of audit interest. Specifically, the auditor considers the extent to which general controls that the entity designed and implemented to achieve specific security management general control objectives are likely to support the effective design, implementation, and operation of general controls relevant to logical and physical access, segregation of duties, configuration management, and contingency planning for the areas of audit interest. For example, security management general controls that the entity designed and implemented to continually and periodically assess the effectiveness of information security and privacy controls are likely to support the effectiveness of other general controls for the areas of audit interest. See section 250 for further discussion on defining the scope of the IS controls assessment, including

identifying areas of audit interest. See also appendix 600C, FISCAM Security Management Questionnaire.

240.10 The auditor may use different audit procedures (inquiry, observation, and inspection) to obtain an understanding of the entity's information security management program.

## 250 Define the Scope of the IS Controls Assessment

250.01 The process for defining the scope of the IS controls assessment is iterative and continues throughout the planning phase. Identifying and obtaining an understanding of the significant business processes, business process controls, and areas of audit interest enable the auditor to begin defining the scope of the IS controls assessment. This allows the auditor to focus efforts on those areas that are necessary to achieving the engagement objectives, thereby reducing or eliminating work associated with other areas.

250.02 Business processes are the primary means through which the entity achieves its operating, reporting, and compliance objectives. Business processes transform inputs into outputs through a series of transactions or activities.[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, acquisitions and procurement, property management, or security). Significant business processes are those that are significant to the engagement objectives. For example, when evaluating the condition of contracting activities performed under an acquisition and procurement program, the engagement team may identify several supporting business processes—acquisition planning, contract development, contract award, contract execution, contract modifications, and contract closeout—that contribute to the condition of the program. Throughout this manual, references to significant business processes may include those the entity performs and those that external parties, including service organizations, contractors, and others, perform on behalf of the entity.

250.03 Business process controls are the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions; activities across business processes; and events between business process applications, their components, and other systems. Business process controls include direct general controls that support information processing objectives (completeness, accuracy, and validity). See section 120 for additional discussion.

250.04 Areas of audit interest are a subset of the entity's information systems that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. For example, at the business process level, areas of audit interest may include business process applications, process automation software, system interfaces, data management systems, specific data files, and system-generated reports. At the system level, areas of audit interest may include operating systems, access control software, and hardware devices used for information processing, data storage, and network communications.

250.05 For federal financial audits, FAM requires the auditor to identify significant business process applications and significant manual processes, assess inherent risk, and document control activities that address such risks. Specifically,

[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.

- FAM 235, Identify Material Line Items, Accounts, Note Disclosures, and Classes of Transactions; Applicable Assertions; Significant Business Process Applications; and Significant Manual Processes, requires the auditor to identify the significant business process applications and significant manual processes for material line items, accounts, note disclosures, and classes of transactions. Identifying and understanding these IT applications and manual processes helps the auditor to understand the flow of transactions, identify the likely sources of potential misstatements and the controls designed to address them, and design control and substantive tests.
- FAM 260, Understand the Entity's Internal Control, requires the auditor to obtain an understanding of the significant business process applications and significant manual processes, the resources to be used in these IT applications and manual processes, and the policies that define (among other things) how information flows through the entity's business processes.
- FAM 265, Identify Risks of Material Misstatement and Assess Inherent Risk, requires the auditor to prepare a line item risk analysis (LIRA) form that documents (among other things) the auditor's assessment of inherent risk for identified risks of material misstatement at the assertion level for material line items, accounts, note disclosures, and classes of transactions. Completing this assessment helps the auditor determine the likelihood and magnitude of misstatement before consideration of any related control activities. The auditor's inherent risk assessment incorporates the inherent risk factors identified by the auditor, including those related to the nature of the entity's IT environment, as applicable.
- FAM 330, Identify Control Objectives, FAM 340, Identify and Understand Control Activities, and FAM 350, Determine the Nature, Timing, and Extent of Control Tests, require the auditor to prepare a specific control evaluation (SCE) worksheet that documents (among other things) the control objectives and control activities that address identified risks of material misstatement at the assertion level related to material line items, accounts, note disclosures, and classes of transactions. The control activities included on an SCE worksheet comprise the manual and IS controls the auditor plans to test to determine whether the stated control objectives, which incorporate the information processing objectives of completeness, accuracy, and validity, are achieved. IS controls listed on an SCE worksheet are generally user and application controls. Additionally, the business process applications and other information systems supporting the IS controls listed on an SCE worksheet are areas of audit interest in the context of an IS controls assessment. The auditor may use the FISCAM Framework for Business Process Controls to facilitate identifying IS control objectives and IS controls for the significant business process applications. Instructions for completing the LIRA form and SCE worksheet are included in FAM 395H, Line Item Risk Analysis Form, and FAM 395G, Specific Control Evaluation Worksheet, respectively.
- FAM 360, Perform Control Tests, requires the auditor to assess the effectiveness of (1) IS controls included in the SCE worksheet (generally user and application controls) and (2) other IS controls on which the effectiveness of each IS control in the SCE worksheet depends, including

- other relevant application controls upon which the control depends
- direct general controls that directly support the effective operation of IS controls included in the SCE worksheet and
- indirect general controls that maintain a suitable environment to support the effective operation of user, application, and direct general controls.

For example, if the IS control is a user control involving the review of a system-generated exception report, the auditor would assess the

- application controls involved in the production of the exception report (e.g., configurable controls establishing thresholds for detecting exceptions);
- direct general controls over the production of the exception report (e.g., access and configuration management controls protecting the exception report's program code from unauthorized changes); and
- indirect general controls over the business process application that produces the exception report (e.g., system-level controls for managing configuration settings for the operating system).

## Identify and Understand Significant Business Processes

250.06 The auditor should identify business processes that are significant to the engagement objectives. The auditor uses professional judgment in determining which business processes are significant.

250.07 The auditor should obtain an understanding of the significant business processes by performing walk-throughs or alternative audit procedures. **A walk-through** is a combination of audit procedures (i.e., observation, inspection, and inquiry) that enable the auditor to understand the steps and resources involved in a significant business process from beginning to end, including the information systems used and the design and implementation of the IS controls involved.

250.08 Walk-throughs may be performed during the planning and testing phases of an engagement. During the planning phase, walk-throughs are primarily performed to obtain an understanding of the significant business processes by tracing one or more transactions, activities, or events through all processing. During the testing phase, walk-throughs are often performed as control tests involving a combination of observation, inquiry, and inspection (which may include reperformance) using nonstatistical selection. Alternative audit procedures generally include inspecting relevant documentation and inquiring of appropriate personnel without directly observing the process and controls.

250.09 When performing walk-throughs of the significant business processes during the planning phase, the auditor may

- observe appropriate personnel performing their assigned duties;
- inquire of appropriate personnel to obtain an understanding of information system processing that cannot be observed directly; and

- inspect business process documentation, such as process narratives, flowcharts, standard operation procedures, desktop guides, and user manuals.

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

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

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

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

250.12 For example, the auditor may determine that the procurement of goods and services is significant to the engagement objectives. The auditor may identify the business activities—processing purchase orders, receiving goods and services, recording accounts payable, and disbursing payments—related to the procurement process. The auditor obtains an understanding of each of the business units and activities involved in the procurement process in sufficient detail to document how purchase transactions are initiated; transaction data flows between business units; information systems are used for information processing; data are input, processed, and output;

system-generated reports are used; and services performed by external parties are incorporated into the procurement process.

250.13 The auditor should inspect available system documentation that explains the processing and flow of data within the business process applications, as well as system interfaces to other information systems and the design of the underlying data management systems. Examples include end user guides, system administration guides, system interface documentation, data flow diagrams, and workflow diagrams.

250.14 The auditor should prepare a written description of each significant business process, including the information systems used. See section 280 for further discussion of documenting an understanding of significant business processes.

## Identify and Understand Business Process Controls Using the FISCAM Framework

250.15 The auditor should identify and obtain an understanding of the business process controls designed to achieve information processing objectives—completeness, accuracy, and validity—based on the auditor's understanding of the significant business processes. This understanding is primarily obtained through walk-throughs of the significant business processes and the inspection of system documentation for the business process applications, system interfaces, and data management systems used within such processes (paragraphs 250.06 through 250.14).

250.16 The auditor should use the FISCAM Framework for Business Process Controls (section 520) to identify relevant business process control objectives and to facilitate identifying controls that the entity designed to achieve those objectives. Relevant control objectives, as used in FISCAM, are those that are necessary to achieve the engagement objectives. For each business process, the auditor identifies

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

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

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

| Critical elements | Control objectives |
|---|---|
| BP.01 Management designs and implements user and application controls to reasonably assure that data | BP.01.01 Data are properly prepared and approved for input into the information system on a timely basis. |
| | BP.01.02 Data input rules detect erroneous data values before information system processing. |

| Critical elements | Control objectives |
|---|---|
| input into the information system are complete, accurate, and valid. | BP.01.03 Data input errors are researched and resolved on a timely basis. |
| BP.02 Management designs and implements user and application controls to reasonably assure that data processing by the information system is complete, accurate, and valid. | BP.02.01 Data processing errors are identified on a timely basis. |
| | BP.02.02 Data processing errors are researched and resolved on a timely basis. |
| BP.03 Management designs and implements user and application controls to reasonably assure that output data are complete, accurate, and valid. | BP.03.01 Data are approved for output. |
| | BP.03.02 Output data errors are identified on a timely basis. |
| | BP.03.03 Output data errors are researched and resolved on a timely basis. |
| BP.04 Management designs and implements general controls to reasonably assure that business process applications are properly managed to achieve information processing objectives. | BP.04.01 Business process application roles and responsibilities are defined and assigned to appropriate personnel. |
| | BP.04.02 Policies and procedures for administering and using business process applications are developed and implemented. |
| | BP.04.03 Business process applications are designed to facilitate the performance of business processes and reasonably assure the completeness, accuracy, and validity of transactions and data. |
| | BP.04.04 Business process applications are designed to facilitate the protection of personally identifiable information. |
| | BP.04.05 The effectiveness of application controls and the adequacy of automated business processes that business process applications perform are periodically assessed. |
| | BP.04.06 Access to business process applications is appropriately controlled. |
| | BP.04.07 Modifications to business process applications and changes to configurable controls within application software are appropriately controlled. |
| BP.05 Management designs and implements general controls to reasonably assure that system interfaces | BP.05.01 System interface roles and responsibilities are defined and assigned to appropriate personnel. |
| | BP.05.02 Policies and procedures for managing system interfaces are developed and implemented. |

| Critical elements | Control objectives |
|---|---|
| are properly managed to achieve information processing objectives. | BP.05.03 System interfaces are designed to exchange information between systems and reasonably assure the completeness, accuracy, and validity of the exchange. |
| | BP.05.04 System interface errors are identified on a timely basis. |
| | BP.05.05 System interface errors are researched and resolved on a timely basis. |
| | BP.05.06 Access to system interface data and user-defined processing of data are appropriately controlled. |
| | BP.05.07 Modifications to system interfaces are appropriately controlled. |
| BP.06 Management designs and implements general controls to reasonably assure that data management systems are properly managed to achieve information processing objectives. | BP.06.01 Data management system roles and responsibilities are defined and assigned to appropriate personnel. |
| | BP.06.02 Policies and procedures for managing data management systems are developed and implemented. |
| | BP.06.03 Data management systems are designed to organize, maintain, and control access to application data to reasonably assure the completeness, accuracy, and validity of transactions and data. |
| | BP.06.04 The completeness, accuracy, and validity of data maintained in data management systems are periodically assessed. |
| | BP.06.05 Access to data management systems is appropriately controlled. |
| | BP.06.06 Modifications to data management systems and data maintained in those systems are appropriately controlled. |

Source: GAO. | GAO-26-108633

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

- If the auditor has identified a data file, which is a collection of records stored in computerized form, as a potential area of audit interest, the auditor would use the framework and
    - the auditor's understanding of the entity's significant business processes to identify the (1) user and application control objectives that, if achieved, would provide reasonable assurance of the completeness, accuracy, and validity of the data file and (2) user and application controls designed by the entity to achieve those objectives and

  - the auditor's understanding of the relevant business process applications, system interfaces, and data management systems to identify the (1) general control objectives that, if achieved, would directly support the effective operation of user and application controls and (2) direct general controls that the entity designed to achieve those objectives.

- If the auditor has identified a business process application as a potential area of audit interest, the auditor would use the framework and
  - the auditor's understanding of the entity's significant business processes to identify the (1) user and application control objectives supported by the business process application and (2) user and application controls designed by the entity to achieve those objectives and
  - the auditor's understanding of the business process application to identify the (1) general control objectives that, if achieved, would directly support the effective operation of user and application controls and (2) direct general controls that the entity designed to achieve those objectives.

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

- the nature and significance of the transactions that the external party processes and
- the degree of interaction between the entity's internal control and the external party controls.[41]

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

250.21 See section 320 for further discussion on identifying relevant IS controls for testing.

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

## Identify and Understand Areas of Audit Interest

250.22 The auditor should identify areas of audit interest at the business process and system levels. Identifying areas of audit interest is an iterative process that primarily occurs during the planning phase.

250.23 The auditor identifies potential areas of audit interest at the business process level based on the auditor's understanding of the information resources used in the significant businesses processes (e.g., business process applications). This understanding is primarily obtained through walk-throughs of the significant business processes (see paragraphs 250.07 through 250.10). For example, during a walk-through of a significant business process, the auditor may observe personnel using reports from an inventory management application to validate inventory counts. Upon inquiry of personnel, the auditor may determine that the volume of transactions processed by the inventory management application is significant. The auditor identifies the inventory management application and its database component as areas of audit interest because the volume of transactions the inventory management application processes and the database component stores is significant to the engagement objectives.

250.24 The auditor identifies potential areas of audit interest at the system level based on the auditor's understanding of each of the potential areas of audit interest at the business process level. This understanding is primarily obtained through the inspection of system documentation for the business process applications. In obtaining an understanding, the auditor considers the

- individuals who fulfill system roles and responsibilities,
- authorization boundary,
- information system components,
- security categorization,
- impact level,
- control dependencies,
- system interconnections,
- security and privacy requirements,
- controls selected to satisfy those requirements, and
- operational environment. [42]

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

- the presence or number of application controls incorporated directly into the business process application,

[42]An information system authorization boundary comprises all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems connected to the information system. Business process applications may be separately authorized or included within a larger information system authorization boundary.

- the dollar value of the transactions processed,
- the volume of transactions processed,
- the sensitivity or significance of the information processed, or
- the existence of an access path to another system that contains sensitive or significant information.

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

- The auditor's understanding of an information system's authorization boundary may assist the auditor in identifying areas of audit interest at the business process level that are excluded from but connected to an information system used in the significant businesses process. For example, after inspecting system documentation for a payroll system identified within a significant business process, the auditor may determine that the payroll system relies on data from a timekeeping system that is not within the same authorization boundary. Because the timekeeping system is a separate information system that may have different security and privacy requirements and controls that have a direct effect on information processing objectives (completeness, accuracy, and validity) relevant to the significant business process, the auditor may identify the timekeeping system as an area of audit interest at the business process level.
- The auditor's understanding of an information system's components and system interconnections may assist the auditor in identifying areas of audit interest at the business process level that may not be evident when observing a significant businesses process. For example, the auditor may not be able to observe the use of system interface software that transfers data between system components during a walk-through of a significant business process.
- The auditor's understanding of the controls that management selected for the information system used in a significant business process may assist the auditor in identifying areas of audit interest at the system level from which the information system inherited certain controls. **Control inheritance** occurs when an information system or information system component receives protection from security or privacy controls that are developed, implemented, assessed, authorized, and monitored by personnel other than those responsible for the information system or information system component. For example, the mechanisms for enforcing logical access control for a business process application may be developed, implemented, assessed, authorized, and monitored as part of a separate information system.
- The auditor's understanding of the operational environment may assist the auditor in identifying areas of audit interest at the system level from which various information systems inherited certain controls used in the significant business processes. For example, in identifying related access paths through the inspection of network and information system diagrams, the auditor may identify areas of audit interest that provide inherited controls the entity employs (or external parties employ on behalf of the entity) to protect the access paths and control the flow of information. In obtaining an understanding of related access paths, the auditor considers

- internet presence and any outward-facing, publicly accessible servers, such as web and email services;
- network segmentation and the location of firewalls, routers, and switches;
- intrusion detection and prevention systems;
- file transfer systems and connections to external parties, as well as inter- and intra-entity connections;
- network management systems;
- wireless connections;
- remote access; and
- whether the use of mobile devices or personally owned systems, components, and devices is permitted.

## 260 Assess IS Control Risk on a Preliminary Basis

260.01 When performing the IS controls assessment, the auditor assesses IS control risk to determine the nature, timing, and extent of IS control tests. **IS control risk** is the likelihood that conditions or events related to the areas of audit interest (1) could significantly affect the entity's ability to achieve its information processing objectives (completeness, accuracy, and validity), and (2) will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls. IS control risk is a function of the design, implementation, and operating effectiveness of the entity's IS controls relevant to the engagement objectives. Some IS control risk will always exist because of the inherent limitations of internal control.

260.02 The auditor's preliminary assessment of IS control risk for each area of audit interest enables the auditor to establish an appropriate basis for planning the IS controls assessment to reduce audit risk to an acceptably low level, as required by GAGAS (2018). While the auditor assesses IS control risk throughout the engagement, risk assessment activities are concentrated in the planning phase.

260.03 In assessing IS control risk on a preliminary basis, the auditor considers the extent to which IS controls will adequately mitigate risk factors to achieve relevant control objectives. The auditor considers inherent risk factors related to the entity's IT environment (section 230), IS control risk factors based on an understanding of the entity's information security management program, and fraud risk factors. The auditor also considers information gathered to evaluate whether the entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant to the engagement objectives (section 230).

260.04 The auditor uses professional judgment in determining (1) the extent of audit procedures necessary to identify IS control risk factors—conditions or events that affect the susceptibility of the area of audit interest to information system processing errors due to ineffective general controls—and (2) the effect of such risk factors on the auditor's preliminary assessment of IS control risk. The auditor may use the results of management's risk assessments, along with other information collected during the planning phase, to arrive at a preliminary assessment of IS control risk. However, the auditor is not required or expected to reperform management's risk assessments when using the results of such to inform the auditor's assessment of IS control risk. The auditor may also consult with an IT specialist when assessing IS control risk.

260.05 The auditor prepares a written preliminary assessment of IS control risk that identifies the risk factors that inform the auditor's assessed level of IS control risk for each area of audit interest. See section 280 for further discussion of documenting the preliminary assessment of IS control risk.

260.06 For federal financial audits, FAM 340, Identify and Understand Control Activities, requires the auditor to identify the risks arising from the use of information technology and the entity's general controls that address such risks. Risks arising from the use of information technology are the conditions or events that affect the susceptibility of IS controls (i.e., application and user controls identified as relevant control activities in the SCE worksheet) to ineffective design or operation due to ineffective general controls at the system or entity level. In the context of FISCAM, such risks are referred to as IS control risk factors. Additionally, FAM 370, Assess

Internal Control on a Preliminary Basis, requires the auditor to perform an assessment of control risk. In the context of a federal financial audit, the auditor's preliminary assessment of IS control risk is incorporated into the financial auditor's overall assessment of control risk as discussed in FAM 370.

## Identify IS Control Risk Factors Related to Areas of Audit Interest

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

- SM.01 Management establishes organizational structures; assigns and communicates responsibilities; and develops plans and processes to implement an information security management program for achieving the entity's information security and privacy objectives. IS control risk factors include conditions or events related to
    - the placement of the chief information officer, chief risk officer, information security officer, and privacy officer positions within the organizational structure;
    - the nature of the IT organizational structure (i.e., a centralized or decentralized structure);
    - the extent to which the IT organizational structure is designed to support the segregation of incompatible duties;
    - the extent to which management demonstrates an appropriate level of interest in and awareness of information security and privacy functions, including those functions that external parties perform;
    - the quality of the entity-level information security management program and privacy management program plans and whether such plans align with the entity's strategic plan;
    - the extent to which the entity's system development life cycle processes adequately address information security and privacy considerations;
    - the extent to which the entity has established an adequate incident response program;
    - the quality of the entity's system security and privacy plans for the areas of audit interest;
    - the quality of the entity's information system contingency plans for the areas of audit interest; and

- the extent to which information security and privacy responsibilities—particularly those pertaining to the areas of audit interest—are clearly defined and appropriately assigned to personnel with the authority and expertise needed to fulfill them.

- SM.02 Management demonstrates a commitment to recruit, develop, and retain individuals who are competent and suitable for their information security and privacy positions. IS control risk factors include conditions or events related to
  - turnover of key personnel involved in IT operations, including turnover that could affect the areas of audit interest (i.e., high or low turnover);
  - the number of personnel with appropriate knowledge, skills, and abilities relative to the size and complexity of the entity's IT operations (i.e., adequate or inadequate number);
  - the adequacy of the security and privacy workforce development and improvement program; and
  - the appropriateness of the information security and privacy training programs.
- SM.03 Management holds individuals and external parties accountable for their internal control responsibilities related to the entity's information security management program. IS control risk factors include conditions or events related to
  - the extent to which information security and privacy policies are enforced;
  - the extent to which the terms and conditions for the protection of controlled unclassified information processed, stored, or transmitted on external systems are clearly documented (e.g., in a memorandum of understanding or service agreement) and understood by entity personnel responsible for enforcement;[43]
  - the extent to which external parties performing IT operations, including information security and privacy functions, on behalf of the entity are held accountable for their assigned internal control responsibilities; and
  - the adequacy of the entity's processes for assessing the effectiveness of information security and privacy controls that external parties

[43]Executive Order No.13556, *Controlled Unclassified Information* (Nov. 4, 2010) (reprinted in 75 Fed. Reg. 68,675 (Nov. 9, 2010), establishes an open and uniform program for managing unclassified information requiring safeguarding or dissemination controls. The National Archives and Records Administration (NARA), which the order directed to implement and oversee the controlled unclassified information (CUI) program, issued a final rule on September 14, 2016, that became effective on November 14, 2016. See 81 Fed. Reg. 63,324 (Sept. 14, 2016), which is codified at 32 C.F.R. part 2002. NARA's CUI regulations define CUI as information the that the federal government creates or possesses, or that an entity creates or possesses for or on behalf of the federal government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. According to NARA's regulations, CUI information may be designated as basic or specified depending on whether specific handling or dissemination controls are required by specific authorizing law, regulation, or government-wide policy. See 32 C.F.R. § 2002.4.

designed, implemented, and operated—particularly those pertaining to the areas of audit interest.

- SM.04 Management identifies, analyzes, and responds to risks, including those related to fraud and improper payments, and significant changes related to the entity's information security management program. IS control risk factors include conditions or events related to
    - the quality of the entity-level risk management strategy for information security and privacy risks;
    - the quality of the entity-level continuous monitoring strategy;
    - the extent to which the entity appropriately considers inherent and control risks, including fraud risk, related to information systems—particularly those information systems identified as areas of audit interest;
    - the extent to which the entity properly identifies, analyzes, and responds to risks arising from (1) internal sources, such as the ability to retain key personnel involved in IT operations or the adequacy of system backups to facilitate the recovery and reconstitution of information systems following a system disruption, and (2) external sources, such as vulnerabilities, flaws, and threats;
    - the extent to which the entity incorporates audit recommendations or identified internal control deficiencies into its risk management processes;
    - the extent to which the entity appropriately modifies information systems—particularly those identified as areas of audit interest—in response to changing conditions on a timely basis; and
    - the extent to which management is involved in major system development or modification decisions.
- SM.05 Management designs and implements policies and procedures to mitigate risks to achieving the entity's information security and privacy objectives to acceptable levels. IS control risk factors include conditions or events related to
    - the quality of the entity's policies and procedures for managing and using business process applications, system interfaces, and data management systems, as well as information security and privacy policies and procedures implemented at the system and entity levels;
    - the extent to which the entity's policies and procedures are clearly documented and understood by entity personnel responsible for enforcement;
    - the extent to which the entity's policies and procedures address appropriate segregation of duties for the entity's IT operations;
    - the complexity of the entity's processes for authorizing information systems and common controls for inheritance by information systems, including the extent to which the entity's authorization processes rely

on information from external parties, such as third-party assessors; and

- the quality of the entity's authorization packages—particularly for those information systems identified as areas of audit interest.

- SM.06 Management establishes and performs monitoring activities to evaluate the effectiveness of the entity's information security management program. IS control risk factors include conditions or events related to
  - the quality of the entity's system-level continuous monitoring strategies and the extent to which the entity's system-level continuous monitoring activities are implemented in accordance with such strategies;
  - the quality of the entity's information security and privacy control assessments for the areas of audit interest;
  - the quality of the entity's information system contingency plan test results for the areas of audit interest;
  - the extent to which the entity appropriately considers whether reliable system-generated information is used for key operating decisions;
  - the extent to which system audit trails are useful as basis for monitoring system and user activities;
  - the extent to which the entity monitors the effectiveness of segregation of duties controls, including alternative IS controls implemented to mitigate risks resulting from incompatible duties that cannot be segregated; and
  - the extent to which the entity adequately identifies and responds to unusual or exceptional conditions.
- SM.07 Management remediates identified internal control deficiencies related to the entity's information security management program on a timely basis. IS control risk factors include conditions or events related to
  - the extent to which the entity timely and appropriately responds to findings, recommendations, or concerns related to its information system controls;
  - the adequacy of the entity's processes for developing, documenting, and periodically reviewing and updating plans of actions and milestones;
  - the extent to which identified control deficiencies and vulnerabilities are analyzed in relation to the entire entity and appropriate corrective actions are applied entity-wide; and
  - the extent to which remediation tasks and milestones are accomplished by scheduled completion dates.

## Identify Fraud Risk Factors

260.08 The engagement team members should discuss fraud risk factors and assess the risk of fraud occurring that is significant to the engagement objectives. It is important that all members of the engagement team are aware of the fraud risk factors identified, including any specific fraud risks or suspected fraud associated with the information technology that the entity employs.

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

260.10 The following control risk factors related to the information technology that the entity employs may increase the risk of fraud:

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

260.11 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.

260.12 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.

260.13 The auditor's training, experience, and understanding of the entity or program being audited may provide a basis for recognizing that some acts coming to the auditor's attention may indicate fraud. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond the auditor's professional expertise and responsibility.

## Assess IS Control Risk on a Preliminary Basis

260.14 The auditor should involve senior members of the engagement team in the assessment of IS control risk. The auditor should preliminarily assess the level of IS control risk for each area of audit interest based on the auditor's understanding of inherent risk factors related to the IT environment, IS control risk factors, and fraud risk factors, as well as any other factors or compensating controls that may mitigate

the effects of identified risk factors. In assessing IS control risk on a preliminary basis, the auditor also considers information gathered to evaluate whether the entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant to the engagement objectives. For each area of audit interest, the auditor assesses preliminary IS control risk at one of three levels:

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

260.15 The auditor's assessed level of IS control risk for each area of audit interest differs from management's security categorizations of information systems and information processed through, stored on, and transmitted by such systems. Security categorization of federal information systems and information, as required by Federal Information Processing Standard (FIPS) 199, is an important first step in the entity's information security and privacy risk management process.[44] Though considered in the context of the same information security objectives of confidentiality, integrity, and availability, the auditor's assessment of IS control risk for each area of audit interest need not match management's security categorizations for the corresponding information systems.

260.16 The auditor should involve senior members of the engagement team in determining the nature, timing, and extent of IS control tests in response to assessed risks. As IS control risk increases, audit risk increases. However, audit risk can be reduced by taking actions such as adding specialists, additional reviewers, and other resources to conduct the engagement, as well as changing the approach to obtain additional evidence, higher-quality evidence, or alternative forms of corroborating evidence.

[44]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

270.01 When planning the IS controls assessment, the auditor identifies general control objectives for each area of audit interest. Such control objectives are a subset of those necessary to achieve the engagement objectives (i.e., relevant control objectives). Achieving relevant general control objectives for areas of audit interest at the system and entity levels maintains a suitable environment to support the effective operation of user, application, and direct general controls (section 250). The engagement objectives and the auditor's understanding of the entity's IT environment, information security management program, significant business processes, business process controls, and areas of audit interest provide the basis for identifying such control objectives.

270.02 The auditor should identify relevant general control objectives for each area of audit interest at the system and entity levels. When identifying such relevant general control objectives, the auditor considers the general control objectives related to the five general control categories: security management, logical and physical access, segregation of duties, configuration management, and contingency planning. Depending on the engagement's objectives, the auditor may determine that it is not necessary to identify relevant general control objectives from all five general control categories.

### Security Management

270.03 The auditor should use the FISCAM Framework for Security Management (section 530) to identify security management general control objectives relevant to each area of audit interest. When identifying relevant security management control objectives, the auditor considers the preliminary level of IS control risk for each area of audit interest.

270.04 Regardless of whether the auditor identifies security management general control objectives as being relevant to the areas of audit interest, the auditor is required to obtain an understanding of the entity's information security management program sufficient to (1) assess the design and implementation of the entity's control environment, risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment and (2) plan the IS controls work necessary to achieve the engagement objectives.

270.05 See section 240 for further discussion on obtaining an understanding of the entity's information security management program. Section 240, table 1, is an excerpt from the FISCAM Framework for Security Management and presents the critical elements and associated control objectives.

### Access Controls (Logical and Physical Access)

270.06 The auditor should use the FISCAM Framework for Access Controls (section 540) to identify logical and physical access general control objectives relevant to each area of audit interest. Table 3 is an excerpt from the FISCAM Framework for Access Controls and presents the critical elements and associated control objectives.

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

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

Source: GAO. | GAO-26-108633

## Segregation of Duties

270.07 The auditor should use the FISCAM Framework for Segregation of Duties (section 550) to identify segregation of duties general control objectives relevant to each area of audit interest. Table 4 is an excerpt from the FISCAM Framework for Segregation of Duties and presents the critical elements and associated control objectives.

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

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

Source: GAO. | GAO-26-108633

## Configuration Management

270.08 The auditor should use the FISCAM Framework for Configuration Management (section 560) to identify configuration management general control objectives relevant to each area of audit interest. Table 5 is an excerpt from the FISCAM Framework for Configuration Management and presents the critical elements and associated control objectives.

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

| Critical elements | Control objectives |
|---|---|
| CM.01 Management designs and implements general controls to develop and maintain secure baseline configurations for information systems. | CM.01.01 Baseline configurations for information systems and system documentation for administrators and users are developed and maintained. |
| | CM.01.02 An inventory of information system components is developed and maintained. |
| | CM.01.03 Configuration items for information systems are identified and placed under configuration management. |
| | CM.01.04 Configuration settings are established and documented for configuration items. |
| CM.02 Management designs and implements general controls to manage changes to entity information systems and information system components. | CM.02.01 Planned changes to configuration items are formally authorized, analyzed, tested, and approved prior to implementation. |
| | CM.02.02 Emergency changes to configuration items are documented, analyzed, and reviewed. |
| | CM.02.03 Information systems and information system components are routinely monitored for deviations from |

| Critical elements | Control objectives |
|---|---|
| | established configuration settings and unauthorized changes. |
| | CM.02.04 Logical access controls relevant to configuration management are selected and employed based on risk. |
| CM.03 Management designs and implements general controls to protect information systems and information system components from vulnerabilities, flaws, and threats. | CM.03.01 Vulnerability monitoring is routinely conducted. |
| | CM.03.02 Critical updates and patches for information systems are implemented, and unsupported information system components are replaced on a timely basis. |
| | CM.03.03 Information systems and information system components are protected from spam and malicious code. |

Source: GAO. | GAO-26-108633

## Contingency Planning

270.09 The auditor should use the FISCAM Framework for Contingency Planning (section 570) to identify contingency planning general control objectives relevant to each area of audit interest. Table 6 is an excerpt from the FISCAM Framework for Contingency Planning and presents the critical elements and associated control objectives for contingency planning.

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

| Critical elements | Control objectives |
|---|---|
| CP.01 Management designs and implements general controls to achieve continuity of operations and prioritize the recovery and reconstitution of information systems that support critical or essential mission and business functions in the event of a system disruption, compromise, or failure. | CP.01.01 Criticality analyses are performed to prioritize mission and business functions and determine the criticality of information systems, information system components, and information system services. |
| | CP.01.02 Information system contingency plans and other organizational plans are established and implemented to continue critical or essential mission and business functions in the event of a system disruption, compromise, or failure, and to eventually restore the information system following a system disruption. |
| | CP.01.03 Information system users and other personnel are trained to fulfill their roles and responsibilities associated with the information system contingency plan in the event of a system disruption. |

| Critical elements | Control objectives |
|---|---|
| | CP.01.04 Information system contingency plans are periodically tested to determine their effectiveness and the entity's readiness to execute them. |
| CP.02 Management designs and implements general controls to prevent or minimize system disruption and potential damage to information resources and facilities due to natural disasters, structural failures, hostile attacks, or errors. | CP.02.01 Environmental controls are appropriately selected and employed based on risk. |
| | CP.02.02 Management has established alternate sites, services, and information security mechanisms to permit the timely resumption of operations supporting critical or essential mission and business functions in the event of a system disruption. |
| | CP.02.03 System backups are regularly conducted, and system media containing backup data and software are properly maintained to facilitate the recovery and reconstitution of information systems following a system disruption. |
| | CP.02.04 Maintenance of information system components is properly performed on a timely basis to prevent or minimize system disruption. |

Source: GAO. | GAO-26-108633

## 280 Prepare Planning Phase Documentation

280.01 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 Understanding of Significant Business Processes

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

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

For federal financial audits, the auditor documents the understanding of significant business processes applications (including information system processing) in cycle memorandums, or other equivalent narratives, and may prepare or obtain related flowcharts (FAM 320.13 and 320.15). FAM 390, Documentation (Internal Control Phase), provides details on preparing a cycle memorandum to document the understanding of significant business process applications.

### Auditor's Preliminary Assessment of IS Control Risk

280.03 The auditor should prepare a written preliminary assessment of IS control risk for each area of audit interest. As part of the auditor's preliminary assessment of IS control risk, the auditor documents determinations regarding preliminary IS control risk and the reasons for such determinations (e.g., the risk factors that informed the auditor's assessments). Risk factors include inherent risk factors related to the IT environment, IS control risk factors, and fraud risk factors. The auditor also documents other factors or compensating controls that may mitigate the effects of identified risk factors.

## Planning Memo and Audit Plan

280.04 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;
- key decisions related to the areas of audit interest;
- the identification of relevant user, application, and general control objectives for each area of audit interest, as applicable; and
- the auditor's basis for such scoping decisions, such as the auditor's understanding of the entity's information security management program and the auditor's preliminary assessment of IS control risk.

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

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

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

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

## FISCAM Assessment Completion Checklist

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

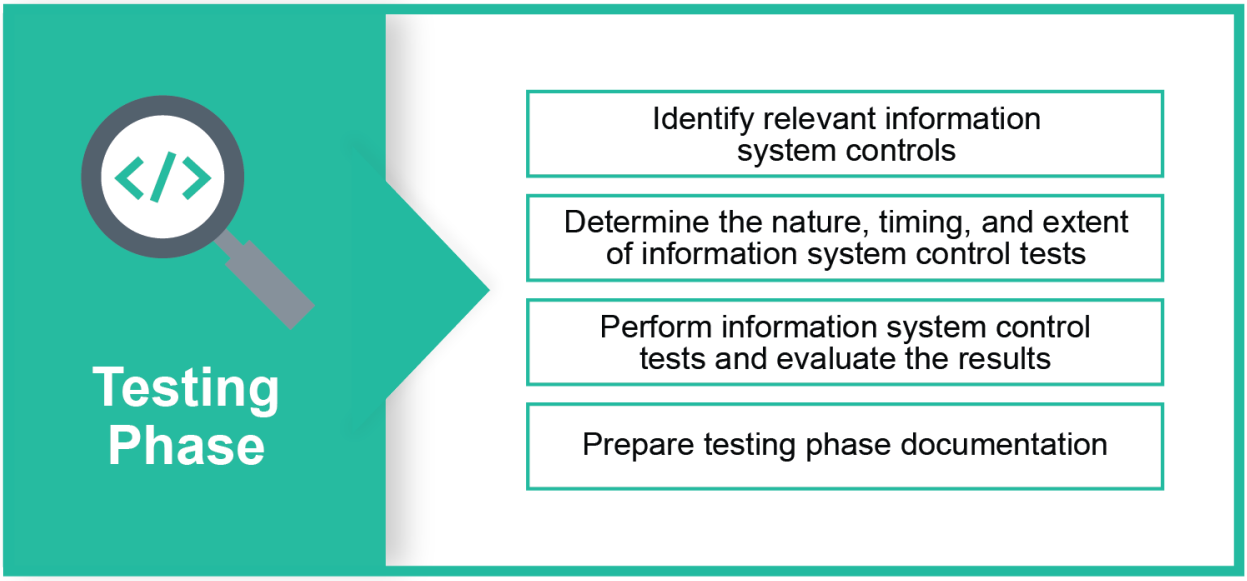
# SECTION 300

## Testing Phase

## 310 Overview of the Testing Phase

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

**Figure 7: Testing Phase Activities**




Source: GAO (data and icons). | GAO-26-108633

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

## 320 Identify Relevant IS Controls

320.01 When performing the IS controls assessment, the auditor identifies relevant IS controls—those user, application, and general controls that are suitably designed and necessary to achieve relevant control objectives and that the auditor plans to test for implementation and operating effectiveness. The auditor uses the FISCAM Framework as part of the process for identifying relevant IS controls. The illustrative controls presented in the FISCAM Framework are consistent with management requirements for information security and privacy control requirements presented in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*.[45] These illustrative controls are examples of IS controls that may achieve the control objectives and, as such, assist the auditor in identifying and obtaining an understanding of the IS controls that the entity designed to achieve the relevant control objectives for each area of audit interest.

320.02 The auditor should obtain a sufficient understanding of the design of the entity's IS controls that are likely to achieve the relevant control objectives for each area of audit interest, if implemented and operating effectively. The auditor primarily obtains this understanding through inquiries of management and personnel with knowledge of the IS controls as applied to the areas of audit interest, and the inspection of relevant documentation describing the design of such controls. The auditor may also observe personnel performing the IS controls. In determining whether such controls are suitably designed, the auditor considers the nature of the IS controls (i.e., the way they are applied) and the documentary evidence available to demonstrate the existence or performance of the controls.

320.03 Of the IS controls that are likely to achieve the relevant control objectives for each area of audit interest, the auditor should identify those controls that achieve the relevant control objectives and improve the efficiency of the auditor's IS control tests. Such IS controls are considered relevant IS controls in the context of an IS controls assessment and will be tested for implementation and operating effectiveness. When determining whether an IS control (or combination of IS controls) will achieve a control objective, the auditor considers the extent to which the IS control relates to the control objective. The more direct the relationship between the IS control and the control objective (as it pertains to the area of audit interest), the more effective the control may be in achieving the objective.

320.04 If there are several IS controls that are likely to be effective in achieving a control objective, the auditor considers

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

[45]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).

320.05 A control dependency exists when the effectiveness of a control depends on the effectiveness of other controls. When the auditor determines that the effective operation of a control depends on the effective operation of other controls, the auditor considers specific risks to the dependent control's effective operation and performs tests of the other controls to determine whether they are suitably designed, properly implemented, and operating effectively to address the specific risks identified. Determining if an IS control is effective often includes assessing the effectiveness of other controls upon which the effectiveness of the IS control depends. For example, the effectiveness of a configurable control within application software will depend on the design of the application control, as well as related logical access and configuration management general controls designed to prevent or detect unauthorized changes to the control. In this example, the auditor would test the application control, as well as the related logical access and configuration management controls, to arrive at a conclusion regarding the effectiveness of the application control.

320.06 Without effective general controls, user and application controls may be rendered ineffective depending on the extent of control dependencies. Consequently, if certain general controls upon which specific user and application controls depend are not likely to be effective, the auditor may forgo further testing of such controls. In such cases, the auditor develops appropriate findings and considers the effect of control risks arising from ineffective user, application, and general controls on the nature, timing, and extent of further audit procedures.

320.07 When selecting general controls for testing, the auditor considers the level (i.e., business process, system, and entity) at which such controls are applied and whether it is more efficient to test certain indirect general controls at the system or entity levels rather than direct general controls at the business process level, assuming they are equally effective. For example, if an entity-level general control for user identification and authentication is likely to achieve a control objective for the appropriate restriction of logical access for multiple areas of audit interest (whether at the business process level or system level), it may be more efficient to test the entity-level general control.

320.08 The auditor may implement a tiered approach to evaluating the effectiveness of IS controls, beginning with entity-level and system-level general controls, followed by business process-level general controls, and finishing with user and application controls. Such an approach may be efficient if the auditor has evidence that certain relevant general controls may not be effective and as a result, the auditor would forgo testing of user and application controls that depend on the effectiveness of those relevant general controls. However, for such an approach to be both efficient and effective, the auditor needs to have an adequate understanding of IS control dependencies (e.g., the extent to which the effectiveness of specific user and application controls depend on the effectiveness of certain general controls).

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

330.01 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 control objectives for each area of audit interest. Once the auditor has identified relevant IS controls (section 320), the auditor determines the nature, timing, and extent of IS control tests. Control tests are a means of obtaining evidence on the implementation and operating effectiveness of relevant IS controls.

330.02 The nature, timing, and extent of IS control tests will vary by IS control.

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

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

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

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

#### Nature of IS Control Tests

330.05 The auditor should determine the nature of IS control tests—observation, inquiry, or inspection (including reperformance)—to be performed for each relevant IS control. This determination is based on the auditor's understanding of the design of the IS control and the evidence available to demonstrate whether the control is properly implemented and operating effectively.

330.06 When determining the nature of IS control tests, the auditor considers the appropriateness—the measure of the quality of evidence that encompasses relevance, validity, and reliability—of the evidence available.

- Relevance refers to the extent to which evidence has a logical relationship with, and importance to, the issue being addressed.

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

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

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

- Observation. The auditor conducts observation tests by observing entity personnel performing IS controls in the normal course of their duties. Observation generally provides highly reliable evidence that a control is properly applied when the auditor is there to observe it. However, it provides no evidence that the control was in operation at any other time. Consequently, the auditor generally supplements observation tests with corroborative evidence obtained from other tests (such as inquiry and inspection) about the operation of controls at other times.
- Inquiry. The auditor conducts inquiry tests by making either oral or written inquiries of entity personnel involved in the application of specific IS controls to determine what they do or how they perform a specific IS control. Such inquiries are typically open ended. Testimonial evidence obtained from inquiry alone is not sufficient; thus, the auditor supplements inquiry with other types of control tests—observation or inspection (which may include reperformance). Combining inquiry with inspection or reperformance typically provides more assurance than inquiry combined only with observation. The reliability of evidence obtained from inquiry depends on various factors, including the following:
    - The competence, experience, knowledge, independence, and integrity of the person of whom the inquiry was made. The reliability of evidence is enhanced when the person possesses these attributes.
    - Whether the evidence is general or specific. Evidence that is specific is usually more reliable than evidence that is general.

- The extent of corroborative evidence obtained. Evidence obtained from several entity personnel is usually more reliable than evidence obtained from only one person.
- Whether the evidence was provided orally or in writing. Generally, evidence provided in writing is more reliable than evidence provided orally.

- Inspection. The auditor conducts inspection tests by examining documents and records for evidence (such as implemented configuration settings, audit records for certain events that require logging, or the existence of initials or signatures on documents or records) that an IS control was performed. Business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals, as well as system design documentation may provide evidence of control design but do not provide evidence that controls are implemented and operating effectively. To use such documentation as part of the evidence of effective IS controls, the auditor obtains additional evidence to demonstrate that the IS controls have been implemented.

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

330.09 To test the implementation and operating effectiveness of relevant IS controls, the auditor uses professional judgment in determining and performing an appropriate mix of IS control tests to obtain sufficient, appropriate evidence to support their conclusions.

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

## Timing of IS Control Tests

330.11 The auditor should determine the timing of control tests to be performed for each relevant IS control. This determination is influenced by factors such as (1) the

engagement type, (2) the audit period, (3) the overall timeline of the engagement, (4) the type of evidence available to the auditor to demonstrate whether the IS control is implemented and operating effectively, and (5) the nature of the test.

## Extent of IS Control Tests

330.12 The auditor should determine the extent of IS control tests to be performed for each relevant IS control. The extent of IS control tests is the quantity of control testing to be performed for a specific IS control. This determination is influenced by the nature of the IS control test, as well as the frequency at which the entity performs the IS control. Additionally, this determination will influence whether the auditor will use statistical sampling or nonstatistical selection methods to determine whether the IS control is operating effectively.

330.13 The frequency at which the entity performs an IS control will inform the auditor's determination regarding the sufficiency of audit evidence obtained from a given IS control test. Generally, IS controls that are performed more frequently will require a greater extent of testing than those that are performed infrequently. For IS controls that do not operate frequently, such as those that operate only once or twice a year (e.g., periodic access recertification), the auditor may determine that it is necessary to test all the items in the population (i.e., all instances in which the IS control was performed during the audit period).

330.14 For IS controls that do not leave documentary evidence of existence or performance, the auditor may test their effectiveness through inquiry and observation. However, the appropriate extent of inquiry and observation is a matter of professional judgment. For application controls, the auditor may observe one or a few instances in which the IS control is performed. The auditor may also verify the completeness, accuracy, and validity of the results the applications produced. However, the auditor's determination regarding the implementation and operating effectiveness of application controls will partially depend on the auditor's conclusions on the effectiveness of the general controls upon which the application controls depend.

330.15 The auditor also considers whether circumstances that warrant the performance of an IS control occurred during the audit period. For example, certain IS controls for managing changes to entity information systems need not be tested for operating effectiveness if no relevant changes were made during the audit period. When such circumstances arise, the auditor corroborates the information obtained to confirm that the IS control was not applicable for the audit period.

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

## Statistical Sampling for IS Control Tests

330.17 The auditor should use attribute sampling and select items either through simple random selection (SRS) or through systematic random selection (SYS), when using statistical sampling to identify items within a population for control testing. SRS is a selection technique in which every combination of sampling units has the same probability of being selected as every other combination of the same number of sampling units—resulting in every member of the population having an equal probability of selection.[46] SYS is a selection technique in which a starting point within the first uniform interval—determined by dividing the number of units in the population by the sample size—is randomly selected and then an item is selected at each uniform interval from the starting point throughout the population. Attribute sampling achieves the objective of selecting items for the sample in such a way that the auditor may reasonably expect the sample to be representative of the relevant population and likely to provide the auditor with a reasonable basis for conclusions about the population.

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

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

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

330.20 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;

[46]American Institute of Certified Public Accountants, *Audit Guide: Audit Sampling*, ed. 2 (Hoboken, N.J.: Wiley 2019).

- identifying the evidence (e.g., source documents or transaction documents demonstrating whether the control is operating effectively) to be tested; and
- determining the period covered by the test.

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

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

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

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

330.23 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.

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

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

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

## Nonstatistical Selection for IS Control Tests

330.26 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 audit period. It may also be the most efficient way to test the control. For example, some IS controls may operate biweekly or weekly. For these controls, statistical sampling may not be efficient or even feasible given the small number of items in the population from which the auditor will select the sample. For these controls that operate less frequently, the effect of other sources of evidence is often greater than the effect for more frequent operating controls.

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

**Table 7: Testing Small Populations**

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

Source: GAO-26-108577. | GAO-26-108633

330.28 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.

## Automated Audit Tools

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

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

330.31 If the auditor plans to use automated audit tools, the auditor should obtain an understanding of 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.

330.32 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.

330.33 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

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

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

330.35 The service organization may use an independent auditor to prepare a service organization report. User entities of service organizations and their auditors may use this report to understand and obtain evidence about the service organization's controls. There are a variety of service organization reports prepared to provide assurance on the design, implementation, and operating effectiveness of various controls. In the context of an IS controls assessment performed using FISCAM, the auditor will generally use service organization reports that focus on controls relevant

to the entity's internal control over financial reporting.[47] These reports provide assurance over the design of internal controls at a point in time (type 1 report) or the design and operating effectiveness of internal controls over a period of time (type 2 report), including IS controls, based on the service organization's description of controls relevant to the service being provided.[48] A service organization report may be intended to satisfy the needs of multiple auditors conducting engagements with varying objectives. As a result, the service auditor's report may or may not address the relevant control objectives identified by the auditor. It is the auditor's responsibility to identify and evaluate the results of relevant tests of controls to determine whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of the relevant IS controls the service organization performs.

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

- assessing the adequacy of the standards under which the service auditor's report was issued;
- evaluating whether the report is for a period that is appropriate for the auditor's purpose;
- evaluating the adequacy of the relevant IS controls that the service organization performed, as described in the service auditor's report, to achieve relevant control objectives and the relevance and adequacy of the service auditor's tests of such controls;
- evaluating the adequacy of the period covered by the service auditor's tests of the IS controls the service organization performed and the time elapsed since performance of such tests;
- evaluating whether the results of the service auditor's tests of the IS controls the service organization performed, as described in the service auditor's report, provide sufficient, appropriate evidence to support the auditor's conclusions;

[47]These reports are issued under the American Institute of Certified Public Accountants' (AICPA) *Standards for Attestation Engagements [Clarified]* (AT-C) 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*. There are other types of reports on service organizations that may be available, including reports on controls at a service organization other than those likely to be relevant to user entities' internal control over financial reporting (for example, controls that are relevant to cybersecurity; supply chain; or user entities' compliance with specified requirements of laws, regulations, contracts, or grant agreements).

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

- determining whether complementary user-entity controls that the service organization identified as necessary to support the effectiveness of relevant IS controls the service organization performed are designed, implemented, and operating effectively;[49] and
- if applicable, evaluating the adequacy of any IS controls a subservice organization performed that are necessary to support the effectiveness of relevant IS controls the service organization performed.

330.37 For federal financial audits, the auditor should refer to *Financial Audit Manual* (FAM) 640, Entities Using a Service Organization, when inspecting a service organization report to obtain evidence about the design, implementation, and operating effectiveness of IS controls that a service organization performs. In such cases, the auditor uses FAM 640A, Service Organization Type 2 Assessment Tool, when determining whether the service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of relevant IS controls.

330.38 For performance audits, the auditor may adapt and apply the FAM Service Organization Type 2 Assessment Tool (FAM 640A) when determining whether a service organization report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of relevant IS controls.

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

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

330.40 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.

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

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

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

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

340.01 Once the auditor has determined the nature, timing, and extent of IS control tests and has updated the detailed test plans for each area of audit interest to document such tests planned for the relevant IS controls, the auditor performs the tests. The auditor performs IS control tests using suitable criteria and evaluates the results, including the significance of any IS control deficiencies identified.

340.02 In evaluating the results, the auditor performs an overall assessment of the evidence obtained and determines whether the audit procedures performed are adequate to reduce audit risk to an acceptably low level. In determining whether relevant IS controls are designed, implemented, and operating effectively to achieve the relevant control objectives for an area of audit interest, the auditor considers whether the evidence obtained supports the final assessment of IS control risk for the area of audit interest. The auditor communicates the results to the overall engagement auditor, if appropriate. The auditor prepares a written results memo (sometimes referred to as a summary memo) for the IS controls assessment to document the overall assessment of the collective evidence obtained and the auditor's final determinations regarding IS control risk and audit risk (section 350).

340.03 For federal financial audits, the auditor identifies control objectives that, if achieved, would address the risks of material misstatement on the SCE worksheet for which IS controls are identified. Additionally, the auditor is required to perform sufficient tests of IS controls that have been suitably designed and properly implemented to achieve the relevant control objectives and support a low assessed level of control risk for the financial audit.

### Perform IS Control Testing

340.04 The auditor should perform control tests of the relevant IS controls using suitable criteria. Criteria may include the relevant provisions in statutes, regulations, executive orders, implementing guidance, directives, policies, contracts, grant agreements, standards, measures, expected performance, defined business practices, and defined benchmarks against which performance of the selected control is compared or evaluated. See section 140 for further discussion on criteria. The evidence obtained through the auditor's IS control tests is included in the auditor's overall assessment of the collective evidence obtained throughout the IS controls assessment.

340.05 For federal financial audits, the auditor should comply with requirements for documenting IS controls that are included on the specific control evaluation worksheet as discussed in FAM 390, Documentation (Internal Control Phase).

### Determine Whether Relevant Control Objectives Are Achieved

340.06 The auditor should evaluate the results of control tests to determine whether relevant IS controls are implemented and operating effectively to achieve the relevant control objectives for each area of audit interest. Identified control deviations related to the design, implementation, or operating effectiveness of relevant IS controls may prevent achieving relevant control objectives and may result in IS control

deficiencies. A **control deviation** is an instance in which a control differs, or deviates, from the auditor's expectations regarding design, implementation, or operating effectiveness. A **control deficiency** is a condition when the design, implementation, or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, errors in information processing on a timely basis.

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

340.07 With assistance from the entity, the auditor investigates and obtains an understanding of the reasons for any IS control deviations. For those IS control deviations that are not resolved through entity-provided additional evidence, the auditor should communicate to management, in writing and on a timely basis, the details of the potential IS control deficiency identified. The auditor should communicate potential IS control deficiencies to the entity in sufficient detail for management to consider whether there are additional factors or compensating controls that are relevant to the auditor's determination of whether (1) a control deficiency exists and (2) the related control objective is achieved.

340.08 The auditor should determine whether there are specific compensating controls that could mitigate a potential IS control deficiency. If the auditor believes that compensating controls could adequately mitigate a potential IS control deficiency and achieve the related control objective, the auditor should obtain evidence that the compensating controls are designed, implemented, and operating effectively. If the compensating controls effectively mitigate the potential IS control deficiency, the auditor can conclude that the control objective is achieved. Nonetheless, the auditor communicates any control deviations identified to the entity. If the potential IS control deficiency is not effectively mitigated, the auditor will generally conclude that it is an IS control deficiency and document the elements of a finding—criteria, condition, cause, and effect. The auditor may also conclude and document the elements of a finding for certain potential IS control deficiencies that, despite being effectively mitigated, represent IS deficiencies. For example, the auditor may determine that a specific IS control selected for testing is not operating effectively. Although compensating controls mitigate the effect of this control failure, the auditor may elect to develop the elements of a finding to facilitate communication with management and to enable management to develop appropriate corrective actions.

340.09 The auditor should communicate to management the criteria, condition, cause, and effect of the IS control deficiencies identified through the IS controls assessment. These items may serve as the basis for recommendations for corrective actions, which are discussed in further detail in paragraphs 430.11 through 430.16.

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

340.10 The auditor should evaluate and document the significance of identified IS control deficiencies. In determining whether, individually or in combination, IS control deficiencies are significant in the context of the engagement objectives, the auditor considers their effect on IS control risk for each area of audit interest, as well as their impact on the effectiveness of relevant business process controls.

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

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

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

340.12 For federal financial audits, if IS control risk is assessed at moderate or high for one or more of the areas of audit interest, the auditor determines the impact of the underlying control deficiencies on the effectiveness of IS controls identified on the SCE worksheet. In determining whether the IS controls identified on the SCE worksheet are operating effectively to address the identified risks of material misstatement, the auditor considers the operating effectiveness of business process controls and indirect general controls. The auditor communicates these determinations to the financial auditor to assist them in completing the SCE worksheet. See section 430 for further discussion on reporting deficiencies.

340.13 For examination-level attestation engagements, the reassessment of IS control risk for each area of audit interest and determination of the impact of the underlying control deficiencies on the effectiveness of relevant business process controls forms the basis of the auditor's determination whether, individually or in combination, the IS control deficiencies are material weaknesses or significant deficiencies.[50] See section 430 for further discussion on reporting deficiencies.

340.14 For performance audits, this reassessment of IS control risk for each area of audit interest and determination of the impact of the underlying control deficiencies on the effectiveness of relevant business process controls forms the basis of the auditor's determination whether, individually or in combination, the IS control deficiencies are significant in the context of the control objectives. In addition, as part of this

[50]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

determination, the auditor considers whether management had previously detected or was otherwise aware of auditor-identified IS control deficiencies. See section 430 for further discussion on reporting deficiencies.

## Assess Sufficiency and Appropriateness of Evidence and Level of Audit Risk

340.15 The auditor should perform an overall assessment of the collective evidence obtained throughout the IS controls assessment to support the auditor's findings and conclusions. The auditor considers whether sufficient, appropriate evidence has been obtained to achieve the engagement objectives and report on the results. Sufficiency and appropriateness of evidence are relative concepts, which may be thought of as a continuum rather than as absolutes. Sufficiency and appropriateness are evaluated in the context of the related findings and conclusions. For example, even though the auditor may identify some limitations or uncertainties about the sufficiency or appropriateness of some of the evidence, the auditor may nonetheless determine that in total there is sufficient, appropriate evidence to support the findings and conclusions.

340.16 The auditor should determine whether the audit procedures performed throughout the IS controls assessment are adequate to reduce audit risk to an acceptably low level. The auditor's overall assessment of the collective evidence obtained and final assessment of IS control risk inform the auditor's conclusion regarding audit risk.

## 350 Prepare Testing Phase Documentation

350.01 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, and extent of audit procedures performed and the results of the IS controls assessment, including the significance of any IS control deficiencies identified.

350.02 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 Detailed Test Plans

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

350.04 The auditor should prepare a written results memo (sometimes referred to as a summary memo) for the IS controls assessment that includes a description of the overall assessment of the collective evidence obtained and the auditor's final determinations regarding IS control risk and audit risk.

350.05 The auditor should update and complete detailed test plans to document the approach for testing controls for the relevant control objectives for each area of audit interest.

350.06 Detailed 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 objectives;
- identify the relevant IS controls selected for testing that are likely to achieve the relevant control objectives;
- describe the nature, timing, and extent of IS control tests for each relevant IS control;
- document the results of completed IS control tests; and
- provide links to supporting documentation.

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

### Sampling Plans

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

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

## Technical Reviews

350.09 When the auditor uses automated audit tools, the auditor should prepare relevant audit documentation in sufficient detail to enable a technical review by audit staff independent of the preparer to determine that

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

## FISCAM Assessment Completion Checklist

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

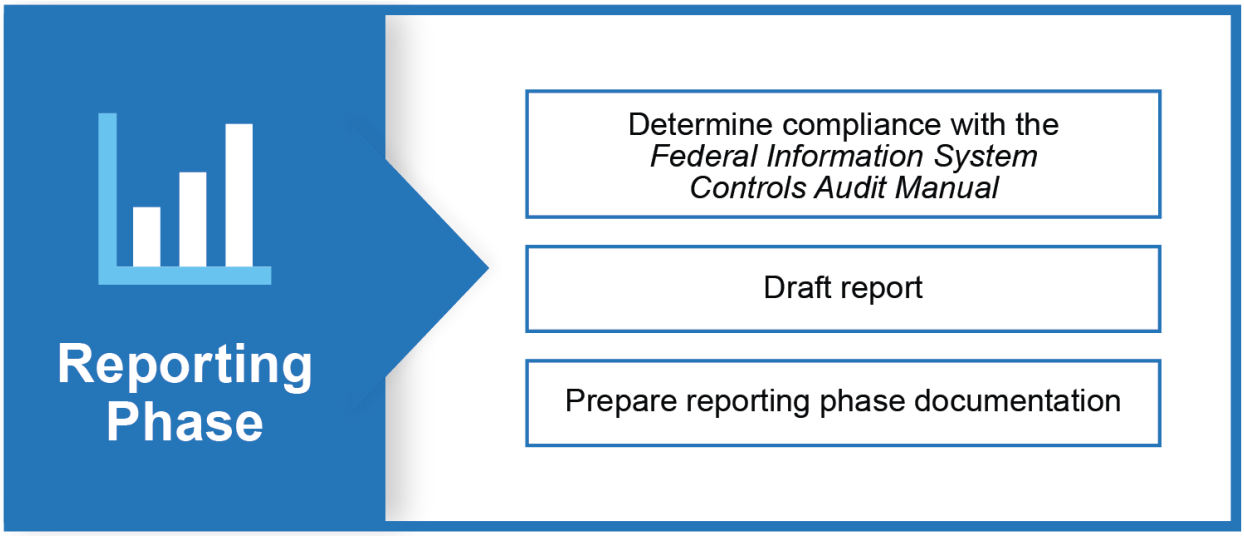
# SECTION 400

## Reporting Phase

## 410 Overview of the Reporting Phase

410.01 The overall objective of the reporting phase is to determine the auditor's compliance with *Federal Information System Controls Audit Manual* (FISCAM) requirements and to communicate the results of the information system (IS) controls assessment. This section addresses the auditor's compliance with the FISCAM methodology and the auditor's responsibilities for communicating the results of the IS controls assessment (see fig. 8).

**Figure 8: Reporting Phase Activities**




Source: GAO (data and icons). | GAO-26-108633

410.02 The auditor documents compliance with the FISCAM methodology by completing the FISCAM assessment completion checklist (app. 600B). The checklist lists FISCAM's requirements for conducting the IS controls assessment based on applicable generally accepted government auditing standards (GAGAS) requirements.

410.03 Depending on the engagement type and objectives, the results of the IS controls assessment may be incorporated into another engagement (e.g., financial audit report) or issued in a separate report. These results include communicating IS control deficiencies and providing recommendations for corrective action.

## 420 Determine Compliance with FISCAM

420.01 The auditor should determine whether the FISCAM methodology was followed. The FISCAM assessment completion checklist (app. 600B) 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

430.01 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.

430.02 The overall engagement auditor considers the engagement objectives, as well as the type of GAGAS engagement (financial audit, attestation engagement, or performance audit) to determine whether to issue a separate report on IS controls is issued or incorporate the results of the IS controls assessment into another engagement. 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.

430.03 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.[51] Each of these elements, including any differences in requirements based on engagement type, are discussed below.

### Objectives, Scope, and Methodology

430.04 Report users need information regarding the engagement objectives, scope, and methodology to understand the purpose of the engagement; the nature and extent of the work performed; the context and perspective regarding what is reported; and any significant limitations in the engagement objectives, scope, or methodology. Report content relevant to objectives, scope, and methodology differs among engagement types. Depending on the engagement type, the overall engagement auditor addresses the specific requirements established in GAGAS (2018).

### Findings, Conclusions, and Recommendations

430.05 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, if appropriate (e.g., the entity's IS controls are or are not effective in achieving the control objectives relevant to the engagement), and communicate identified deficiencies;

[51]If fraud is discovered as part of the engagement, the auditor addresses reporting requirements established in GAGAS (2018).

- 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 within the context of the engagement objectives, such as how they relate to (1) the design, implementation, and operating effectiveness of relevant IS controls or (2) the reliability of data intended to materially support findings, conclusions, or recommendations.

430.06 Generally, when internal control deficiencies are determined to be significant to the engagement objectives, such deficiencies are reported.[52] 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

430.07 GAGAS reporting requirements for federal financial audits relevant to internal control are addressed in the *Financial Audit Manual* (FAM), including the reporting of material weaknesses and significant deficiencies.[53] See section 340 for additional information on evaluating the significance of IS control deficiencies. The overall engagement auditor should comply with the reporting requirements, including requirements for classifying control weaknesses, as discussed 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 of 1982 and the Federal Financial Management Improvement Act of 1996.

## Attestation Engagements

430.08 Under GAGAS (2018), for examination-level attestation engagements, the overall engagement auditor should include in the examination report all internal control deficiencies considered to be significant deficiencies or material weaknesses that the auditor identified based on the engagement work performed.

## Performance Audits

430.09 The overall engagement auditor should include in the audit report (1) the scope of the auditor's work on internal control and (2) any deficiencies in internal control that are significant within the context of the engagement objectives and based upon the audit work performed.

430.10 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 overall engagement auditor should include those deficiencies in the report or

[52]A deficiency in internal control, including IS controls, exists 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, misstatements on a timely basis.

[53]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

communicate those deficiencies in writing to audited entity officials. If the written communication is separate from the audit report, the overall engagement auditor should refer to that written communication in the audit report.

## Presentation of Findings, Conclusions, and Recommendations

430.11 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 (paragraph 340.07). For performance audits, the extent to which the elements of a finding are developed depends on the engagement objectives.

430.12 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.
- Cause is the factor or factors responsible for the difference between the condition and the criteria and may serve as a basis for recommendations.
- 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.

430.13 The overall engagement 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 overall engagement 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 overall engagement 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 engagement objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions.

430.14 When reporting on the results of the audit work, the overall engagement 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 the 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 overall engagement auditor evaluates any potential limitations of the work on the auditor's report and the needs and expectations of users.

430.15 The overall engagement 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.

430.16 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

430.17 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.[54] 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.[55] Therefore, for reports that contain, or may contain, information prohibited from public disclosure, the overall engagement auditor should request that the source agency perform a classification, security, or sensitivity review of the draft report. The overall engagement auditor should evaluate entity concerns and make appropriate report revisions or redactions, considering legal or regulatory requirements.

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

430.19 The overall engagement 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.

430.20 When the audit organization is subject to public records laws, the overall engagement 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

[54]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.

[55]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.

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.

## 440 Prepare Reporting Phase Documentation

440.01 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

440.02 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 of the departure on performing the engagement, engagement conclusions, findings, and any related reports. 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. 600B).

### FISCAM Assessment Completion Checklist

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

# SECTION 500

## FISCAM Framework

## 510 Overview of the FISCAM Framework

510.01 The FISCAM Framework is an objectives-based control framework that is intended to be used in conjunction with the FISCAM methodology (sections 200 through 400). This framework provides guidance to assist the auditor in (1) identifying relevant control objectives and (2) identifying and understanding the entity's information system (IS) controls that are likely to achieve the relevant control objectives and are most efficient for testing. While the FISCAM Framework does not include auditor requirements, it is an integral part of the FISCAM methodology (sections 240, 250, 270, and 320).

510.02 The FISCAM Framework consists of six control categories, 24 critical elements, 81 control objectives, and associated illustrative controls. **Control categories** are broad groupings of controls based on similar types of risk. Control categories consist of the following: business process controls, security management, access controls, configuration management, segregation of duties, and contingency planning. **Critical elements** are components of a control category that are necessary for maintaining adequate IS controls within the FISCAM control category. **Control objectives** are the aim or purpose of specified IS controls and address risks to achieving the critical elements. **Illustrative controls** are examples of IS controls that may achieve the control objectives. The FISCAM control categories are consistent with those included in generally accepted government auditing standards (GAGAS).[56] The critical elements and control objectives are consistent with the principles and attributes included in *Standards for Internal Control in the Federal Government* (Green Book).[57] See paragraph 110.19 for additional discussion on the consistency between the FISCAM Framework and the Green Book's principles and attributes.

510.03 This section presents the FISCAM Framework with illustrative audit procedures and references to associated information security and privacy controls published in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*.[58] Illustrative controls and audit procedures provide guidance to assist the auditor in evaluating management's efforts to satisfy the critical elements. The illustrative controls are consistent with management's information security and privacy controls, as included in NIST Computer Security Resource Center publications. Specifically, each illustrative control aligns with one or more of the control statements for the information security and privacy controls published in NIST SP 800-53.[59] The FISCAM Framework references these control statements using the NIST's alphanumeric numbering scheme, which includes the abbreviations for the control families as shown in table 8.

[56]GAO, *Government Auditing Standards: 2018 Revision Technical Update April 2021*, GAO-21-368G (Washington, D.C.: April 2021).
[57]GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 2025).
[58]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).
[59]Each of the information security and privacy controls published in NIST SP 800-53 includes references to other sources—including statutes, executive orders, and implementing guidance—for additional information related to the control, if any. See section 140 for additional information on criteria.

**Table 8: National Institute of Standards and Technology's Information Security and Privacy Control Family Abbreviations**

| ID | FAMILY |
|---|---|
| AC | Access Control |
| AT | Awareness and Training |
| AU | Audit and Accountability |
| CA | Assessment, Authorization, and Monitoring |
| CM | Configuration Management |
| CP | Contingency Planning |
| IA | Identification and Authentication |
| IR | Incident Response |
| MA | Maintenance |
| MP | Media Protection |
| PE | Physical and Environmental Protection |
| PL | Planning |
| PM | Program Management |
| PS | Personnel Security |
| PT | Personally Identifiable Information Processing and Transparency |
| RA | Risk Assessment |
| SA | System and Services Acquisition |
| SC | System and Communications Protection |
| SI | System and Information Integrity |
| SR | Supply Chain Risk Management |

Source: National Institute of Standards and Technology. | GAO-26-108633

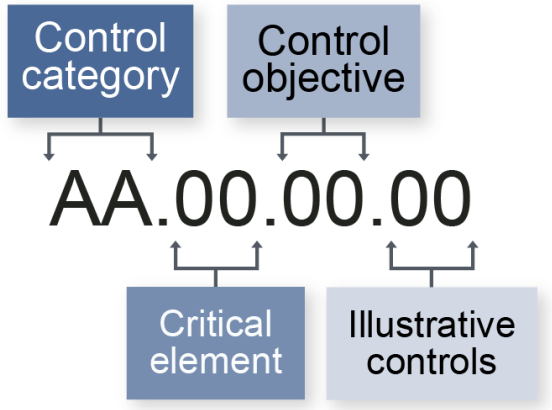
510.04 Though the FISCAM Framework presents illustrative controls based on the control statements in NIST SP 800-53, the framework is not intended to be used as criteria. Considering the illustrative controls, the auditor identifies the entity's IS controls that may achieve the control objectives. The auditor is ultimately responsible for obtaining an understanding of those IS controls in sufficient detail to assess IS control risk and design appropriate audit procedures.

510.05 Though the FISCAM Framework presents illustrative audit procedures, the framework is not intended to be used as an audit plan. Rather, it is incumbent upon the auditor to prepare an audit plan, which includes a detailed test plan for each

area of audit interest, that supports achieving the engagement objectives and responds to the auditor's assessment of IS control risk. 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 control objectives.

510.06 The FISCAM Framework, illustrative audit procedures, and referenced NIST SP 800-53 controls are presented in table format by control category. Each table is organized in a hierarchical structure (section 110, fig. 3) to facilitate the auditor's planning, testing, and reporting procedures. The control categories, critical elements, control objectives, and illustrative controls are presented using a four-tiered alphanumeric numbering scheme as depicted in figure 9. In addition, the critical elements and control objectives are designated using dark blue and light gray shading, respectively. In contrast, illustrative controls, illustrative audit procedures, and referenced NIST SP 800-53 controls are presented without shading.

**Figure 9: The Federal Information System Controls Audit Manual Framework Numbering Scheme**




Source: GAO. | GAO-26-108633

## 520 FISCAM Framework for Business Process Controls

520.01 The business process (BP) controls category relates to the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions; activities across business processes; and events between business process applications, their components, and other systems.

520.02 The FISCAM Framework for Business Process Controls (see table 9) includes six critical elements that are necessary for establishing adequate controls within this control category:

- BP.01 Management designs and implements user and application controls to reasonably assure that data input into the information system are complete, accurate, and valid.
- BP.02 Management designs and implements user and application controls to reasonably assure that data processing by the information system is complete, accurate, and valid.
- BP.03 Management designs and implements user and application controls to reasonably assure that output data are complete, accurate, and valid.
- BP.04 Management designs and implements general controls to reasonably assure that business process applications are properly managed to achieve information processing objectives.
- BP.05 Management designs and implements general controls to reasonably assure that system interfaces are properly managed to achieve information processing objectives.
- BP.06 Management designs and implements general controls to reasonably assure that data management systems are properly managed to achieve information processing objectives.

520.03 Assessing business process controls involves evaluating management's efforts to satisfy each of these critical elements. When evaluating management's efforts for each critical element, the auditor considers whether the associated control objectives (shown in table 9), if achieved, will address risks to information processing objectives—completeness, accuracy, and validity—relevant to the engagement objectives. Ineffective business process controls may result in incomplete, inaccurate, or invalid data.

**Table 9: FISCAM Framework for Business Process (BP) Controls**

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.01 Management designs and implements user and application controls to reasonably assure that data input into the information system are complete, accurate, and valid. | | |
| BP.01.01 Data are properly prepared and approved for input into the information system on a timely basis. | | |
| BP.01.01.01 Input data are derived from appropriate sources. | Obtain an understanding of the entity's processes and methods for preparing data for input through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as source documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Observe appropriate personnel as they prepare data for input and inspect any source documentation or additional support prepared.<br>Observe any reviews of source documentation or additional support prepared.<br>Through inquiry and inspection, obtain an understanding of the entity's processes and methods to maintain evidence of input activities for subsequent review or reference.<br>Inspect a selection of transactions and trace selected data from the information system back to sources from which the data originated. | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Consider whether any of the selected data have been manipulated from their original form.<br>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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect a selection of transactions, or a selected batch of transactions, and assess the use of control totals in the processing of such transactions.<br>Determine whether control totals are appropriately employed when practicable.<br>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 those from a processed set of records (output) to those of the same set of records before processing (input). | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>Inspect a selection of transactions and assess the use of sequence checking in the processing of such transactions.<br>Determine whether sequence checking is appropriately employed when practicable.<br>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. | NIST SP 800-53, SI-10 |
| 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 | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inquiry of appropriate personnel and<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Observe appropriate personnel as they perform user-defined processing of data. Observe any reviews of such processing.<br>Inspect program code to obtain an understanding of the automated processing being performed.<br>Through inquiry and inspection, obtain an understanding of the entity's processes and methods to maintain evidence of user-defined processing 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.<br>Determine whether user-defined processing of data is appropriately controlled.<br>Note: Some business process applications may allow user-defined processing of data, whereby a 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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*Related control: BP.04.03.09* | Obtain an understanding of the entity's processes and methods for preparing data for input through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as source documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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 review activities for subsequent review or reference.<br>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.<br>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. | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.01.02 Data input 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.<br>*Related controls: BP.01.02.03, BP.02.01.01, BP.02.01.02, BP.04.03.10, BP.04.05.01, and BP.06.03.04* | Obtain an understanding of the entity's use of data input controls within the significant business processes through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 input 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 data input errors.<br>Observe a user attempt to subvert the data input controls to prevent duplicate entries. Note any error messages and whether the transaction is suspended or processed.<br>Inspect system design documentation and applicable system configuration files to assess the design of key data input controls, including the specified definitions for data format and content.<br>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. | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 an 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.<br>*Related control: BP.01.02.03* | Obtain an understanding of the entity's use of data input controls within the significant business processes through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 input 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 data input errors.<br>Observe a user attempt to subvert the data input controls to prevent duplicate entries. Note any error messages and whether the transaction is suspended or processed. | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect system design documentation and applicable system configuration files to assess the design of key data input controls, including the specified definitions for data format and content.<br>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 produces combinations thereof when input data are not accepted.<br>*Related controls: BP.01.02.01, BP.01.02.02, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.01.02, and AC.05.01.03* | Obtain an understanding of the entity's use of error messages and event logging within the significant business processes through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 data input errors.<br>Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems.<br>Inspect audit records for the event types selected for logging that are applicable to relevant information systems. Consider the appropriateness of the documentation obtained, including any reports | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-12<br>NIST SP 800-53, SI-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | produced using log management software and reviewed by management.<br>Determine whether relevant information systems appropriately generate error messages, post log entries, or produce 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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as error or suspense reports.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>Determine whether rejected input data are held in suspense and identified on error reports until the errors are researched and appropriately resolved. | NIST SP 800-53, AU-02<br>NIST SP 800-53, SI-11 |
| BP.01.03 Data input errors are researched and resolved on a timely basis. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.01.03.01 Data input 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 input errors through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as error or suspense reports.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect a selection of error or suspense reports and consider whether data input 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.<br>Determine whether data input errors are appropriately researched to properly identify and remediate the cause(s) of the errors. | NIST SP 800-53, SI-10 |
| BP.01.03.02 Data input errors are resolved through the entry or upload of corrected input data. | Obtain an understanding of the entity's processes and methods for resolving data input errors through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of other relevant documentation, such as documentation for error resolution.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect a selection of error or suspense reports and consider whether data input errors and rejected input data are being resolved through the entry or upload of corrected input data.<br>Determine whether data input errors are appropriately resolved through the entry or upload of corrected input data. | |
| BP.01.03.03 Manual overrides of data input errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.<br>*Related controls: BP.02.02.03 and BP.03.03.03* | Obtain an understanding of the entity's processes and methods for manually overriding data input errors through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as documentation for error resolution.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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, AU-02<br>NIST SP 800-53, AU-06<br>NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect a selection of error or suspense reports and consider whether manual overrides of data input 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.<br>Determine whether manual overrides of information system data input errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.<br>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 controls to reasonably assure that data processing by the information system is complete, accurate, and valid. | | |
| BP.02.01 Data processing errors are identified on a timely basis. | | |
| BP.02.01.01 The system validates that in-process data match definitions for format and content, such as character set, length, numerical range, and acceptable values, and will not continue processing data that do not satisfy these definitions.<br>*Related controls: BP.01.02.01, BP.04.03.10, BP.04.05.02, and BP.06.03.04* | Obtain an understanding of the entity's use of data input controls within the significant business processes through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 input controls to help ensure the accuracy and validity of data as they move through the process. Identify key system interfaces or other key system entry points for in-process data.<br>Inspect system design documentation and applicable system configuration files to assess the design of key data input controls, including the specified definitions for data format and content.<br>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.<br>*Related controls: BP.01.02.01, BP.01.02.03, BP.02.01.03, BP.02.01.05, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.01.02, and AC.05.01.03* | Obtain an understanding of the entity's use of event logging within the significant business processes through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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. | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems.<br>Inspect audit records for the event types selected for logging that are applicable to relevant information systems. Consider the appropriateness of the documentation obtained, including any reports produced using log management software and reviewed by management.<br>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.<br>*Related control: BP.02.01.02* | Obtain an understanding of the entity's processes and methods for reviewing information system data processing logs through<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as information system data processing logs.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 use of information system data processing logs.<br>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. | NIST SP 800-53, AU-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether relevant information systems perform appropriate reconciliations to identify potential data processing errors. | NIST SP 800-53, SI-10 |
| BP.02.01.05 The system generates an error message, posts a log entry when data processing errors occur, or both. | Obtain an understanding of the entity's use of error messages and event logging within the significant business processes through<br>• inquiry of appropriate personnel; | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-12<br>NIST SP 800-53, SI-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| *Related controls: BP.01.02.03, BP.02.01.02, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.01.02, and AC.05.01.03* | • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as system design documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems.<br>Inspect audit records for the event types selected for logging that are applicable to relevant information systems. Consider the appropriateness of the documentation obtained, including any reports produced using log management software and reviewed by management.<br>Determine whether relevant information systems appropriately generate an error message, post a log entry, or produce combinations thereof when data processing errors occur. | |
| 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<br>• inquiry of appropriate personnel; | NIST SP 800-53, AU-02<br>NIST SP 800-53, SI-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as error or suspense reports.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect a selection of error or suspense reports and consider whether data processing errors are identified.<br>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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as error or suspense reports.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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.<br>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, correcting 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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as documentation for error resolution.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect a selection of error or suspense reports and consider whether data processing errors are being resolved on a timely basis through | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | the correction of data, the correction of coding errors in computer programs, or a combination of such actions.<br>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.<br>*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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as documentation for error resolution.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>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. | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-06<br>NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.03 Management designs and implements user and application controls to reasonably assure that output data are complete, accurate, and valid. | | |
| BP.03.01 Data are approved for output. | | |
| BP.03.01.01 The format and content of output data are aligned with management's definitions.<br>*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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such outputs involved in the significant business processes.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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. | NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether the format and content of output data are aligned with management's definitions.<br>Note: Output data may include data files and system-generated reports. | |
| BP.03.02 Output data errors are identified on a timely basis. | | |
| 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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>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<br>NIST SP 800-53, SI-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as error or suspense reports.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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. | NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |
| 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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and | NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of other relevant documentation, such as documentation for error resolution.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect a selection of error or suspense reports and consider whether output data errors are being resolved through the correction of data, the correction of coding errors in computer programs, or a combination of such actions.<br>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.<br>*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<br>• inquiry of appropriate personnel;<br>• inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and<br>• inspection of other relevant documentation, such as documentation for error resolution.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-06<br>NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | business process, the format and content of inputs and outputs involved, and the sources of relevant input data.<br>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.<br>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.<br>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.04 Management designs and implements general controls to reasonably assure that business process applications are properly managed to achieve information processing objectives. | | |
| BP.04.01 Business process application roles and responsibilities are defined and assigned to appropriate personnel. | | |
| BP.04.01.01 Business process application ownership is appropriately assigned.<br>*Related controls: BP.05.01.01, BP.06.01.01, SM.01.02.02, SM.01.02.03, and SM.01.06.05* | Obtain an understanding of business process application roles and responsibilities, including business process application and information system ownership, through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as system security and privacy plans.<br>Identify the business process application owners for the relevant information systems. Consider whether they are senior management | NIST SP 800-53, PL-02<br>NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities.<br>Determine whether business process application and information system ownership has been appropriately assigned.<br>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 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 | Obtain an understanding of the business process application responsibilities for information resource owners, users, and security administrators, as well as appropriate authorizing officials, through<br>• inquiry of appropriate personnel and | NIST SP 800-53, AC-22<br>NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| security administrators, as well as appropriate authorizing officials.<br>*Related controls: BP.05.01.02, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, SM.01.02.02, SM.01.02.03, SM.01.06.05, and SD.01.01.01* | • inspection of relevant documentation, such as system security and privacy plans.<br>Identify the information resource owners, users, and security administrators, as well as appropriate authorizing officials, for the relevant information systems. Consider whether they possess appropriate skills and technical expertise to satisfy their assigned responsibilities.<br>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.<br>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 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. | NIST SP 800-53, PM-24 |
| 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 | Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating | NIST SP 800-53, AC-01<br>NIST SP 800-53, AT-01<br>NIST SP 800-53, AU-01 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| applications are developed, documented, approved, and periodically reviewed and updated. Such policies and procedures appropriately<br>• consider risk;<br>• address data management, including data input 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;<br>• address changes to business process application functionality through modifications to application software or changes to configurable controls within application software;<br>• address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external parties, and compliance;<br>• identify and describe the relevant processes;<br>• consider general and application controls;<br>• consider segregation of duties controls; and | system-level and business process-level policies and procedures for administering and using business process applications through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>Through inquiry, inspection, and observation, identify information system (IS) 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 IS controls are designed, implemented, and operating effectively. Consider whether<br>• policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external parties, and compliance;<br>• 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 general and application controls, as well as segregation of duties controls; and<br>• policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity's internal control objectives.<br>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. | NIST SP 800-53, CA-01<br>NIST SP 800-53, CM-01<br>NIST SP 800-53, CP-01<br>NIST SP 800-53, IA-01<br>NIST SP 800-53, IR-01<br>NIST SP 800-53, MA-01<br>NIST SP 800-53, MP-01<br>NIST SP 800-53, PE-01<br>NIST SP 800-53, PL-01<br>NIST SP 800-53, PM-01<br>NIST SP 800-53, PS-01<br>NIST SP 800-53, PT-01<br>NIST SP 800-53, RA-01<br>NIST SP 800-53, SA-01<br>NIST SP 800-53, SC-01<br>NIST SP 800-53, SI-01<br>NIST SP 800-53, SR-01 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| • help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities. | 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 IS 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 IS controls. | |
| BP.04.03 Business process applications are designed to facilitate the performance of business processes and reasonably assure the completeness, accuracy, and validity of transactions and data. | | |
| BP.04.03.01 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 general and application controls observed during the walk-throughs are consistent with those documented in system documentation and align with prescribed information protection requirements for the business process applications and information systems.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.<br>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. | NIST SP 800-53, CM-12<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, PM-32<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05<br>NIST SP 800-53, SA-08<br>NIST SP 800-53, SC-27<br>NIST SP 800-53, SI-22 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br><br>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.<br><br>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.<br><br>Application module interaction may be depicted in call graphs, data flow diagrams, and control flow diagrams. A data dictionary or data 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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.<br>Determine whether the significant business processes are standardized and automated as practicable. | NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |
| 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.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. When appropriate, inspect program code to assess the design of the automated business processes and corresponding application controls.<br>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.<br>Determine whether the automated business processes and corresponding application controls are suitably designed and properly | NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | implemented to reasonably assure that transactions are complete, accurate, and valid.<br>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.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. When appropriate, inspect program code to assess the design of the automated business processes and corresponding application controls.<br>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.<br>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<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | records maintained in data management systems are complete, accurate, and valid.<br>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.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. When appropriate, inspect program code to assess the design of the automated business processes and corresponding application controls.<br>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.<br>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. | NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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. | |
| BP.04.03.06 Automated business processes and corresponding 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. | 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 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.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. When appropriate, inspect program code to assess the design of the automated business processes and corresponding application controls.<br>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.<br>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, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |
| BP.04.03.07 Access controls are incorporated into the design of automated business processes and corresponding application | Perform walk-throughs of the significant business processes. Consider whether access controls are incorporated into the design of automated | NIST SP 800-53, AC-05<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| controls to prevent users from executing incompatible transactions within the business process application through menus, screens, or other user interfaces.<br>*Related controls: SD.01.01.01, SD.01.01.02, SD.01.02.01, SD.01.02.02, and SD.01.03.01* | business processes and corresponding application controls to prevent users from executing incompatible transactions.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.<br>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 business process application through menus, screens, or other user interfaces. | NIST SP 800-53, SA-05 |
| BP.04.03.08 Transaction processing roles are aligned with management's authorizations for users and processes acting on behalf of users.<br>*Related control: BP.04.06.02*<br>*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.<br>Inspect system design documentation, system security and privacy plans, role permission matrices, and policies and procedures demonstrating the design of transaction processing roles and criteria for role membership.<br>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 appropriateness of the documentation obtained when performing control tests. 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. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether transaction processing roles are aligned with management's authorizations for users and processes acting on behalf of users. | |
| BP.04.03.09 Approval workflows within the business process application are aligned with management's authorizations for users and appropriately controlled.<br>*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.<br>Inspect system design documentation, system security and privacy plans, role 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. Consider the appropriateness of the documentation obtained when performing control tests.<br>Perform walk-throughs of the significant business processes. Consider whether approval workflows within the business process application prevent unauthorized users from approving transactions and enforce appropriate segregation of duties.<br>Determine whether approval workflows within the business process application are aligned with management's authorizations for users and appropriately controlled. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06<br>NIST SP 800-53, CM-05 |
| 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.<br>*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. | NIST SP 800-53, SI-10<br>NIST SP 800-53, SI-11<br>NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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. | |
| 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 relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.<br>*Related controls: BP.03.01.01 and BP.04.05.03* | 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 relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the format and content of output data and their distribution.<br>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 relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.<br>Note: Management may have procedures in place to monitor the replication of output data within or outside the entity. | NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*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<br>• inquiry of appropriate personnel, including any senior officials responsible for the training, and<br>• inspection of relevant documentation, such as training course materials.<br>Consider whether<br>• training course materials have been recently reviewed and updated, as appropriate;<br>• mandatory training courses are identified and communicated to information system users as a condition for system access, as applicable; and<br>• management adequately monitors the completion status of applicable mandatory training courses for information system users.<br>Determine whether management has established, documented, maintained, and monitored user training that focuses on the correct use of the business process application.<br>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 | NIST SP 800-53, AT-03<br>NIST SP 800-53, AT-04<br>NIST SP 800-53, SA-16 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 (PII). | | |
| 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 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 PII processing needs for the business process applications and information systems.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.<br>Determine whether business process application characteristics are defined, implemented, and documented with appropriate consideration for privacy.<br>Note: Entities are required to define business processes with consideration for privacy and determine the PII 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 it establishes or modifies 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 (OMB) | NIST SP 800-53, PM-11<br>NIST SP 800-53, PT-06<br>NIST SP 800-53, PT-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | guidance, the notice describes the existence and character of the system and identifies<br>• the system of records, the purpose of the system,<br>• the authority for maintenance of the records,<br>• the categories of records maintained in the system,<br>• the categories of individuals about whom records are maintained,<br>• the routine uses to which the records are subject, and<br>• additional details about the system as described in OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.<br>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. | |
| BP.04.04.02 Automated business processes and corresponding application controls are designed to provide notice to information system users about the processing of PII. | 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 | NIST SP 800-53, PT-04<br>NIST SP 800-53, PT-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| When appropriate, the processes and controls also allow information system users to consent to the processing of their PII. | system users about the processing of PII and, when appropriate, allow information system users to consent to the processing of their PII.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.<br>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.<br>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 PII and, when appropriate, information system users to consent to the processing of their PII.<br>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 PII and, when appropriate, information system users to consent to the processing of their PII. | |
| BP.04.04.03 Automated business process and corresponding application controls are designed to apply processing conditions for specific categories of PII based on risk. | 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 PII based on risk.<br>Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of | NIST SP 800-53, PT-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | automated business processes and corresponding application controls.<br>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.<br>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 PII are based on risk.<br>Note: Entities apply any conditions or protections that may be necessary for specific categories of PII. These conditions may be required by relevant provisions in 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 requirements that apply. | |
| BP.04.04.04 Management develops, documents, and periodically reviews and updates a map of system data actions that process PII. | 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 PII through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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<br>• discrete data actions,<br>• elements of PII being processed in the data actions, | NIST SP 800-53, CM-13 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • system components involved in the data actions, and<br>• the owners or operators of those system components.<br>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.<br>Note: Data actions are system operations that process PII. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. Understanding what PII is being processed (e.g., the sensitivity of the PII), how PII 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 PII) provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system.<br>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 application controls and the adequacy of automated business processes that business process applications perform are periodically assessed. | | |
| BP.04.05.01 Management periodically reviews implemented configuration settings, parameters, and tolerances for data input | Obtain an understanding of the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for data input controls through<br>• inquiry of appropriate personnel and | NIST SP 800-53, CA-02<br>NIST SP 800-53, CM-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| controls against specified definitions for input data format and content.<br>*Related control: BP.01.02.01* and *BP.04.03.10* | • inspection of relevant documentation, such as policies and procedures.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings, parameters, and tolerances for data input controls during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's policies and procedures.<br>Inspect implemented configuration settings, parameters, and tolerances for data input controls to independently assess whether such are consistent with management's specified definitions for input data.<br>Determine whether the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for data input controls are designed, implemented, and operating effectively. | |
| 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.<br>*Related control: BP.02.01.01 and BP.04.03.10* | Obtain an understanding of the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for data input controls through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings, parameters, and tolerances for in-process data input controls during the audit period. Consider whether such actions were appropriate and | NIST SP 800-53, CA-02<br>NIST SP 800-53, CM-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | performed in accordance with the entity's policies and procedures. Inspect implemented configuration settings, parameters, and tolerances for in-process data input controls to independently assess whether such are consistent with management's specified definitions for in-process data.<br>Determine whether the entity's processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for in-process data input controls 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.<br>*Related controls: BP.03.01.01, BP.04.03.10, 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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-02<br>NIST SP 800-53, CM-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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-02 |
| 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).<br>*Related control: BP.06.05.01*<br>*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 appropriateness of system-generated evidence when performing control tests. 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.<br>Determine whether business process application roles and corresponding access privileges are appropriately authorized and assigned to users with a valid business purpose (least privilege). | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 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.<br>*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 using the business process applications and information systems relevant to the significant business processes.<br>Observe the execution of sensitive transactions. Consider whether the users involved in this process are appropriately authorized to perform such actions.<br>Observe the approval of transactions and inspect any documentary evidence related to such approvals. Consider whether the users involved in approving transactions that others initiated are appropriately authorized to perform such actions.<br>Determine whether the execution of sensitive transactions and the approval of transactions initiated by other users are appropriately controlled.<br>Note: In FISCAM, sensitive means the nature of information 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. Only users authorized to execute sensitive transactions or approve transactions that others initiated can access such transactions or functions within the business process application through menus, screens, or other user interfaces. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*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.<br>Inspect system design documentation, system security and privacy plans, role permission matrices, and policies and procedures demonstrating the design of transaction processing roles and criteria for role membership.<br>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 appropriateness of system-generated evidence when performing control tests. 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.<br>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. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06 |
| 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, identify key output data, including key reports generated by the business process applications and information systems relevant to the significant business processes.<br>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.<br>Determine whether key output data, including key reports generated by the business process applications and information systems relevant | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06<br>NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | to the significant business processes, are appropriately restricted to authorized users and other individuals for authorized purposes.<br>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. | |
| BP.04.06.05 The business process application logs events associated with failed user attempts to perform unauthorized data input, processing, or output procedures.<br>*Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.05.04.05, BP.06.05.03, AC.05.01.02, and AC.05.01.03* | Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identify key event types for logging associated with the entity's procedures for data input, processing, and output.<br>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.<br>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.<br>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, | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-03<br>NIST SP 800-53, AU-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>*Related control: CM.02.01.02*<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to modify application software. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that modifications to application software are appropriately authorized, tested, and approved.<br>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.<br>Determine whether modifications to application software are authorized, tested, and approved. | NIST SP 800-53, SA-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.04.07.02 Changes to configurable controls within application software are appropriately controlled.<br>*Related control objectives: CM.02.01 and CM.02.02* | Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identify configurable controls within application software relevant to the significant business processes.<br>Obtain an understanding of the entity's processes and methods to change configurable controls within application software through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to change configurable controls. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that changes to configurable controls within application software are appropriately controlled.<br>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.<br>Determine whether changes to configurable controls within application software are appropriately controlled. | NIST SP 800-53, CM-03 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 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 processes or tools to detect unauthorized changes to application software.<br>*Related controls: BP.06.06.05 and CM.02.03.03* | Obtain an understanding of the entity's processes and methods for detecting unauthorized changes to application software through<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's integrity verification tools, and<br>• 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.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Inspect the implemented configuration settings for the integrity verification tools employed in connection with the business process | NIST SP 800-53, CM-06<br>NIST SP 800-53, SI-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>Determine whether management properly employs integrity verification tools to detect unauthorized changes to application software.<br>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 controls to reasonably assure that system interfaces are properly managed to achieve information processing objectives. | | |
| BP.05.01 System interface roles and responsibilities are defined and assigned to appropriate personnel. | | |
| BP.05.01.01 System interface ownership is appropriately assigned.<br>*Related controls: BP.04.01.01, BP.06.01.01, SM.01.02.02, SM.01.02.03, and SM.01.06.05* | Obtain an understanding of system interface roles and responsibilities, including system interface ownership, through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as system security and privacy plans.<br>Identify the system interface owners for the relevant information systems. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities.<br>Determine whether system interface ownership has been appropriately assigned.<br>Note: System interface ownership comprises overall responsibility and accountability for management of the system interface, including ensuring that the system interface is properly processed on a timely basis in a secure manner. Thus, any changes to the design of the | NIST SP 800-53, PL-02<br>NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | system interface, modifications to the tools and techniques for system interface processing, or changes to corresponding access controls generally require the approval of the system interface owner or the owner's authorized delegate. | |
| BP.05.01.02 Responsibilities for system interface processing and correcting any errors are assigned to appropriate personnel, which may include users from the source and target systems.<br>*Related controls: BP.04.01.02, BP.05.06.02, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, SD.01.01.01, SM.01.02.02, SM.01.02.03, and SM.01.06.05* | Obtain an understanding of the responsibilities for system interface processing and correcting any errors through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.<br>See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether assigned individuals possess appropriate skills and technical expertise to satisfy their responsibilities.<br>Determine whether the responsibilities for system interface processing and correcting any errors have been clearly defined and assigned to appropriate personnel.<br>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-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |
| BP.05.02 Policies and procedures for managing system interfaces are developed and implemented. | | |
| BP.05.02.01 Policies and procedures applied at the system and business process levels for managing system interfaces are developed, documented, approved, and periodically | 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 system interfaces through | NIST SP 800-53, AC-01<br>NIST SP 800-53, AT-01<br>NIST SP 800-53, AU-01 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| reviewed and updated. Such policies and procedures appropriately<br>• consider risk;<br>• address the tools and techniques for system interface processing, including the use of job scheduling software, the timing of the system interface, and any dependences on upstream jobs or processes;<br>• address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external parties, and compliance;<br>• identify and describe the relevant processes;<br>• consider general and application controls;<br>• consider segregation of duties controls; and<br>• help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities. | • inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>Through inquiry, inspection, and observation, identify IS 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 IS controls are designed, implemented, and operating effectively. Consider whether<br>• policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external parties, and compliance;<br>• 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 general and application controls as well as segregation of duties controls; and<br>• policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purposes and support achieving the entity's internal control objectives.<br>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.<br>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 | NIST SP 800-53, CA-01<br>NIST SP 800-53, CM-01<br>NIST SP 800-53, CP-01<br>NIST SP 800-53, IA-01<br>NIST SP 800-53, IR-01<br>NIST SP 800-53, MA-01<br>NIST SP 800-53, MP-01<br>NIST SP 800-53, PE-01<br>NIST SP 800-53, PL-01<br>NIST SP 800-53, PM-01<br>NIST SP 800-53, PS-01<br>NIST SP 800-53, PT-01<br>NIST SP 800-53, RA-01<br>NIST SP 800-53, SA-01<br>NIST SP 800-53, SC-01<br>NIST SP 800-53, SI-01<br>NIST SP 800-53, SR-01 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | assess the design, implementation, and operating effectiveness of IS 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 system 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 IS controls. | |
| BP.05.03 System interfaces are designed to exchange information between systems and reasonably assure the completeness, accuracy, and validity of the exchange. | | |
| BP.05.03.01 System interface characteristics are defined, implemented, and documented.<br>*Related controls: SM.03.02.01, SM.03.02.02, and AC.01.01.01* | Perform walk-throughs of the significant business processes. Consider whether the system interfaces observed during the walk-throughs 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 system interface includes appropriate specifications based on relevant business requirements.<br>Inspect system design documentation, system security and privacy plans, interconnection security agreements, system 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 procedures demonstrating the design of system interfaces involved in the significant business processes.<br>Determine whether system interfaces are defined, implemented, and documented to reasonably assure the confidentiality, integrity, and availability of information.<br>Note: System interface design documentation is maintained to support the entity's authorization process and to facilitate configuration | NIST SP 800-53, CA-03<br>NIST SP 800-53, CA-09<br>NIST SP 800-53, CM-12<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-05<br>NIST SP 800-53, SA-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | management and change control procedures. System interface characteristics include the tools and techniques for system 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 system interface or interface schedule, and any system balancing requirements and information security requirements. System 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 system interfaces observed during the walk-throughs 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 system interface includes appropriate hashing algorithms or other mechanisms based on relevant business requirements.<br>Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of system interfaces involved in the significant business processes.<br>Determine whether hashing algorithms or other mechanisms are employed to help ensure the integrity of interfaced data. | NIST SP 800-53, SC-13 |
| BP.05.03.03 Encryption techniques are employed to protect the confidentiality of interfaced data when appropriate.<br>*Related control: AC.03.02.02* | Perform walk-throughs of the significant business processes. Consider whether the system interfaces observed during the walk-throughs 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 | NIST SP 800-53, SC-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | design of each system interface includes appropriate encryption techniques based on relevant business requirements.<br>Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of system interfaces involved in the significant business processes.<br>Determine whether encryption techniques are employed to protect the confidentiality of interfaced data when appropriate. | |
| 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 system interface processing, including the use of job scheduling software, the timing of each system 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.<br>Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of system interfaces involved in the significant business processes.<br>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.<br>Determine whether the automated business processes and corresponding application controls are suitably designed and properly | NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | implemented to reasonably assure that interfaced data are processed once and only once.<br>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, system interface files may be automatically archived or deleted from the production environment after processing. | |
| BP.05.04 System 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 or submodule are received by the target system or submodule. | Obtain an understanding of any mechanisms that the entity employs to notify users when files sent from a source system are received by the target system through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.<br>See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Perform walk-throughs of the significant business processes. Observe the use of any mechanisms that the entity employs to notify users when files sent from a source system are received by the target system.<br>Determine whether the mechanisms that the entity employs 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.<br>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<br>NIST SP 800-53, SI-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.05.04.02 A mechanism is employed to notify users when a system interface fails or specific data are rejected. | Obtain an understanding of any mechanisms that the entity employs to notify users when a system interface fails or specific data are rejected through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.<br>See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Perform walk-throughs of the significant business processes. Observe the use of any mechanisms that the entity employs to notify users when a system interface fails or specific data are rejected.<br>Determine whether the mechanisms that the entity employs to notify users when a system interface fails or specific data are rejected are suitably designed and properly implemented based on risk. | NIST SP 800-53, SI-10<br>NIST SP 800-53, SI-11 |
| BP.05.04.03 Appropriate personnel monitor the status of system interfaces processed through job scheduling software.<br>*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 system interfaces involved in the significant business processes through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.<br>See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of system interfaces processed through job scheduling software. | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Observe personnel as they perform procedures for monitoring the status of system interfaces processed through job scheduling software. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned business process application responsibilities. Consider whether the procedures observed are consistent with those documented by the entity.<br>Determine whether appropriate personnel monitor the status of system interfaces processed through job scheduling software.<br>Note: A mechanism may also be employed to notify users when a system 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 system 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure the integrity of interfaced data.<br>Inspect available documentation for a selection of reconciliations performed during the audit period. Consider whether such | NIST SP 800-53, SI-10<br>NIST SP 800-53, SI-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | reconciliations were appropriate and performed in accordance with the entity's policies and procedures for reconciling interfaced data.<br>Determine whether reconciliations of interfaced data from the source and target systems are appropriately performed to verify the integrity of interfaced data.<br>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 System interface processing events are logged to permit management oversight.<br>*Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.06.05.03, AC.05.01.02, and AC.05.01.03* | Obtain an understanding of the entity's processes and methods to monitor the status of system interfaces involved in the significant business processes through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.<br>See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of system interfaces. Identify the event types for logging relevant to system interface processing. Consider whether the event types selected for logging are adequate to support error identification, research, and resolution.<br>Determine whether system interface processing events relevant to the significant business processes are appropriately logged to permit management oversight. | NIST SP 800-53, AU-02<br>NIST SP 800-53, AU-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.05.04.06 Management reviews system interface processing logs on a timely basis.<br>*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 system interfaces involved in the significant business processes through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.<br>See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of system interfaces.<br>Inspect available audit records for a selection of events that occurred during the audit period applicable to the system 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 system interfaces. Consider the appropriateness of the documentation obtained, including any reports produced by log management software, when performing control tests.<br>Determine whether management appropriately reviews system interface processing logs on a timely basis. | NIST SP 800-53, AU-06 |
| BP.05.05 System interface errors are researched and resolved on a timely basis. | | |
| BP.05.05.01 System interface processing errors are researched to identify and remediate their causes. | For the system interfaces involved in the significant business processes, obtain an understanding of the entity's processes and | NIST SP 800-53, SI-10<br>NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | methods to identify and remediate the causes of system interface processing errors through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to identify and remediate the causes of system interface processing errors. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that system interface processing errors are adequately researched to timely identify and remediate their causes.<br>Inspect available documentation for a selection of system 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 system 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.<br>Determine whether system interface processing errors are appropriately researched to identify and remediate their causes.<br>Note: System interface processing logs and audit trails are used to identify and follow up on system interface processing errors. The corrections to system interface processing errors are included in the audit trail. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.05.05.02 System interface processing errors are resolved by correcting data, correcting coding errors in computer programs, or a combination thereof. | For the system interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to identify and remediate the causes of system interface processing errors through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to identify and remediate the causes of system interface processing errors. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that system interface processing errors are properly resolved.<br>Inspect available documentation for a selection of system 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.<br>Determine whether system interface processing errors are properly resolved by correcting data, correcting coding errors in computer programs, or a combination thereof. | NIST SP 800-53, SI-10 |
| BP.05.06 Access to system interface data and user-defined processing of data are appropriately controlled. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.05.06.01 User-defined processing of data prior to system interface processing is appropriately controlled.<br>R*elated 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 system interface processing, as well as the processes and methods by which user-defined processing of data is controlled.<br>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.<br>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.<br>Determine whether user-defined processing of data prior to system interface processing is appropriately controlled.<br>Note: Some system interfaces may require user-defined processing of data prior to system interface processing, whereby a user may establish or modify processing steps to prepare the data for the system interface. This frequently occurs when business process 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. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.05.06.02 The execution of system interfaces is appropriately controlled.<br>*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 system interfaces involved in the significant business processes are executed.<br>Observe the execution of system 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 system interfaces processed through job scheduling software. Consider whether the users involved in the execution of system interfaces involving significant business processes are appropriately authorized to perform such actions.<br>Determine whether the execution of system interfaces is appropriately controlled. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06 |
| BP.05.06.03 Any data files generated during system interface processing are properly secured from unauthorized access, modification, or disposal. | Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identify key data files generated during system interface processing.<br>Obtain an understanding of the entity's processes and methods to secure key data files generated through system 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.<br>Determine whether key data files generated during system interface processing are properly secured from unauthorized access, modification, or disposal. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06<br>NIST SP 800-53, SI-12<br>NIST SP 800-53, SI-15 |
| BP.05.06.04 Any data files generated during system 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, identify key data files generated during system interface processing.<br>Obtain an understanding of the entity's processes and methods to automatically archive or delete key data files generated through | NIST SP 800-53, SI-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | system interface processing from the production environment after processing.<br>Determine whether key data files generated during system interface processing are automatically archived or deleted from the production environment after processing. | |
| BP.05.07 Modifications to system interfaces are appropriately controlled. | | |
| BP.05.07.01 Modifications to the tools and techniques for system interface processing, including any job scheduling software employed, are appropriately controlled.<br>*Related control: BP.05.04.03*<br>*Related control objectives: CM.02.01 and CM.02.02* | For the system interfaces involved in the significant business processes, obtain an understanding of the entity's processes and methods to modify the tools and techniques for system interface processing through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to modify the tools and techniques for system interface processing. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that modifications to the tools and techniques for system interface processing are appropriately controlled.<br>Inspect available documentation for a selection of modifications to the tools and techniques for system 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 | NIST SP 800-53, CM-03 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 system interface processing.<br>Determine whether modifications to the tools and techniques for system 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.<br>*Related control objectives: CM.02.01 and CM.02.02* | For the system 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to change mapping tables. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled.<br>Inspect available documentation for a selection of changes to mapping tables for the system interfaces involved in the significant business processes that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including | NIST SP 800-53, CM-03 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 system interfaces involved in the significant business processes.<br>Determine whether changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled.<br>Note: When mapping tables are used, it is important that controls are designed and implemented to reasonably assure that they 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 controls to reasonably assure that data management systems are properly managed to achieve information processing objectives. | | |
| BP.06.01 Data management system roles and responsibilities are defined and assigned to appropriate personnel. | | |
| BP.06.01.01 Data ownership is appropriately assigned.<br>*Related controls: BP.04.01.01, BP.05.01.01, SM.01.02.02, SM.01.02.03, and SM.01.06.05* | Obtain an understanding of data management system roles and responsibilities, including data ownership, through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as system security and privacy plans. | NIST SP 800-53, PL-02<br>NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Identify the data owners for the relevant information systems. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities.<br>Determine whether data ownership has been appropriately assigned.<br>Note: Data ownership comprises overall responsibility and accountability for managing 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.<br>*Related controls: BP.04.01.02, BP.05.01.02, BP.06.01.03, BP.06.01.04, and BP.06.01.05, SM.01.02.02, SM.01.02.03, SM.01.06.05, and SD.01.01.01* | Obtain an understanding of the responsibilities for requesting, authorizing, and implementing changes to the schema or structure of the database through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether assigned individuals possess appropriate skills and technical expertise to satisfy their responsibilities.<br>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. | NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.06.01.03 Responsibilities for requesting, authorizing, and implementing changes to transaction and master data through the database management software are assigned to appropriate personnel.<br>*Related controls: BP.04.01.02, BP.05.01.02, BP.06.01.02, BP.06.01.04, BP.06.01.05, SM.01.02.02, SM.01.02.03, SM.01.06.05, and SD.01.01.01* | Obtain an understanding of the responsibilities for requesting, authorizing, and implementing changes to transaction and master data through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities.<br>Determine whether the responsibilities for requesting, authorizing, and implementing changes to transaction and master data have been clearly defined and assigned to appropriate personnel.<br>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-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| BP.06.01.04 Responsibilities for database table maintenance are assigned to appropriate personnel.<br>*Related controls: BP.04.01.02, BP.05.01.02, BP.06.01.02, BP.06.01.03, BP.06.01.05, SM.01.02.02, SM.01.02.03, SM.01.06.05, and SD.01.01.01* | Obtain an understanding of the responsibilities for database table maintenance through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities.<br>Determine whether the responsibilities for database table maintenance have been clearly defined and assigned to appropriate personnel.<br>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-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |
| BP.06.01.05 Responsibilities for monitoring changes to the database, including changes to transaction and master data, are assigned to appropriate personnel.<br>*Related controls: BP.04.01.02, BP.05.01.02, BP.06.01.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, SM.01.02.02, SM.01.02.03, SM.01.06.05, and SD.01.01.01* | Obtain an understanding of the responsibilities for monitoring changes to the database through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. | NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether the responsibilities for monitoring changes to the database have been clearly defined and assigned to appropriate personnel.<br>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.06.02 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<br>• consider risk;<br>• address changes to the schema or structure of the database, including any required approvals or authorizations;<br>• address changes to transaction and master data made outside the business process application through the database management software;<br>• address database table maintenance; | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>Through inquiry, inspection, and observation, identify IS 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 IS controls are designed, implemented, and operating effectively. Consider whether<br>• policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external parties, and compliance;<br>• procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be | NIST SP 800-53, AC-01<br>NIST SP 800-53, AT-01<br>NIST SP 800-53, AU-01<br>NIST SP 800-53, CA-01<br>NIST SP 800-53, CM-01<br>NIST SP 800-53, CP-01<br>NIST SP 800-53, IA-01<br>NIST SP 800-53, IR-01<br>NIST SP 800-53, MA-01<br>NIST SP 800-53, MP-01<br>NIST SP 800-53, PE-01<br>NIST SP 800-53, PL-01<br>NIST SP 800-53, PM-01<br>NIST SP 800-53, PS-01<br>NIST SP 800-53, PT-01<br>NIST SP 800-53, RA-01 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| • address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external parties, and compliance;<br>• identify and describe the relevant processes;<br>• consider general and application controls;<br>• consider segregation of duties controls; and<br>• help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities. | held accountable for their actions, and appropriately consider general and application controls and segregation of duties controls; and<br>• policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity's internal control objectives.<br>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.<br>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 IS 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 IS controls. | NIST SP 800-53, SA-01<br>NIST SP 800-53, SC-01<br>NIST SP 800-53, SI-01<br>NIST SP 800-53, SR-01 |
| BP.06.03 Data management systems are designed to organize, maintain, and control access to application data to reasonably assure the completeness, accuracy, and validity of transactions and data. | | |
| BP.06.03.01 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 | NIST SP 800-53, CM-12<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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.<br>Determine whether data management system characteristics, including the schema or structure of the database, 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.<br>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 input controls 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. | NIST SP 800-53, SA-08<br>NIST SP 800-53, SI-10 |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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<br>NIST SP 800-53, SA-05<br>NIST SP 800-53, SI-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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. | |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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.<br>Determine whether transaction data requirements are established and implemented into the database design to help ensure that transaction data are complete, accurate, and valid. | NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-05<br>NIST SP 800-53, SI-10 |
| BP.06.03.04 Null values or invalid values are not accepted in key fields.<br>*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 data input errors that occur when null values or invalid values are entered.<br>Inspect system design documentation, system security and privacy plans, applicable system configuration files, and policies and procedures demonstrating the defined parameters for key fields.<br>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<br>NIST SP 800-53, SA-05<br>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. | 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. | NIST SP 800-53, AC-05<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| *Related controls: SD.01.01.01, SD.01.01.02, SD.01.02.02, and SD.01.03.01* | Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database.<br>Determine whether access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data.<br>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.<br>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.<br>*Related control objective: AC.02.03* | Obtain an understanding of the database schema or structure through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Identify the access paths to data and the processes and methods for controlling data management system administrative functions.<br>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.<br>Determine whether the schema or structure of the database is aligned with management's authorizations for users.<br>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 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 relevant information systems perform to control logical access to sensitive application data through<br>• inquiry of appropriate personnel and<br>• 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. | NIST SP 800-53, AC-23<br>NIST SP 800-53, SC-13<br>NIST SP 800-53, SC-28 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• adequately address the components of the information systems, including related operating systems, business process applications, and data management systems;<br>• employ encryption techniques when appropriate based on risk;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that access to sensitive application data is restricted to authorized individuals for authorized purposes.<br>Determine whether sensitive application data are appropriately controlled and encrypted when appropriate.<br>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.<br>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-05<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>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-05<br>NIST SP 800-53, PM-11<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 were appropriate and performed in accordance with the entity's policies and procedures.<br>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<br>NIST SP 800-53, SI-18 |
| BP.06.04.02 Management periodically reviews master data records to help ensure that master data are consistent between business process application modules and | Obtain an understanding of the entity's processes and methods for periodically reviewing master data records through<br>• inquiry of appropriate personnel and | NIST SP 800-53, SI-10<br>NIST SP 800-53, SI-18 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| among other information systems using the same master data. | • inspection of relevant documentation, such as policies and procedures.<br>See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether the entity's processes and methods for periodically reviewing master data records are designed, implemented, and operating effectively. | |
| 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).<br>*Related control: BP.04.06.01*<br>*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 appropriateness of system-generated evidence when performing control tests. 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.<br>Determine whether data management system roles and corresponding access privileges are appropriately authorized and assigned to users with a valid business purpose (least privilege). | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06 |
| BP.06.05.02 Access control requirements for specialized data management processes used to facilitate interoperability between business process applications and functions | 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 | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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. | 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.<br>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.<br>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. | |
| BP.06.05.03 The data management system logs events associated with changes to business process application data, including master data.<br>*Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, AC.05.01.02, and AC.05.01.03* | Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identify key event types for logging associated with the entity's procedures for data input, processing, and output.<br>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.<br>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-02<br>NIST SP 800-53, AU-03<br>NIST SP 800-53, AU-12 |
| BP.06.06 Modifications to data management systems and data maintained in those systems are appropriately controlled. | | |
| BP.06.06.01 Changes to the schema or structure of each database are appropriately controlled. | Obtain an understanding of the entity's processes and methods to change the schema or structure of databases through<br>• inquiry of appropriate personnel and | NIST SP 800-53, CM-03 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of relevant documentation, such as policies and procedures.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that changes to the schema or structure of the database are appropriately controlled.<br>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.<br>Determine whether changes to the schema or structure of the database are appropriately controlled. | |
| 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<br>• inquiry of appropriate personnel and | NIST SP 800-53, CM-03<br>NIST SP 800-53, SI-19 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of relevant documentation, such as policies and procedures.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• are suitably designed and properly implemented based on risk;<br>• address the entity's approach for de-identification, if applicable; and<br>• reasonably assure that changes to transaction and master data made through the database management software are appropriately controlled.<br>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.<br>Determine whether changes to transaction and master data made through the database management software are appropriately controlled.<br>Note: De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Many datasets 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. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Trained individuals remove PII from datasets 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 each 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 the entity documented.<br>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-03<br>NIST SP 800-53, CM-06 |
| 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<br>• inquiry of appropriate personnel and | NIST SP 800-53, SC-28 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of relevant documentation, such as policies and procedures.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether management regularly performs database table maintenance. | |
| BP.06.06.05 Management employs integrity verification tools to detect unauthorized changes to data management systems and data maintained in these systems.<br>*Related controls: BP.04.07.03 and CM.02.03.03* | 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<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's integrity verification tools, and<br>• 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.<br>See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 | NIST SP 800-53, CM-06<br>NIST SP 800-53, SC-28<br>NIST SP 800-53, SI-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | appropriate personnel and whether appropriate action was taken on a timely basis to address any unauthorized changes detected.<br>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.<br>Determine whether management properly employs integrity verification tools to detect unauthorized changes to data management systems and data maintained in these systems. | |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-26-108633

## 530 FISCAM Framework for Security Management

530.01 The security management (SM) category provides the foundation of a 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 managing risk, developing and implementing effective security policies, assigning and communicating responsibilities, and monitoring the adequacy of the entity's IS controls.

530.02 The FISCAM Framework for Security Management (see table 10) includes seven critical elements:

- SM.01 Management establishes organizational structures, assigns and communicates responsibilities, and develops plans and processes to implement an information security management program for achieving the entity's information security and privacy objectives.
- SM.02 Management demonstrates a commitment to recruit, develop, and retain individuals who are competent and suitable for their information security and privacy positions.
- SM.03 Management holds individuals and external parties accountable for their internal control responsibilities related to the entity's information security management program.
- SM.04 Management identifies, analyzes, and responds to risks, including those related to fraud and improper payments, and significant changes related to the entity's information security management program.
- SM.05 Management designs and implements policies and procedures to mitigate risks to achieving the entity's information security and privacy objectives to acceptable levels.
- SM.06 Management establishes and performs monitoring activities to evaluate the effectiveness of the entity's information security management program.
- SM.07 Management remediates identified internal control deficiencies related to the entity's information security management program on a timely basis.

530.03 Assessing security management controls involves evaluating the entity's efforts to satisfy each of these critical elements. When evaluating management's efforts for each critical element, the auditor considers whether the associated control objectives (shown in table 10), if achieved, will address IS control risk relevant to the engagement objectives. Ineffective security management controls may result in information security management responsibilities being unclear, misunderstood, or improperly implemented. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

**Table 10: FISCAM Framework for Security Management (SM)**

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.01 Management establishes organizational structures, assigns and communicates responsibilities, and develops plans and processes to implement an information security management program for achieving the entity's information security and privacy objectives. | | |
| SM.01.01 Organizational structures are established to enable the entity to plan, execute, control, and assess the information security and privacy functions. | | |
| SM.01.01.01 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as applicable organizational charts, business or organizational unit descriptions, and staffing plans.<br>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-09<br>NIST SP 800-53, SA-02 |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as applicable organizational charts, business or organizational unit descriptions, and staffing plans.<br>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-09<br>NIST SP 800-53, SA-02 |
| 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 | NIST SP 800-53, PL-09<br>NIST SP 800-53, SA-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| independence, authority, expertise, and resources is established and documented. | • inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of information security management program documentation.<br>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-02 |
| SM.01.02.02 Senior management officials are assigned as authorizing officials for information systems and for common controls that organizational systems may inherit.<br>*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, and SM.05.02.01* | Identify the assigned authorizing officials for the relevant information systems 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.<br>Obtain an understanding of the tasks senior management officials perform to satisfy their responsibilities as authorizing officials through<br>• inquiry of appropriate personnel, including the authorizing officials, and<br>• inspection of information security management program documentation. | NIST SP 800-53, CA-06<br>NIST SP 800-53, PM-10<br>NIST SP 800-53, SA-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether senior management officials have been assigned as authorizing officials for the relevant information systems and the common controls that such systems inherit.<br>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.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of information security management program documentation.<br>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.<br>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 | NIST SP 800-53, PM-03<br>NIST SP 800-53, PM-23<br>NIST SP 800-53, PM-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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. | |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of privacy management program documentation.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of privacy management program documentation.<br>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-03<br>NIST SP 800-53, PM-23<br>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 | Obtain an understanding of the responsibilities of the chief risk officer, or senior accountable official for risk management, through | NIST SP 800-53, PM-29 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| processes with strategic, operational, and budgetary planning processes and to reasonably assure consistent risk management practices across the organization. | • inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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. | |
| SM.01.03 Planning documentation related to the entity's information security management program is developed and maintained. | | |
| 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<br>• approval by a senior official with responsibility and accountability for the risk being incurred;<br>• requirements of the entity's information security management program, including the coordination among organizational entities responsible for information security;<br>• descriptions of the program management controls and common controls for meeting requirements; and<br>• assignment of roles and responsibilities for the | 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<br>• inquiry of appropriate personnel, including the senior official responsible for the plan, and<br>• inspection of relevant documentation.<br>Inspect the entity-level information security management program plan. Consider whether the plan<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s);<br>• is aligned with the entity-level strategic plan;<br>• includes required information in accordance with authoritative criteria; and<br>• is adequate to guide the implementation of the entity's information security management program and achieve the entity's information security objectives.<br>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. | NIST SP 800-53, PM-01<br>NIST SP 800-53, PM-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| information security management program. | Throughout the engagement, determine whether the entity-level information security management program plan has been implemented. | |
| SM.01.03.02 Management develops, documents, and periodically reviews and updates an entity-level privacy management program plan. This program plan includes<br>• approval by a senior official with responsibility and accountability for the risk being incurred;<br>• descriptions of the privacy management program strategic goals and objectives;<br>• descriptions of the requirements of a privacy management program, including the coordination among organizational entities responsible for information security;<br>• descriptions of the privacy controls for meeting those requirements; and<br>• assignment of roles and responsibilities for the privacy management program. | 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<br>• inquiry of appropriate personnel, including the senior official responsible for the plan, and<br>• inspection of relevant documentation.<br>Inspect the entity-level privacy management program plan. Consider whether the plan<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s);<br>• includes required information in accordance with authoritative criteria; and<br>• is adequate to guide the implementation of the entity's privacy management program and achieve the entity's privacy objectives.<br>Determine whether the entity-level privacy management program plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, determine whether the entity-level privacy management program plan has been implemented. | NIST SP 800-53, PM-18<br>NIST SP 800-53, PM-19<br>NIST SP 800-53, PM-20<br>NIST SP 800-53, PM-21<br>NIST SP 800-53, PM-22<br>NIST SP 800-53, PM-25<br>NIST SP 800-53, PM-26<br>NIST SP 800-53, PM-27<br>NIST SP 800-53, PT-02<br>NIST SP 800-53, PT-03 |
| SM.01.04 System development life cycle processes that incorporate information security and privacy considerations are established. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.01.04.01 System development life cycle processes are developed, documented, and periodically reviewed and updated.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect documentation demonstrating the design and implementation of the entity's system development life cycle processes. Consider whether the processes<br>• identify roles and responsibilities;<br>• are integrated with the entity's risk management processes;<br>• 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;<br>• incorporate operations security controls;<br>• 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;<br>• facilitate tracing of source code to design specifications and functional requirements during testing;<br>• establish the standards, tools, and tool configurations used in source code development;<br>• provide for validation, verification, and flaw remediation used in source code development; | NIST SP 800-53, SA-03<br>NIST SP 800-53, SA-08<br>NIST SP 800-53, SA-10<br>NIST SP 800-53, SA-11<br>NIST SP 800-53, SA-15<br>NIST SP 800-53, SA-17<br>NIST SP 800-53, SA-22<br>NIST SP 800-53, SC-04<br>NIST SP 800-53, SC-31<br>NIST SP 800-53, SC-36<br>NIST SP 800-53, SC-38<br>NIST SP 800-53, SI-23<br>NIST SP 800-53, SR-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • facilitate replacing or providing alternative support for system components that the developer, vendor, or manufacturer no longer supports;<br>• establish system documentation requirements;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• are adequate to provide a foundation for the successful development, implementation, and operation of entity information systems.<br>Determine whether the system development life cycle processes have been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, consider whether the system development life cycle processes have been implemented.<br>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 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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the enterprise architecture of the entity. Consider whether the enterprise architecture<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s);<br>• is integrated with the entity's risk management processes; and<br>• adequately addresses security and privacy considerations for the entity.<br>Determine whether the enterprise architecture has been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, determine whether the enterprise architecture has been implemented.<br>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 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. | NIST SP 800-53, PM-07 |
| SM.01.05 An incident response program is established. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.01.05.01 The entity has developed and documented and periodically reviews and updates an entity-level incident response plan that<br>• provides the entity with a road map for implementing its incident response capability;<br>• describes the structure and organization of the incident response capability;<br>• provides a high-level approach for how the incident response capability fits into the entity's organizational structure;<br>• meets the unique requirements of the entity, which relate to mission, size, structure, and functions;<br>• defines reportable incidents;<br>• provides metrics for measuring the incident response capability within the entity;<br>• defines the resources and management support needed to effectively maintain and mature an incident response capability;<br>• addresses the sharing of incident information; | 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<br>• inquiry of appropriate personnel, including the senior officials responsible for the plan, and<br>• inspection of relevant documentation.<br>Inspect the entity-level incident response plan. Consider whether the plan<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s);<br>• includes required information in accordance with authoritative criteria; and<br>• is adequate to guide the implementation of the entity's incident response program and achieve the entity's information security and privacy objectives.<br>Determine whether the entity-level incident response plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, determine whether the entity-level incident response plan has been implemented. | NIST SP 800-53, IR-08<br>NIST SP 800-53, SR-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| • is reviewed and approved by management; and<br>• explicitly designates responsibility for incident response to appropriate personnel.<br>*Related controls: SM.04.01.01, SM.04.01.02, and 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<br>• incident response training to system users consistent with their assigned roles and responsibilities;<br>• documented testing of the entity's incident response capabilities and follow-up on findings;<br>• appropriate incident-handling activities supported by automated mechanisms and incident response team members with the necessary knowledge, skills, and abilities;<br>• appropriate incident-monitoring mechanisms to track and document incidents; | Obtain an understanding of the entity's incident response program through<br>• inquiry of appropriate personnel, including the senior officials responsible for the plan, and<br>• inspection of relevant documentation.<br>Inspect documentation for the entity's incident response program. Consider whether<br>• 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;<br>• the entity tests its incident response capabilities to determine their effectiveness and identifies potential weaknesses or deficiencies for follow-up;<br>• 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; | NIST SP 800-53, IR-02<br>NIST SP 800-53, IR-03<br>NIST SP 800-53, IR-04<br>NIST SP 800-53, IR-05<br>NIST SP 800-53, IR-06<br>NIST SP 800-53, IR-07<br>NIST SP 800-53, PE-20<br>NIST SP 800-53, PM-15<br>NIST SP 800-53, SC-05<br>NIST SP 800-53, SC-06<br>NIST SP 800-53, SC-26<br>NIST SP 800-53, SC-30<br>NIST SP 800-53, SC-40<br>NIST SP 800-53, SC-42<br>NIST SP 800-53, SC-44<br>NIST SP 800-53, SC-48<br>NIST SP 800-53, SI-05<br>NIST SP 800-53, SR-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| • a means for reporting incident information;<br>• appropriate incident response assistance;<br>• a process for gathering forensic evidence and conducting forensic analysis;<br>• links to other relevant security and privacy groups and associations;<br>• monitoring, generating, and disseminating security alerts, advisories, and directives, as applicable; and<br>• protection against denial-of-service attacks.<br>*Related controls: SM.02.03.01, SM.02.03.02, and AC.05.02.04* | • incident-monitoring mechanisms maintain records about each incident, the status of the incident, and other pertinent information necessary for forensic analysis, as well as the evaluation of incident details, trends, and handling activities;<br>• incidents are reported in accordance with relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, and guidelines;<br>• incident information is used to inform risk assessments or control assessments;<br>• incident response support resources are adequate;<br>• forensic evidence is gathered and forensic analysis is performed when appropriate;<br>• there are links to other relevant security and privacy groups and associations;<br>• security alerts, advisories, and directives are monitored, generated, and disseminated, as applicable;<br>• techniques are employed to prevent adversarial attacks based on risks; and<br>• denial-of-service attacks can be limited or eliminated.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, including management's criteria for designating information systems as major information systems.<br>Inspect the entity-level inventory of major information systems. Consider whether<br>• the relevant information systems are appropriately included in the inventory,<br>• management's criteria for designating information systems as major information systems are suitable and consistently applied, and<br>• the inventory has been recently reviewed and updated and is complete. | NIST SP 800-53, PM-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether the entity-level inventory of major information systems has been appropriately documented, periodically reviewed and updated, and properly approved. | |
| 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.<br>*Related control: SM.04.02.01* | Obtain an understanding of the entity-level process for selecting and implementing security controls for major applications and general support systems through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect the control baseline for each relevant information system. Consider whether each control baseline has been selected and tailored based on<br>• the impact level of the corresponding system and<br>• the entity-level process for selecting and implementing security controls.<br>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.<br>Throughout the engagement, determine whether the security controls included in the control baselines for relevant information systems are designed, implemented, and operating effectively.<br>Note: Control baselines are predefined sets of controls that represent a starting point for protecting information and information systems. Subsequent tailoring of selected control baselines allows for | NIST SP 800-53, PL-10<br>NIST SP 800-53, PL-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 (Public Law 113-283) (FISMA) and the Privacy Act of 1974 (codified, as amended, at 5 U.S.C. § 552a) (PRIVACT).<br>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 categorization and is described in Federal Information Processing Standard (FIPS) 199. Security categorization of federal information and information systems, as required by FIPS 199, is the first step in the risk management process.<br>After 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 information security objectives are low. A moderate-impact system is a system in which at least one of the information security objectives is moderate and no information security objective is high. Finally, a high-impact system is a system in which at least one information security objective is high. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the system-level CONOPS documents for each relevant information system. Consider whether CONOPS documents<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• are adequate to describe the operation of the information systems from the perspective of information security and privacy.<br>Determine whether the system-level CONOPS documents for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved. | NIST SP 800-53, PL-07 |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the system-level security and privacy architectures for each relevant information system. Consider whether the security and privacy architectures<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); | NIST SP 800-53, PL-08<br>NIST SP 800-53, PM-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • are consistent with the enterprise architecture;<br>• are integrated with the risk management and system development life cycle processes; and<br>• are adequate to describe the structure and behavior of the system's security and privacy processes.<br>Determine whether the system-level security and privacy architectures for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, determine whether the system-level security and privacy architectures for relevant information systems have been implemented.<br>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 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.<br>*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, 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, including the entity-level inventory of major information systems.<br>Inspect the system security and privacy plans for each relevant information system. Consider whether the plans | NIST SP 800-53, AC-14<br>NIST SP 800-53, PL-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s);<br>• include required information in accordance with authoritative criteria; and<br>• 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.<br>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.<br>Throughout the engagement, determine whether the system security and privacy plans for relevant information systems have been implemented.<br>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 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 subsequently assessing the effectiveness of the control.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the system-level supply chain risk management plan for each relevant information system. Consider whether the plans<br>• have been recently reviewed and updated, as appropriate;<br>• include required information in accordance with authoritative criteria; and<br>• are adequate to identify, assess, and manage supply chain risks relevant to the system.<br>Determine whether the system-level supply chain risk management plans for relevant information systems are effectively designed, have been appropriately documented, and are periodically reviewed and updated.<br>Throughout the engagement, determine whether the system-level supply chain risk management plans for relevant information systems have been implemented.<br>Note: System-level supply chain risk management plans can be stand-alone plans or part of system security and privacy plans. | NIST SP 800-53, SR-02<br>NIST SP 800-53, SR-03 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.02 Management demonstrates a commitment to recruit, develop, and retain individuals who are competent and suitable for their information security and privacy positions. | | |
| SM.02.01 Expectations of competence and suitability for key information security and privacy roles are established and communicated. | | |
| SM.02.01.01 A security and privacy workforce development and improvement program is established and documented.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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.<br>Determine whether the information security and privacy roles and responsibilities, as well as position risk designation, are accurately identified and included in position descriptions.<br>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, timing, and extent of the entity's screening activities. | NIST SP 800-53, PS-02<br>NIST SP 800-53, PS-09 |
| SM.02.01.03 Incompatible duties are included in position descriptions.<br>*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.<br>Determine whether incompatible duties are accurately identified and included in position descriptions. | NIST SP 800-53, AC-05 |
| SM.02.02 Screening activities are completed, and access agreements are signed prior to access authorization. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether references for prospective employees are contacted and background investigations and agency checks are properly performed based on position risk designations.<br>Note: Position risk designations inform the nature, timing, and extent of screening activities performed by the entity, including contacting references and performing background investigations and agency checks. | NIST SP 800-53, PS-02<br>NIST SP 800-53, PS-03<br>NIST SP 800-53, SA-21 |
| SM.02.02.02 Rescreening activities, including periodic reinvestigations, are performed based on position risk designations as required by relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria. | Obtain an understanding of the entity's processes and methods for performing rescreening activities, including periodic reinvestigations, through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process. | NIST SP 800-53, PS-02<br>NIST SP 800-53, PS-03<br>NIST SP 800-53, SA-21 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether rescreening activities, including periodic reinvestigations, are performed based on position risk designations as required by relevant provisions in 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.<br>*Related controls: SM.02.03.03, AC.02.03.03, and CM.01.01.04* | Obtain an understanding of the entity's process and methods for obtaining signed access agreements from individuals through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect available documentation for a selection of accounts that were created during the audit period.<br>Determine whether the entity obtains signed access agreements prior to granting access to information and information systems.<br>Note: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. | NIST SP 800-53, CM-10<br>NIST SP 800-53, CM-11<br>NIST SP 800-53, MP-07<br>NIST SP 800-53, PL-04<br>NIST SP 800-53, PS-06 |
| 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 program that incorporates lessons learned from internal or external security incidents or | Obtain an understanding of the entity's processes and methods for establishing, documenting, and periodically reviewing and updating | NIST SP 800-53, AT-02<br>NIST SP 800-53, AT-04<br>NIST SP 800-53, PM-14 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*Related controls: BP.04.03.12, SM.01.05.02, SM.02.01.01, and SM.02.03.02* | information security and privacy literacy training and awareness techniques through<br>• inquiry of appropriate personnel, including any senior officials responsible for the information security and privacy literacy training and awareness program, and<br>• inspection of relevant documentation, such as literacy training course materials demonstrating the incorporation of lessons learned from internal or external security incidents or breaches.<br>Inspect documentation for the information security and privacy literacy training and awareness program. Consider whether<br>• 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;<br>• lessons learned from internal or external security incidents or breaches are incorporated into literacy training course materials and awareness techniques;<br>• mandatory training courses are identified and communicated to information system users as a condition of system access, as applicable; and<br>• management monitors and maintains records of the completion status of applicable mandatory training courses for information system users.<br>Determine whether the information security and privacy literacy training and awareness program is effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Throughout the engagement, determine whether the information security and privacy literacy training and awareness program has been implemented. | |
| 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.<br>*Related controls: BP.04.03.12, SM.01.05.02, 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<br>• inquiry of appropriate personnel, including any senior officials responsible for the role-based information security and privacy training program, and<br>• 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.<br>Inspect documentation for the role-based information security and privacy training program. Consider whether<br>• 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;<br>• lessons learned from internal or external security incidents or breaches are incorporated into role-based training content;<br>• mandatory training courses are identified and communicated to information system users as a condition of system or role-based access, as applicable; and<br>• management monitors and maintains records of the completion status of applicable mandatory training courses for information system users. | NIST SP 800-53, AT-03<br>NIST SP 800-53, AT-04<br>NIST SP 800-53, PM-14 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether the role-based information security and privacy training program is effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses.<br>Throughout the engagement, determine whether the role-based information security and privacy training program has been implemented. | |
| 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.<br>*Related controls: BP.04.03.12, SM.02.02.03, AC.02.03.03, and CM.01.01.04* | 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<br>• inquiry of appropriate personnel, including information system users, and<br>• inspection of relevant documentation, including access agreements.<br>Inspect available documentation for a selection of accounts that were created during the audit period.<br>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<br>NIST SP 800-53, CM-11<br>NIST SP 800-53, MP-07<br>NIST SP 800-53, PL-04<br>NIST SP 800-53, PS-06 |
| 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<br>• inquiry of appropriate personnel, | NIST SP 800-53, AT-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• results of employee training, including employee feedback, are retained and evaluated by personnel with the authority to take or delegate appropriate actions, and | NIST SP 800-53, AT-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • actions, such as updates to course materials or instruction methods, are taken in response to evaluations of training, as appropriate.<br>Determine whether the results of employee training are evaluated by appropriate personnel and appropriate actions are taken. | |
| 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:<br>• review ongoing need for logical and physical access authorizations;<br>• modify, disable, or remove accounts when associated access privileges or accounts are no longer needed;<br>• collect property, equipment, and physical access authorization credentials;<br>• conduct exit interviews;<br>• escort terminated employees out of the entity's facilities; and<br>• identify the period during which nondisclosure requirements remain in effect for terminated employees.<br>*Related control: AC.02.03.04* | Obtain an understanding of the entity's processes and methods for completing transfer and termination activities through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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.<br>Consider whether<br>• logical and physical access authorizations for transferred personnel were reviewed to determine whether an ongoing need for such access exists;<br>• accounts were timely modified, disabled, or removed when associated access privileges or accounts are no longer needed due to transfer or termination;<br>• property, equipment, and physical access authorization credentials were timely collected;<br>• exit interviews were conducted;<br>• terminated employees were escorted out of the entity's facilities; and<br>• the period during which nondisclosure requirements remain in effect was identified for terminated employees. | NIST SP 800-53, PS-04<br>NIST SP 800-53, PS-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 appropriateness 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.<br>Determine whether appropriate transfer and termination activities are completed on a timely basis. | |
| SM.03 Management holds individuals and external parties accountable for their internal control responsibilities related to the entity's information security management program. | | |
| SM.03.01 Information security and privacy policies and procedures are enforced. | | |
| SM.03.01.01 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<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect relevant documentation for a selection of IT management personnel who have recently been subject to the entity's formal sanctions process.<br>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-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.03.02 External parties are held accountable for their assigned internal control responsibilities related to the entity's information security and privacy objectives. | | |
| SM.03.02.01 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.<br>*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<br>• inquiry of appropriate personnel and<br>• 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.<br>Inspect the interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, or other exchange agreements for the relevant information systems. Consider whether such documentation<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s); and<br>• is adequate to reasonably assure the protection of controlled unclassified information that is processed, stored, or transmitted on external systems.<br>Inspect the contracts executed between the entity and external parties for the acquisition of information systems, information system components, or information system services. Consider whether the | NIST SP 800-53, AC-20<br>NIST SP 800-53, AC-21<br>NIST SP 800-53, CA-03<br>NIST SP 800-53, PM-17<br>NIST SP 800-53, PS-07<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | contracts include, either explicitly or by reference to an exchange agreement, the following requirements, descriptions, and criteria:<br>• security and privacy functional requirements and related controls;<br>• strength of mechanism requirements;<br>• security and privacy assurance requirements;<br>• security and privacy documentation requirements and related controls;<br>• descriptions of the system development environment and the environment in which the system is intended to operate;<br>• roles and responsibilities for information security, privacy, and supply chain risk management; and<br>• acceptance criteria.<br>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.<br>Throughout the engagement, determine whether the terms and conditions for the protection of controlled unclassified information have been implemented.<br>Note: Entities may incorporate provisions related to exchange agreements into formal contracts, especially for system 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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.03.02.02 An entity-level process for assessing the effectiveness of information security and privacy controls that external parties design, implement, or operate is established and implemented.<br>*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 parties design, implement, or operate through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures,<br>• inspection of relevant service organization reports, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Through inquiry, inspection, and observation, identify IS controls relevant to the significant business processes and areas of audit interest that external parties design, implement, or operate. Consider the control baseline for each relevant information system when identifying such controls. See also SM.01.05.01.<br>Inspect relevant documentation related to the entity's assessment of information security and privacy controls that external parties design, implement, and operate. Consider whether the entity's assessment<br>• is based on current information;<br>• addresses any controls the entity designs, implements, or operates that are necessary to achieve the external parties' control objectives; and<br>• is adequate to support the entity's conclusions on the effectiveness of information security and privacy controls that external parties design, implement, or operate.<br>Determine whether the entity-level process for assessing the effectiveness of information security and privacy controls that external parties design, implement, or operate is effectively designed and implemented to achieve the entity's information security and privacy | NIST SP 800-53, CA-01<br>NIST SP 800-53, CA-06<br>NIST SP 800-53, PS-07<br>NIST SP 800-53, SA-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | objectives and hold external parties accountable for their assigned internal control responsibilities.<br>Throughout the engagement, determine whether IS controls relevant to the significant business processes and areas of audit interest that external parties design, implement, or operate are effective.<br>See also section 330 for guidance on using service organization reports.<br>Note: 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.<br>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 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.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 party 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 party through<br>• inquiry of appropriate personnel, such as authorizing officials and information system owners;<br>• inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>See also SM.05.02.01, SM.05.02.02, and SM.05.02.03.<br>If applicable, determine whether the interorganizational joint authorization process for systems with multiple authorizing officials and at least one authorizing official from an external party is effectively designed and implemented to achieve the entity's information security and privacy objectives and hold external parties accountable for their assigned internal control responsibilities. | NIST SP 800-53, CA-06<br>NIST SP 800-53, SA-09 |
| SM.03.03 Complementary user-entity controls related to external parties are identified, implemented, and operating effectively. | | |
| SM.03.03.01 Complementary user-entity controls related to external parties are identified, implemented, and operating effectively.<br>*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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and | NIST 800-53, SA-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of other relevant documentation, such as service organization reports and internal control testing results.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether management identified all relevant complementary user-entity controls from the external party'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.<br>Perform tests of effectiveness over relevant complementary user-entity controls, as appropriate.<br>Inspect the external party's service organization report and consider whether relevant controls at the external party are appropriately designed, implemented, and operating effectively.<br>Determine whether the complementary user-entity controls related to external parties are identified, implemented, and operating effectively.<br>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. | |
| SM.04 Management identifies, analyzes, and responds to risks, including those related to fraud and improper payments, and significant changes related to the entity's information security management program. | | |
| SM.04.01 Risk management strategies are developed, documented, and maintained. | | |
| SM.04.01.01 An entity-level risk management strategy for information security and privacy | Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating the | NIST SP 800-53, PE-23 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*Related controls: SM.01.05.01, AC.04.01.01, CM.03.01.01, and CM.03.02.01* | entity-level risk management strategy for information security and privacy risks through<br>• inquiry of appropriate personnel, including the senior officials responsible for the strategy, and<br>• inspection of relevant documentation.<br>Inspect the entity-level risk management strategy for information security and privacy risks. Consider whether the strategy<br>• has been recently reviewed and updated, as appropriate;<br>• includes required information in accordance with authoritative criteria;<br>• demonstrates that the entity has determined assumptions and constraints affecting risk assessments, organizational risk tolerance, and priorities to guide and inform risk-based decisions; and<br>• 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.<br>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.<br>Throughout the engagement, determine whether the entity-level risk management strategy has been implemented. | NIST SP 800-53, PM-09<br>NIST SP 800-53, PM-10<br>NIST SP 800-53, PM-12<br>NIST SP 800-53, PM-16<br>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 assessments and monitoring, as well as the process for correlating, analyzing, and responding to control assessment and | 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<br>• inquiry of appropriate personnel, including the senior officials responsible for the strategy, and | NIST SP 800-53, PM-14<br>NIST SP 800-53, PM-31 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| monitoring results, is developed, documented, and periodically reviewed and updated.<br>*Related controls: SM.01.05.01, SM.06.01.01, CM.03.01.01, and CM.03.02.01* | • inspection of relevant documentation.<br>Inspect the entity-level continuous monitoring strategy. Consider whether the strategy<br>• has been recently reviewed and updated, as appropriate;<br>• includes required information in accordance with authoritative criteria;<br>• establishes the metrics, frequency, and type(s) of control assessments and the monitoring to be performed;<br>• defines the process for correlating, analyzing, and responding to control assessment and monitoring results; and<br>• 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.<br>Determine whether the entity-level continuous monitoring strategy is effectively designed, has been appropriately documented, and is periodically reviewed and updated.<br>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<br>• inquiry of appropriate personnel, including the senior officials responsible for the strategy, and<br>• inspection of relevant documentation.<br>Inspect the entity-level supply chain risk management strategy. Consider whether the plan | NIST SP 800-53, PM-30<br>NIST SP 800-53, SR-03<br>NIST SP 800-53, SR-04<br>NIST SP 800-53, SR-05<br>NIST SP 800-53, SR-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • has been recently reviewed and updated, as appropriate;<br>• is aligned with the entity-level risk management strategy for information security and privacy risks;<br>• includes required information in accordance with authoritative criteria;<br>• addresses the development, acquisition, maintenance, and disposal of systems, system components, and system services; and<br>• is adequate for prioritizing the entity's implementation of activities to assess, respond to, and monitor supply chain risks.<br>Determine whether the entity-level supply chain risk management strategy is effectively designed, has been appropriately documented, and is periodically reviewed and updated.<br>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.<br>*Related controls: SM.01.06.02 and SM.01.06.05* | 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<br>• inquiry of appropriate personnel, including authorizing officials responsible for approving security categorization decisions;<br>• inspection of relevant documentation, including system security and privacy plans;<br>• inspection of relevant policies and procedures; and | NIST SP 800-53, RA-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect the system security and privacy plans for each relevant information system. Consider whether the plans<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• 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.<br>Determine whether the security categorization for each relevant information system 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<br>• identify threats to and vulnerabilities in the system;<br>• determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it | Obtain an understanding of the entity's processes and methods for conducting and documenting risk assessments through<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• 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.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, RA-03<br>NIST SP 800-53, RA-06<br>NIST SP 800-53, RA-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| processes, stores, or transmits, and any related information; and<br>• determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information (PII).<br>*Related controls: SM.04.02.03, SM.04.02.04, and SM.04.02.05* | Inspect the risk assessments relevant to the significant business processes and areas of audit interest, including any risk assessments conducted and documented for the relevant information systems. Consider whether the risk assessments<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s);<br>• identify threats to and vulnerabilities in the respective systems;<br>• 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<br>• determine the likelihood and impact of adverse effects on individuals arising from the processing of PII.<br>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.<br>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.<br>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, timing, and extent of further audit procedures. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*Related controls: SM.04.02.02, SM.04.02.04, and CM.03.01.02* | Inspect risk assessment reports, security and privacy plans, or other entity-defined documents detailing the results of risk assessments conducted and documented for the relevant information systems.<br>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-08<br>NIST SP 800-53, RA-05 |
| SM.04.02.04 Risk assessment results, including validation and mitigation, are documented, analyzed, and approved by management.<br>*Related controls: SM.04.02.03, SM.04.02.02, and SM.04.02.06* | Obtain an understanding of the entity's processes and methods for analyzing and responding to risks through<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation, including risk response documentation, demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 relevant information systems. Consider whether the risk response documentation<br>• has been approved by the appropriate senior official(s) and<br>• is adequate to demonstrate that risks identified through the risk assessment process have been appropriately analyzed as part of the risk response process. | NIST SP 800-53, RA-03<br>NIST SP 800-53, RA-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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. | |
| 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.<br>*Related control: SM.04.02.02* | Inspect risk assessment reports, security and privacy plans, or other entity-defined documents detailing the results of risk assessments conducted and documented for the relevant information systems.<br>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.<br>Determine whether the frequency of the entity's reassessment of risks is appropriate. | NIST SP 800-53, RA-03 |
| SM.04.02.06 Findings from risk assessments, security assessments, privacy assessments, monitoring activities, and audits are addressed within appropriate time frames in accordance with organizational risk tolerance.<br>*Related control: SM.04.02.04* | Inspect documentation detailing the status of actions taken or in progress to address findings from risk assessments, security assessments, privacy assessments, monitoring activities, and audits, which are relevant to the significant business processes and areas of audit interest.<br>Determine whether relevant findings from risk assessments, security assessments, privacy assessments, monitoring activities, and audits are addressed within appropriate time frames in accordance with organizational risk tolerance. | NIST SP 800-53, RA-07 |
| SM.05 Management designs and implements policies and procedures to mitigate risks to achieving the entity's information security and privacy objectives to acceptable levels. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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 and system levels and are approved by management. They also appropriately<br>• consider risk;<br>• address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as external parties, and compliance;<br>• describe the process;<br>• consider general and application controls;<br>• consider segregation of duties controls; and<br>• ensure that users can be held accountable for their actions.<br>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. | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, including the entity's policies and procedures relevant to the significant business processes and areas of audit interest.<br>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 security and privacy policies and procedures are designed, implemented, and operating effectively.<br>Through inquiry, inspection, and observation, identify IS 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 IS controls are designed, implemented, and operating effectively. Consider whether<br>• policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external parties, and compliance;<br>• 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 general and application controls and segregation of duties controls; and | NIST SP 800-53, AC-01<br>NIST SP 800-53, AT-01<br>NIST SP 800-53, AU-01<br>NIST SP 800-53, CA-01<br>NIST SP 800-53, CM-01<br>NIST SP 800-53, CP-01<br>NIST SP 800-53, IA-01<br>NIST SP 800-53, IR-01<br>NIST SP 800-53, MA-01<br>NIST SP 800-53, MP-01<br>NIST SP 800-53, PE-01<br>NIST SP 800-53, PL-01<br>NIST SP 800-53, PM-01<br>NIST SP 800-53, PS-01<br>NIST SP 800-53, PT-01<br>NIST SP 800-53, RA-01<br>NIST SP 800-53, SA-01<br>NIST SP 800-53, SC-01<br>NIST SP 800-53, SI-01<br>NIST SP 800-53, SR-01 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity's internal control objectives.<br>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 IS 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 the implementation and operating effectiveness of IS 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.<br>*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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures;<br>• inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the relevant information systems.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, CA-06<br>NIST SP 800-53, PM-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect the authorization packages for each relevant information system. Consider whether<br>• the information contained in the authorization package is updated on an ongoing basis through comprehensive continuous monitoring activities,<br>• authorization decisions flow logically from the supporting rationale documented within the authorization package,<br>• authorization decisions are made on a timely basis in accordance with the entity-defined frequency, and<br>• the entity-defined frequency for reauthorizations is appropriate.<br>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.<br>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.<br>The authorizing official reviews the components of the authorization package to make an authorization decision to grant or deny authorization to operate (ATO) for the system. For common controls, the authorization decision indicates to the common control provider, and to the system owners of inheriting systems, whether the common controls are authorized to be provided. The authorization decision is included with the authorization package. The authorizing official establishes an authorization termination date or authorization | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | frequency when the system is operating under an ongoing authorization.<br>Under ongoing authorization, the authorizing official reviews continuous monitoring information to conduct ongoing risk determination and risk acceptance activities at the specified authorization frequency. If the risk does not remain acceptable, the authorizing official indicates that the risk is no longer acceptable and requires further risk response or a full denial of the authorization. The Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) conducts reviews of cloud services that are used throughout the government. JAB issues a provisional authority to operate (P-ATO) for cloud services that pass its review. Although provisional authorization is given through FedRAMP, JAB does not have the authority to issue an ATO for a system at the entity—including common controls. However, the entity's authorizing official may use the P-ATO documentation package from FedRAMP and accept that endorsement for the entity-owned system. | |
| 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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the relevant information systems.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, CA-06<br>NIST SP 800-53, PM-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect the authorization packages for each of the relevant information systems. Consider whether<br>• the information contained in the authorization package is updated on an ongoing basis through comprehensive continuous monitoring activities,<br>• authorization decisions flow logically from the supporting rationale documented within the authorization package,<br>• authorization decisions are made on a timely basis in accordance with the entity-defined frequency, and<br>• the entity-defined frequency for reauthorizations is appropriate.<br>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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the relevant information systems.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, CA-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect the authorization packages for each of the relevant information systems. Consider whether each authorization package<br>• includes required information in accordance with authoritative criteria and<br>• is adequately documented to support the authorization decisions expressed therein.<br>Determine whether the authorization package for each relevant information system includes the authorization to operate, executive summary, system security and privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.<br>Note: Reviewing the authorization packages may be useful in assessing risk and determining the nature, timing, and extent of further audit procedures. | |
| 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.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. | Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level continuous monitoring strategies through<br>• inquiry of appropriate personnel, including the senior official(s) responsible for the strategies, and<br>• inspection of relevant documentation.<br>Inspect the system-level continuous monitoring strategy for each relevant information system. Consider whether each of the strategies<br>• has been recently reviewed and updated, as appropriate; | NIST SP 800-53, CA-07<br>NIST SP 800-53, PM-31 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| *Related controls: SM.04.01.02, CM.03.01.01, and CM.03.02.01* | • is aligned with the entity-level continuous monitoring strategy;<br>• includes required information in accordance with authoritative criteria;<br>• establishes the metrics, frequency, and type(s) of control assessments and monitoring to be performed;<br>• defines the process for correlating, analyzing, and responding to control assessment and monitoring results; and<br>• is adequate for prioritizing the entity's implementation of activities to facilitate ongoing awareness of the security and privacy posture of the information system.<br>Determine whether the system-level continuous monitoring strategy for each of the relevant information systems is effectively designed, has been appropriately documented, and is periodically reviewed and updated.<br>Throughout the engagement, determine whether the system-level continuous monitoring strategy for each of the relevant information systems has been implemented. | |
| SM.06.01.02 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.<br>*Related control: SM.06.01.03* | Obtain an understanding of management's process for performing system-level control monitoring activities to assess controls and identify risks through<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process, such as relevant system-level control monitoring documentation, | NIST SP 800-53, CA-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | the system-level continuous monitoring strategy, and the entity-level continuous monitoring strategy.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect relevant system-level control monitoring documentation for each relevant information system. Consider whether<br>• system-level control monitoring activities are implemented in accordance with the system-level continuous monitoring strategy and<br>• system-level control monitoring documentation is adequate to facilitate ongoing awareness of the security and privacy posture of the information system.<br>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.<br>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 auditors, inspectors general, or other assessors. Reviewing system-level control monitoring documentation may be useful in assessing risk and determining the nature, timing, and extent of further audit procedures. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SM.06.01.03 Assessors with appropriate skills and technical expertise periodically perform security and privacy control assessments.<br>*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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process, such as relevant control assessment plans and reports.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect relevant control assessment plans and reports for each relevant information system. Consider whether<br>• the security and privacy control assessments were performed recently and used current information,<br>• the control assessment plan was reviewed and approved by the authorizing official prior to performing the assessment,<br>• the security and privacy control assessments were performed by assessors with sufficient objectivity, appropriate skills and technical expertise, and<br>• the control assessment report is adequate to facilitate communication of the security and privacy posture of the information system.<br>Determine whether security and privacy control assessments for the relevant information system are properly performed on a periodic basis by assessors with appropriate skills and technical expertise.<br>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 FISMA (codified, in part, at 44 U.S.C. § 3554), system design and | NIST SP 800-53, CA-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>*Related control: SM.06.01.03* | Inspect relevant control assessment reports for each relevant information system and inquire with appropriate personnel to obtain an understanding of how control assessment results are documented and shared. Consider whether<br>• 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<br>• communication mechanisms exist to facilitate the sharing of control assessment reports with appropriate personnel.<br>Determine whether control assessment reports are shared with appropriate personnel and document the assessment results in sufficient detail. | NIST SP 800-53, CA-02 |
| 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<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the process.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, PM-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect the performance measures and compliance metrics for information security and privacy functions applicable to the relevant information systems. Consider whether<br>• management periodically evaluates the performance measures and compliance metrics and<br>• management uses the performance measures and compliance metrics appropriately to measure the effectiveness or efficiency of the information security and privacy functions.<br>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 remediating 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.<br>*Related controls: SM.07.01.02 and SM.07.01.03* | Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating plans of action and milestones through<br>• inquiry of appropriate personnel, including the authorizing officials for relevant information systems, and<br>• inspection of relevant documentation, including plans of action and milestones included in the authorization packages for relevant information systems.<br>Inspect plans of action and milestones for relevant information systems. Consider whether these plans | NIST SP 800-53, CA-05<br>NIST SP 800-53, PM-04<br>NIST SP 800-53, SR-03 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • have been recently reviewed and updated, as appropriate;<br>• are consistent with the entity-level risk management strategy;<br>• respond to risk;<br>• focus on remediating the root causes of identified deficiencies and vulnerabilities; and<br>• 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.<br>Determine whether the plans of action and milestones for relevant information systems have been appropriately documented and periodically reviewed and updated.<br>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.<br>*Related control: SM.07.01.01* | Inspect plans of action and milestones for the relevant information systems. 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<br>• specify when entity-wide corrective actions are necessary and<br>• are adequate to guide the implementation of entity-wide corrective actions to fully resolve (or substantially | NIST SP 800-53, PM-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | mitigate risks associated with) identified deficiencies and vulnerabilities.<br>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.<br>*Related control: SM.07.01.01* | Inspect plans of action and milestones for the relevant information systems and inquire with appropriate personnel to obtain an understanding of how management reasonably assures that remediation tasks and milestones are accomplished within scheduled completion dates. Consider whether the plans of action and milestones<br>• have been recently reviewed and updated, as appropriate;<br>• reflect reasonable scheduled completion dates; and<br>• 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.<br>Determine whether remediation tasks and milestones are accomplished by scheduled completion dates. | NIST SP 800-53, CA-05 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-26-108633

## 540 FISCAM Framework for Access Controls

540.01 The access controls (AC) category, also known as logical and physical access, limits access or detects inappropriate access to information resources (i.e., data and information technology), thereby protecting these resources against unauthorized modification, intentional or unintentional loss, impairment, and disclosure. Logical access controls require users to authenticate themselves and limit the files and other information resources that authenticated users can access and the actions that they can execute. Physical access controls involve restricting physical access to information resources and facilities.

540.02 The FISCAM Framework for Access Controls (see table 11) includes five critical elements:

- AC.01 Management designs and implements general controls to appropriately protect information system boundaries in response to risks.
- AC.02 Management designs and implements general controls to appropriately restrict logical access to information systems to authorized individuals for authorized purposes.
- AC.03 Management designs and implements general controls to appropriately protect data in response to risks.
- AC.04 Management designs and implements general controls to appropriately restrict physical access to information resources to authorized individuals for authorized purposes.
- AC.05 Management designs and implements detective general controls to appropriately monitor logical and physical access in response to risks.

540.03 Assessing access controls involves evaluating the entity's efforts to satisfy each of the critical elements. When evaluating management's efforts for each critical element, the auditor considers whether the associated control objectives (shown in table 11), if achieved, will address IS control risk relevant to the engagement objectives. Ineffective access controls may result in unauthorized access to, modification of, or disclosure of sensitive data and programs and disruption of critical operations.

**Table 11: FISCAM Framework for Access Controls (AC)**

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| AC.01 Management designs and implements general controls to appropriately protect information system boundaries in response to risks. | | |
| AC.01.01 Connectivity to the information system is appropriately controlled. | | |
| AC.01.01.01 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.<br>*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<br>• inquiry of appropriate personnel, including authorizing officials, network engineers, system developers, and network and system administrators, and<br>• inspection of relevant documentation, such as network maps, system security and privacy plans, and exchange agreements.<br>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 relevant information systems. 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.<br>Identify key system information exchanges relevant to the significant business processes. Determine whether key system information exchanges were appropriately established based on risk.<br>Inspect system security and privacy plans, interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level | NIST SP 800-53, AC-04<br>NIST SP 800-53, CA-03<br>NIST SP 800-53, CA-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | agreements, user agreements, nondisclosure agreements, or other exchange agreements applicable to the key system information exchanges. Consider whether such documentation<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by appropriate senior official(s);<br>• includes required information in accordance with authoritative criteria;<br>• accurately describes the key system information exchanges; and<br>• 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.<br>Determine whether key system information exchanges have been appropriately documented, periodically reviewed and updated, and properly approved.<br>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.<br>*Related control: CM.01.04.01* | Obtain an understanding of the entity's processes and methods for structuring networks and configuring network components through<br>• inquiry of appropriate personnel, including network engineers, system developers, and network and system administrators; | NIST SP 800-53, AC-04<br>NIST SP 800-53, SC-07<br>NIST SP 800-53, SC-37<br>NIST SP 800-53, SC-46 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inspection of relevant policies and procedures; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 relevant information systems. 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.<br>Determine whether networks are appropriately structured and network components are properly configured to protect access paths within and between relevant information systems. | NIST SP 800-53, SC-49<br>NIST SP 800-53, SC-50 |
| AC.01.01.03 The system uniquely identifies and authenticates devices before establishing connections. | Obtain an understanding of the processes and methods that relevant information systems employ to uniquely identify and authenticate devices before establishing a connection through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation.<br>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<br>• adequately address the access paths within and between the relevant information systems; | NIST SP 800-53, IA-03<br>NIST SP 800-53, IA-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • adequately address the components of the information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that devices are properly identified and authenticated before connections to relevant information systems, or their components, are established.<br>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.<br>*Related control: AC.01.01.05* | Obtain an understanding of the processes and methods that relevant information systems employ to control and protect remote access (dial-up or broadband) through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation.<br>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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk; and | NIST SP 800-53, AC-03<br>NIST SP 800-53, AC-17 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • reasonably assure that remote access to information systems or their components is appropriately controlled and protected.<br>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.<br>Obtain an understanding of the entity's processes and methods to log and monitor remote access to relevant information systems and their components through<br>• 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<br>• 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 management reviews.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether remote access is appropriately controlled and protected for relevant information systems.<br>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. | Obtain an understanding of the entity's processes and methods to control and protect wireless access to entity networks, network | NIST SP 800-53, AC-18<br>NIST SP 800-53, SC-43 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| *Related control: AC.01.01.04* | components, information systems, and information system components through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation.<br>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, and information system components. Consider whether such processes and methods<br>• include procedures for identifying and remediating rogue wireless access points;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that wireless access to entity networks, network components, information systems, and information system components is appropriately controlled and protected.<br>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.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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<br>• 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<br>• 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 management reviews.<br>See AC.05.01and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether wireless access to entity networks, network components, information systems, and information system components is appropriately controlled and protected.<br>Note: A rogue wireless access point is an unauthorized node on a network that connects to a wired network using a wireless network standard. | |
| AC.01.01.06 System connectivity using 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<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to enable or prevent the use of | NIST SP 800-53, AC-17<br>NIST SP 800-53, AC-18<br>NIST SP 800-53, AC-19<br>NIST SP 800-53, AC-20<br>NIST SP 800-53, SC-43 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | mobile devices and personally owned systems, components, or devices. Consider whether such processes and methods<br>• include entity-level policies on the use of mobile devices and personally owned systems, components, or devices;<br>• include procedures for requesting and approving the use of mobile devices and personally owned systems, components, or devices;<br>• 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;<br>• include mechanisms to monitor and enforce software update or configuration requirements imposed on individual users;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that system connectivity using mobile devices and personally owned systems, components, or devices is approved only when appropriate to perform assigned official duties.<br>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 systems, components, or devices to perform significant business processes.<br>Determine whether system connectivity using mobile devices and personally owned systems, components, or devices is approved only when appropriate to perform assigned official duties. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation, such as policies and procedures for managing network connectivity and implemented configuration settings, found in applicable system configuration files.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that network connections are appropriately disconnected.<br>Determine whether network connections are automatically disconnected at the end of communications sessions where connectivity is not intended to be continual. | NIST SP 800-53, SC-10 |
| 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 | Obtain an understanding of the entity's processes and methods to use device locks to prevent unauthorized access to systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for managing device locks and implemented configuration settings for initiating device | NIST SP 800-53, AC-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| using identification and authentication procedures. | locks after a specified period of inactivity, found in applicable system configuration files.<br>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<br>• include entity-level policies on the use of device locks before leaving systems unattended,<br>• are suitably designed and properly implemented based on risk, and<br>• reasonably assure that device locks are consistently and properly initiated and remain in effect until users reestablish access using identification and authentication procedures.<br>Observe a user initiate a device lock.<br>Observe the system to determine whether the system automatically initiates a device lock after a period of inactivity.<br>Determine whether device locks are properly used to prevent unauthorized access to systems. | |
| 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 relevant information systems employ to automatically terminate user sessions when certain conditions or events occur through<br>• inquiry of appropriate personnel and<br>• 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. | NIST SP 800-53, AC-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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<br>• identify the conditions or events that will prompt the information system to automatically terminate a user session,<br>• are suitably designed and properly implemented based on risk, and<br>• reasonably assure that user sessions are appropriately terminated.<br>Observe the occurrence of the conditions or events that should prompt an information system to automatically terminate a user session.<br>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<br>• before users log onto a system and until they acknowledge the notifications (for example, U.S. government system, consent to monitoring, penalties for unauthorized use, privacy notices) and<br>• after successful log-on to the system (for example, date and time of last log-on and unsuccessful log-ons). | Inquire of appropriate personnel, including users, to obtain an understanding of the entity's use of system notifications for the relevant information systems.<br>Observe appropriate personnel as they obtain access to relevant information systems.<br>Determine whether appropriate notifications are displayed on screen before users log onto a system and after successful log-on. | NIST SP 800-53, AC-08<br>NIST SP 800-53, AC-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| AC.02 Management designs and implements general controls to appropriately restrict logical access to information systems to authorized individuals for authorized purposes. | | |
| AC.02.01 Identification and authentication requirements are established. | | |
| AC.02.01.01 Identification and authentication is unique to each user (or process acting on behalf of a user), except in specially approved instances (for example, when individuals access public websites or other publicly accessible systems).<br>*Related control: AC.02.01.06* | 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 a user) through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• 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.<br>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 a user). Consider whether such processes and methods<br>• include entity-level policies requiring unique identification and authentication of users and processes;<br>• 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;<br>• include procedures for requesting and approving exceptions to the requirement for unique identification and authentication of users and processes; | NIST SP 800-53, IA-02<br>NIST SP 800-53, IA-08<br>NIST SP 800-53, IA-09<br>NIST SP 800-53, AC-14 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • 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;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that identification and authentication is unique to each user (or process acting on behalf of user), except in specially approved instances.<br>Inquire of appropriate personnel to obtain an understanding of any specially approved instances in which unique identification and authentication is not required.<br>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<br>• has been recently reviewed and updated, as appropriate;<br>• describes the status of any mitigating factors or compensating controls cited as part of the entity's approval of the exception;<br>• 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<br>• demonstrates that the exception was properly approved in accordance with the entity's procedures. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Identify any specially approved instances that affect the relevant information systems or their components, including related operating systems and data management systems.<br>Obtain an understanding of any compensating controls cited as part of the entity's approval of relevant exceptions through<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, such as policies and procedures; and<br>• observation of the entity's application of compensating controls.<br>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.<br>Determine whether identification and authentication applicable to relevant information systems and their components is unique to each user (or process acting on behalf of a 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.<br>*Related control: AC.02.04.01* | Obtain an understanding of any entity-level policies or procedures governing the selection of authenticators through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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 | NIST SP 800-53, IA-05<br>NIST SP 800-53, IA-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • have sufficient strength of mechanism for their intended use,<br>• were selected in accordance with the entity's policies and procedures, and<br>• are suitably designed and properly implemented based on risk.<br>Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components.<br>Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components.<br>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 relevant information systems employ to protect authenticators and authentication information feedback from unauthorized disclosure or modification through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• 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.<br>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 | NIST SP 800-53, IA-05<br>NIST SP 800-53, IA-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | whether such processes and methods are suitably designed and properly implemented based on risk.<br>Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. Consider whether authentication information feedback is obscured.<br>Determine whether the authenticators and authentication information feedback applicable to relevant information systems and their 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.<br>*Related control: AC.02.02.02* | Obtain an understanding of any entity-level policies or procedures governing PKI-based authentication methods through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• validate certificates by constructing a certification path to an accepted trust anchor,<br>• establish user control over the corresponding private key,<br>• map the authenticated identity to the user account, and<br>• satisfy information security requirements in accordance with authoritative criteria.<br>Inspect certificate parameters.<br>Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. | NIST SP 800-53, IA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components.<br>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. | |
| AC.02.01.05 Password-based authenticators<br>• are not displayed when entered;<br>• are changed periodically (e.g., every 30 to 90 days);<br>• contain alphanumeric and special characters;<br>• are sufficiently complex (e.g., not easily guessed, minimum length, no words, etc.);<br>• have an appropriate life (e.g., automatically expire);<br>• are prohibited from reuse for a specified period (e.g., at least six generations); and<br>• are not the same as the user ID. | Obtain an understanding of any entity-level policies or procedures governing the use of password-based authenticators through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• are not displayed when entered;<br>• are changed periodically (e.g., every 30 to 90 days);<br>• contain alphanumeric and special characters;<br>• are sufficiently complex (e.g., not easily guessed, minimum length, no words, etc.);<br>• have an appropriate life (e.g., automatically expire);<br>• are prohibited from reuse for a specified period (e.g., at least six generations);<br>• are not the same as the user ID; and<br>• satisfy information security requirements in accordance with authoritative criteria. | NIST SP 800-53, IA-05<br>NIST SP 800-53, IA-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Inspect access control software authentication parameters.<br>Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components.<br>Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components.<br>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. | |
| AC.02.01.06 Shared or group authenticators are only used in specially approved instances.<br>*Related control: AC.02.01.01* | Obtain an understanding of the entity's processes and methods to reasonably assure that shared or group authenticators are not used through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• 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.<br>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<br>• include entity-level policies requiring unique identification and authentication of users and processes;<br>• identify (preferably within the entity-level policies) any specific conditions or circumstances in which unique identification and authentication may not be necessary | NIST SP 800-53, AC-02<br>NIST SP 800-53, IA-02<br>NIST SP 800-53, IA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | and for which an exception may be requested and approved;<br>• include procedures for requesting and approving exceptions to the requirement for unique identification and authentication of users and processes;<br>• 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;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that shared or group authenticators are not used, except in specially approved instances.<br>Inquire of appropriate personnel to obtain an understanding of any specially approved instances in which shared or group authenticators are permitted.<br>Inspect documentation for any specially approved instances in which shared or group authenticators are permitted. Consider whether the documentation for any specially approved instances<br>• has been recently reviewed and updated, as appropriate;<br>• describes the status of any mitigating factors or compensating controls cited as part of the entity's approval of the exception;<br>• 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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • demonstrates that the exception was properly approved in accordance with the entity's procedures.<br>Identify any specially approved instances that affect the relevant information systems or their components, including related operating systems and data management systems.<br>Obtain an understanding of any compensating controls cited as part of the entity's approval of relevant exceptions through<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, such as policies and procedures; and<br>• observation of the entity's application of compensating controls.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>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.<br>Determine whether shared or group authenticators are only used in specially approved instances.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures for system component installation and configuration.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect password files using audit software to verify whether common vendor-supplied passwords are in use.<br>Determine whether vendor-supplied default passwords are replaced during installation for relevant information systems. | NIST SP 800-53, IA-05 |
| 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<br>• inquiry of appropriate personnel, including network engineers, system developers, and network and system administrators, and<br>• 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.<br>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<br>• include entity-level policies prohibiting passwords embedded in programs; | NIST SP 800-53, IA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • 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;<br>• include procedures for requesting and approving exceptions to the prohibition for passwords embedded in programs;<br>• 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;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that passwords embedded in programs are not used, except in specially approved instances.<br>Identify any specially approved instances that affect the relevant information systems or their components, including related operating systems and data management systems.<br>Obtain an understanding of any compensating controls cited as part of the entity's approval of relevant exceptions through<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, such as policies and procedures; and<br>• observation of the entity's application of compensating controls.<br>Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | with any specially approved instances affecting relevant information systems or their components.<br>Determine whether passwords embedded in programs are only used in specially approved instances.<br>Note: An embedded password is a password that is included in 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 using 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 relevant information systems through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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).<br>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. | NIST SP 800-53, IA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel, including users, and<br>• inspection of relevant documentation and account policy settings.<br>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.<br>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-07 |
| 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 relevant information systems employ to limit consecutive log-on attempts through<br>• inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation.<br>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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk; and | NIST SP 800-53, AC-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • reasonably assure that consecutive attempts to log on with invalid passwords within a certain period are limited.<br>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.<br>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<br>• 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<br>• 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 management reviews.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>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. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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.<br>*Related control: AC.04.01.04* | Obtain an understanding of the entity's processes and methods for presenting, validating, and verifying evidence of an individual's identity through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>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<br>• based on applicable identity assurance-level requirements and<br>• before the entity provides user credentials for the individual.<br>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.<br>*Related control: AC.02.01.04* | Obtain an understanding of the entity's process and methods for issuing PKI certificates through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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<br>• issued in accordance with an approved certificate policy or<br>• obtained from an approved service provider. | NIST SP 800-53, SC-17 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Determine whether PKI certificates are issued in accordance with an approved certificate policy or obtained from an approved service provider.<br>Determine whether only approved trust anchors are included in trust stores or certificate stores that the entity manages. | |
| AC.02.02.03 Identity providers and authorization servers are implemented to manage user, device, and non-person entity identities, attributes, and access rights supporting authentication and authorization decisions based on risk. | Obtain an understanding of any entity-level policies or procedures governing the selection and use identity providers and authorization servers through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of identity providers and authorization servers. Consider whether the identity providers and authorization servers<br>• are appropriate for their intended use,<br>• were selected in accordance with the entity's policies and procedures, and<br>• are suitably designed and properly implemented based on risk.<br>Determine whether identity providers and authorization servers are properly implemented to manage user, device, and non-person entity identities, attributes, and access rights. | NIST SP 800-53, IA-13 |
| AC.02.02.04 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 relevant information systems employ to implement session-level controls through | NIST SP 800-53, SC-20<br>NIST SP 800-53, SC-21<br>NIST SP 800-53, SC-22<br>NIST SP 800-53, SC-23 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation, such as policies and procedures for managing sessions, as well as implemented configuration settings, found in applicable system configuration files.<br>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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that appropriate session-level controls are implemented.<br>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).<br>Determine whether appropriate session-level controls are implemented. | |
| AC.02.02.05 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 relevant information systems employ to require user reauthentication when specific circumstances or situations occur through<br>• inquiry of appropriate personnel and | NIST SP 800-53, IA-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • 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.<br>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<br>• 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;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that user reauthentication is required as appropriate.<br>Observe the occurrence of the specific circumstances or situations that should prompt the information system to require a user to reauthenticate.<br>Determine whether specific circumstances or situations that require the information systems to reauthenticate users are appropriate based on risk. | |
| AC.02.02.06 Concurrent sessions are appropriately controlled. | Obtain an understanding of the processes and methods that relevant information systems employ to control concurrent sessions through<br>• inquiry of appropriate personnel, including network and system administrators, and | NIST SP 800-53, AC-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • 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.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that concurrent sessions are appropriately controlled.<br>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.<br>Obtain an understanding of the entity's processes and methods to log and monitor concurrent sessions on relevant information systems through<br>• 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<br>• inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | that log management software produces and management reviews.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether concurrent sessions on relevant information systems are appropriately controlled. | |
| AC.02.02.07 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of digital signatures and other nonrepudiation mechanisms employed in connection with the significant business processes, the relevant information systems, and their components. Consider whether the digital signatures and other nonrepudiation mechanisms<br>• were selected in accordance with the entity's policies and procedures and<br>• are suitably designed and properly implemented based on risk.<br>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.<br>Determine whether the digital signatures and other nonrepudiation mechanisms are appropriately employed in connection with the | NIST SP 800-53, AU-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | significant business processes, the relevant information systems, and their components.<br>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. | | |
| AC.02.03.01 The types of accounts that are allowed and specifically prohibited for use for the system are defined and documented.<br>*Related control: SD.01.02.02* | 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 relevant information systems through<br>• inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and<br>• inspection of relevant documentation.<br>Inspect relevant system documentation identifying the types of accounts allowed and specifically prohibited for use for relevant information systems. Consider whether<br>• the definitions include usage and restriction conditions and<br>• the criteria for group and role membership are specified.<br>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.<br>Inspect a system-generated list of accounts. Consider the appropriateness of system-generated evidence when performing | NIST SP 800-53, AC-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | control tests. Consider whether the list includes undefined or prohibited types of accounts. Determine whether the types of accounts established are appropriate.<br>Note: Account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. | |
| AC.02.03.02 Access authorizations for each type of account are defined, documented, and periodically reviewed and updated.<br>*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<br>• inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and<br>• inspection of relevant documentation.<br>Inspect relevant policies and procedures for access authorization and account management, system security and privacy plans, and other documentation identifying the account types and their access authorization for the relevant information systems. Consider whether<br>• privileged and nonprivileged users and their authorized access are accurately identified and<br>• the access that information system users are authorized to have is compatible with segregation of duties requirements.<br>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.<br>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-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| AC.02.03.03 Account management processes are implemented to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed.<br>*Related controls: SM.02.02.03, SM.02.03.03, and CM.01.01.04* | Obtain an understanding of the entity's processes and methods for creating, enabling, modifying, disabling, and removing accounts applicable to the relevant information systems through<br>• inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials;<br>• inspection of relevant policies and procedures for access authorization and account management; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>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. | NIST SP 800-53, AC-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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.<br>*Related control: SM.02.05.01* | Obtain an understanding of the entity's processes and methods for modifying, disabling, or removing accounts applicable to the relevant information systems through<br>• inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials;<br>• inspection of relevant policies and procedures for account management; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>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.<br>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 appropriateness of the documentation obtained, including any system-generated listings, when performing control tests. | NIST SP 800-53, AC-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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 appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.<br>Determine whether the account management processes applicable to relevant information systems are designed, implemented, and operating effectively to reasonably assure that accounts are timely 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).<br>*Related controls: AC.02.03.02, AC.02.04.01, SD.01.02.02, and SD.01.02.05* | Obtain an understanding of the entity's processes and methods for limiting system access to individuals with a valid business purpose for the relevant information systems through<br>• inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials, and<br>• 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.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that system access is limited to individuals with a valid business purpose. | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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.<br>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 appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.<br>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.<br>*Related controls: CM.02.02.01 and CM.02.04.01* | Obtain an understanding of the entity's processes and methods to control emergency and temporary access to the relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for the use of emergency and temporary accounts, including firecall IDs.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to control emergency and temporary access to the relevant information systems. Consider whether such processes and methods<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• include entity-level policies governing the use of emergency and temporary accounts, including firecall IDs; | NIST SP 800-53, AC-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • 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;<br>• 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;<br>• include procedures for requesting and approving the use of emergency and temporary accounts;<br>• include procedures for creating, enabling, modifying, disabling, and removing emergency and temporary accounts;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that emergency and temporary access to information systems is appropriately controlled and protected.<br>Obtain an understanding of the entity's processes and methods to log and monitor emergency and temporary access to the relevant information systems through<br>• 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<br>• inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | that log management software produces and management reviews.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Observe appropriate personnel as they obtain access to the relevant information systems 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.<br>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 appropriateness of the documentation obtained, including any logs of the use of emergency or temporary accounts, when performing control tests.<br>Determine whether emergency and temporary access to the relevant information systems is appropriately controlled.<br>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 management 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 | NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inquiry of appropriate personnel, including network and system administrators, and<br>• inspection of relevant documentation, such as policies and procedures for managing access to shared file systems.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that access to shared file systems relevant to the significant business processes is appropriately restricted.<br>Observe appropriate personnel as they obtain access to the shared file systems relevant to the significant business processes. Consider whether the processes and methods observed to restrict access to shared file systems are consistent with those the entity has documented.<br>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.<br>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 appropriateness of the | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | documentation obtained, including any logs of changes to access control parameters, when performing control tests.<br>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<br>• 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<br>• 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 management reviews.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether access to shared file systems relevant to the significant business processes is appropriately restricted. | |
| 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 relevant information systems through<br>• inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials;<br>• inspection of relevant policies and procedures for access authorization, account management, and periodic access recertification; and | NIST SP 800-53, AC-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect available documentation for a selection of instances in which access to the relevant information systems 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 appropriateness of the documentation obtained, including any system-generated listings of accounts, when performing control tests.<br>Determine whether the processes for periodically reviewing access to the relevant information systems are designed, implemented, and operating effectively to reasonably assure that system access is appropriate. | |
| AC.02.03.09 Access control parameters are set to apply access control decisions and enforce access as authorized.<br>*Related control: SD.01.02.02* | Obtain an understanding of the processes and methods that relevant information systems employ to apply access control decisions and enforce access as authorized through<br>• inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and<br>• 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. | NIST SP 800-53, AC-03<br>NIST SP 800-53, AC-24<br>NIST SP 800-53, AC-25 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that access control parameters are properly set to apply access control decisions and enforce access as authorized.<br>For each relevant information system, identify the directory names for files, datasets, libraries, and other information resources critical to achieving information security or information processing objectives. For example, information resources may include files that operating systems rely upon and use. Inspect the access control parameters for such information 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 datasets or resources and reports detailing privileges granted to specific users or accounts that provide access to datasets, libraries, and other information 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.<br>Inspect available documentation for a selection of instances in which access control parameters applicable to relevant information systems were modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity's | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | policies and procedures for managing access control software. Consider the appropriateness of the documentation obtained, including any system-generated access control lists or system configuration files, when performing control tests.<br>Obtain an understanding of the entity's processes and methods to log and monitor changes to access control parameters through<br>• 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<br>• 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 management reviews.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether access control parameters applicable to relevant information systems are properly set to apply access control decisions and enforce access as authorized.<br>Note: Access control parameters are set to apply access control decisions to datasets, libraries, and other information resources. Standard naming conventions are generally established and used as a basis for controlling access to information 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 | Obtain an understanding of the entity's processes and methods for the relevant information systems to reasonably assure that system | NIST SP 800-53, CM-07<br>NIST SP 800-53, SC-41 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| are necessary to support entity operations through, for example,<br>• installing only required functions and services based on least functionality,<br>• restricting access to required functions and services based on least privilege,<br>• monitoring the use of functions and services, and<br>• employing appropriate tools and technologies to identify and prevent the use of prohibited functions and services.<br>*Related controls: SD.01.02.02, CM.01.04.01, and CM.03.01.01* | functions and services are limited to those necessary to support entity operations through<br>• inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and<br>• 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.<br>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<br>• include policies and procedures for installing only required functions and services based on least functionality,<br>• include policies and procedures for restricting access to required functions and services based on least privilege,<br>• address monitoring the use of functions and services,<br>• employ appropriate tools and technologies to identify and prevent the use of prohibited functions and services,<br>• are suitably designed and properly implemented based on risk, and<br>• reasonably assure that system functions and services are limited to those that are necessary to support entity operations. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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 relevant information systems employ to prohibit remote activation of collaborative computing devices and applications through<br>• inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and<br>• 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.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that the information systems prohibit remote activation of collaborative computing devices and applications.<br>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 controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Determine whether relevant information systems prohibit remote activation of collaborative computing devices.<br>Note: Collaborative computing devices and applications include remote meeting devices and applications, networked whiteboards, 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 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.<br>*Related controls: AC.02.01.02, AC.02.03.02, AC.02.03.05, and SD.01.02.05* | Obtain an understanding of the entity's processes and methods for the relevant information systems to reasonably assure that the use of privileged accounts is appropriately restricted through<br>• inquiry of appropriate personnel, including privileged users, network and system administrators, information resource owners, and authorizing officials, and<br>• 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.<br>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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• include entity-level policies governing the use of privileged accounts; | NIST SP 800-53, AC-02<br>NIST SP 800-53, AC-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • identify (preferably within the entity-level policies) the specific functions or tasks that individuals may perform while using privileged accounts;<br>• maintain a complete listing of individuals who are authorized to use privileged accounts, which is shared with authorizing officials and other IT management personnel;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that privileged access is limited to individuals or processes with a valid business purpose.<br>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.<br>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 appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.<br>Determine whether the use of privileged accounts is restricted to individuals or processes with a legitimate need for privileged access to information 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<br>• inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT | NIST SP 800-53, AC-02<br>NIST SP 800-53, AU-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | management personnel responsible for the entity's log management tools and software, and<br>• 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 management reviews.<br>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<br>• adequately address the components of the relevant information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk;<br>• reasonably assure that reports that log management software produces and management reviews are complete and accurate; and<br>• reasonably assure that the entity takes appropriate action to identify and address any access anomalies.<br>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 management reviews. Consider the appropriateness of these reports when performing control tests.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether the use of privileged accounts is appropriately logged and adequately monitored. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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 utilities applicable to the relevant information systems through<br>• 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<br>• 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 management reviews.<br>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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• are suitably designed and properly implemented based on risk;<br>• reasonably assure that logical access to maintenance tools and utilities applicable to relevant information systems is appropriately controlled and logged;<br>• reasonably assure that reports that log management software produces and management reviews are complete and accurate; and | NIST SP 800-53, AC-02<br>NIST SP 800-53, MA-02<br>NIST SP 800-53, MA-03<br>NIST SP 800-53, MA-04<br>NIST SP 800-53, MA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • reasonably assure that management takes appropriate action to identify and address any access anomalies.<br>Observe appropriate personnel as they obtain logical access to maintenance tools and utilities applicable to relevant information systems. Consider whether the processes and methods for controlling logical access are consistent with those documented by the entity.<br>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 management reviews. Consider the appropriateness of these reports when performing control tests.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>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 relevant information systems employ to control logical access to authenticators and authentication services and directories through<br>• inquiry of appropriate personnel, including authorizing officials, system developers, and network and system administrators, and<br>• 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. | NIST SP 800-53, AC-02<br>NIST SP 800-53, IA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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<br>• adequately address the components of the information systems, including related operating systems and data management systems;<br>• employ encryption techniques when appropriate based on risk;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that access to authenticators and authentication services and directories is restricted to authorized individuals for authorized purposes.<br>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<br>• 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<br>• 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 management reviews. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether authenticators and authentication services and directories applicable to relevant information systems and their components are appropriately controlled and encrypted when necessary. | |
| AC.02.04.05 Mobile code is appropriately controlled. | Obtain an understanding of the entity's processes and methods to control mobile code through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to control mobile code. Consider whether such processes and methods<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that mobile code is appropriately controlled.<br>Determine whether mobile code is appropriately controlled.<br>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-18<br>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 its entity-defined security functions. | Obtain an understanding 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 through<br>• inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and | NIST SP 800-53, SC-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inspection of relevant documentation.<br>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<br>• identify and adequately address the trusted components of the information systems;<br>• are suitably designed and properly implemented based on risk; and<br>• reasonably assure that an isolated, trusted communications path between the user and trusted components of the information system is established.<br>Determine whether the information systems established 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.<br>Note: Entities employ trusted paths for trustworthy, high-assurance connections between systems' security functions and users, including during system log-ons. | |
| AC.03 Management designs and implements general controls to appropriately protect data in response to risks. | | |
| AC.03.01 Media controls are appropriately selected and employed based on risk. | | |
| AC.03.01.01 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 relevant information systems through | NIST SP 800-53, MP-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inquiry of appropriate personnel, including users, information resource owners, and authorizing officials, and<br>• inspection of relevant documentation.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• 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.<br>Determine whether access to printed and digital media containing data removed from relevant information systems is appropriately limited to authorized individuals for authorized purposes.<br>Note: Digital media include diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Nondigital media include 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 relevant information systems employ to mark output and associate attributes with internal data in storage, process, and transmission through<br>• inquiry of appropriate personnel, including system developers, users, information resource owners, and authorizing officials, and<br>• inspection of relevant documentation. | NIST SP 800-53, AC-16<br>NIST SP 800-53, MP-03<br>NIST SP 800-53, SC-16 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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<br>• are suitably designed and properly implemented based on risk;<br>• employ standard practices for marking output, including the use of standard naming conventions;<br>• employ standard practices for associating security and privacy attributes to internal data, including the labeling of data; and<br>• reasonably assure that associated security and privacy attributes are not modified when information is exchanged between information systems and their components.<br>Determine whether relevant information systems appropriately mark output and associate attributes with internal data in storage, process, and transmission.<br>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 (PII), and identification of personal information within data objects.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Observe the entity's processes and methods for controlling the collection, transport, and delivery of system media associated with relevant information systems.<br>Inspect available documentation for a selection of instances in which system media associated with relevant information systems were collected, transported, or delivered during the audit period.<br>Determine whether the collection, transport, and delivery of system media associated with relevant information systems are appropriately controlled. | NIST SP 800-53, MP-05 |
| AC.03.01.04 System media are securely stored according to their sensitivity until destroyed or sanitized. | Obtain an understanding of the entity's processes and methods for storing system media associated with the relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Observe the entity's processes and methods for storing system media associated with relevant information systems. Consider whether the | NIST SP 800-53, MP-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | processes and methods adequately address the sensitivity of data contained within such media and legal and entity information retention requirements.<br>Determine whether system media associated with relevant information systems are securely stored according to their sensitivity until destroyed or sanitized. | |
| 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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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 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.<br>Inspect a selection of recently sanitized digital media and determine whether such have been properly sanitized.<br>Inspect a selection of disposal records data, documentation, tools, or system components and determine whether such have been properly disposed of.<br>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. | NIST SP 800-53, MP-06<br>NIST SP 800-53, MP-08<br>NIST SP 800-53, SR-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• are appropriate for their intended use,<br>• were selected in accordance with the entity's policies and procedures, and<br>• are suitably designed and properly implemented based on risk.<br>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. | NIST SP 800-53, SC-13<br>NIST SP 800-53, SC-28 |
| AC.03.02.02 Encryption techniques are implemented to protect data communications when appropriate.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, SC-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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<br>• are appropriate for their intended use,<br>• were selected in accordance with the entity's policies and procedures, and<br>• are suitably designed and properly implemented based on risk.<br>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. | |
| 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 relevant information systems. Consider whether the authentication mechanisms<br>• are appropriate and<br>• are suitably designed and properly implemented based on risk.<br>Determine whether appropriate mechanisms are properly employed for authentication to cryptographic modules applicable to relevant information systems.<br>Note: Authentication mechanisms are hardware- or software-based mechanisms that force users to prove their identities before accessing information. | NIST SP 800-53, IA-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| 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 relevant information systems through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed in connection with cryptographic key generation distribution, storage, access, and destruction.<br>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 general controls to appropriately restrict physical access to information resources to authorized individuals for authorized purposes. | | |
| AC.04.01 Physical access controls are appropriately selected and employed based on risk. | | |
| AC.04.01.01 Physical and environmental hazards to facilities where systems and system components reside are assessed and included as part of the entity-level risk management strategy for information security and privacy risks.<br>*Related control: SM.04.01.01* | Obtain an understanding of the entity-level process for assessing physical and environmental hazards to the facilities where relevant information systems reside through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the entity-level risk management strategy for information security and privacy risks.<br>Determine whether physical and environmental hazards to the facilities where relevant information systems reside are appropriately | NIST SP 800-53, PE-23 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | assessed and included as part of the entity-level risk management strategy.<br>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 relevant information systems within applicable facilities through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the position of system components within the applicable facilities.<br>Inspect a diagram of the physical layout of the facilities where relevant information systems reside. Identify sensitive areas housing critical system components or concentrations of system resources (e.g., data centers and server rooms).<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the position of system components comprising relevant information systems within the facilities. Consider whether nonessential support entities residing at the facilities are co-located with the system components. See AC.04.01.06 for considerations related to physical access controls.<br>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.<br>Note: Entities consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be | NIST SP 800-53, PE-18<br>NIST SP 800-53, PE-19<br>NIST SP 800-53, PE-21 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | near systems. Such proximity can increase the risk of unauthorized access to entity communications. When possible, system components should not be co-located 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 relevant information systems reside through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the list of individuals with authorized access to these facilities. Consider whether the list<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s); and<br>• is adequate to clearly identify individuals with authorized access and the individuals authorizing the access.<br>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 appropriateness of the documentation obtained, including any system-generated listings of recently separated personnel.<br>Determine whether the list of individuals with authorized access to the facilities where relevant information systems reside has been appropriately documented, periodically reviewed and updated, and properly approved. | NIST SP 800-53, PE-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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.<br>*Related control: AC.02.02.01* | Obtain an understanding of the entity's process and methods for issuing physical access authorizations credentials through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures.<br>Inspect available documentation for a selection of individuals for whom physical access authorization credentials were issued during the audit period.<br>Observe practices for safeguarding unissued physical access authorization credentials.<br>Determine whether physical access authorization credentials are properly issued to individuals who are authorized to access facilities where relevant information systems reside.<br>Note: Physical access authorization credentials include ID badges, identification cards, and smart cards. | NIST SP 800-53, MA-05<br>NIST SP 800-53, PE-02 |
| 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 to be escorted by individuals with authorized access to facilities where systems reside. | Obtain an understanding of any entity-level policies or procedures governing visitor access to the facilities where relevant information systems reside through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures for managing visitor access to applicable facilities.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, MA-05<br>NIST SP 800-53, PE-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Inspect available documentation for a selection of individuals who visited the facilities where relevant information systems reside during the audit period. Consider whether<br>• the visitor screening activities performed, including any background screening requirements completed prior to a visitor accessing the facilities, are appropriate based on risk;<br>• the conditions or circumstances requiring visitors to be escorted are consistently applied and appropriate based on risk; and<br>• the maintenance of records associated with visitor access to the facilities is sufficient to demonstrate the performance of applicable general controls associated with a visitor's access.<br>Observe entries to and exits from facilities where relevant information systems reside during and after normal business hours.<br>Determine whether the general controls associated with visitor access to the facilities where relevant information systems 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 employment of physical access controls based on risk, including<br>• guards and guard posts; | Obtain an understanding of the physical access controls that the entity employs for the facilities where relevant information systems reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the entity's use of physical access controls. | NIST SP 800-53, PE-03<br>NIST SP 800-53, PE-08<br>NIST SP 800-53, PE-16 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| • physical access devices and barriers;<br>• physical access logs, including visitor access records, used in conjunction with lists of individuals with authorized access;<br>• requirements for individuals to carry or display ID badges (including visitor badges); and<br>• physical perimeter security checks, patrols, and inspections. | Inspect a diagram of the physical layout of the facilities where relevant information systems 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).<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the physical access controls that the entity employs 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.<br>Observe practices for safeguarding physical access devices, such as keys and combinations, applicable to the key access points.<br>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 reside.<br>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. | |
| 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 | Obtain an understanding of the physical access monitoring controls that the entity employs for the facilities where relevant information systems reside through | NIST SP 800-53, PE-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| through the selection and employment of physical access monitoring controls based on risk, including<br>• guards and guard posts,<br>• video surveillance equipment, and<br>• physical intrusion alarms. | • inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the entity's use of physical access monitoring controls.<br>Inspect a diagram of the physical layout of the facilities where relevant information systems 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).<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the physical access monitoring controls that the entity employs 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.<br>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 reside.<br>Note: Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. | |
| 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 relevant information systems reside, including physical access to sensitive areas housing critical system components or concentrations of system resources within such facilities, through | NIST SP 800-53, PE-06<br>NIST SP 800-53, PE-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and<br>• 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 management reviews.<br>Inspect documentation demonstrating the design and implementation of the entity's processes and methods to log and monitor physical access to the facilities where relevant information systems 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<br>• are suitably designed and properly implemented based on risk,<br>• reasonably assure that reports that log management software produce and management reviews are complete and accurate, and<br>• reasonably assure that the entity takes appropriate action to identify and address any physical access anomalies.<br>Observe the entity's processes and methods for logging and monitoring physical access to the facilities where relevant information systems reside, including physical access to sensitive areas housing critical system components or concentrations of system resources within such facilities. Consider the appropriateness of the reports that log management software produces and management reviews when performing control tests. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Inspect reports that log management software produces. Compare physical access log entries in the reports to authorized access lists or visitor access records, as appropriate.<br>Observe entries to and exits from facilities where relevant information systems reside, including sensitive areas housing critical system components or concentrations of system resources within such facilities. Consider whether reports that the log management software produce are properly updated as authorized personnel or visitors enter and exit facilities where systems reside, as well as sensitive areas within such facilities.<br>See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.<br>Determine whether physical access to facilities where relevant information systems 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.<br>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 that the entity employs to control physical access to system distribution and transmission lines within the facilities where relevant information systems reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and | NIST SP 800-53, PE-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • observation of the entity's use of security controls applicable to system distribution and transmission lines.<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the security controls that the entity employs 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.<br>Determine whether physical access to system distribution and transmission lines is appropriately controlled.<br>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 relevant information systems reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the entity's processes and methods for controlling physical access to system output devices.<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the controls that the entity employs to manage | NIST SP 800-53, PE-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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.<br>Determine whether physical access to system output devices is appropriately controlled.<br>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 relevant information systems reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the entity's processes and methods for controlling physical access to power equipment and cabling.<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the controls that the entity employs 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 manage physical access to power equipment and cabling are designed, implemented, and operating effectively. | NIST SP 800-53, PE-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Determine whether physical access to power equipment and cabling is appropriately controlled.<br>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 general controls 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<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's intrusion detection tools and software, and<br>• 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 management reviews.<br>Inspect documentation demonstrating the design and implementation of the entity's intrusion detection system. Consider whether the entity's intrusion detection system<br>• adequately addresses the relevant information systems processes;<br>• adequately addresses the components of relevant information systems;<br>• adequately addresses the placement of intrusion detection sensors and incident thresholds; | NIST SP 800-53, SI-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • is suitably designed and properly implemented based on risk;<br>• reasonably assures that reports or alerts produced by intrusion detection software and reviewed by management are complete and accurate; and<br>• reasonably assures that appropriate information is provided to management to facilitate action in response to attacks or indicators of potential attacks, as well as unauthorized local, network, or remote connections.<br>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.<br>*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, SM.01.05.01, AC.05.01.02, AC.05.01.04, AC.05.01.05, AC.05.01.06, AC.05.01.07, AC.05.02.01, and AC.05.02.03* | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to the relevant information systems, including related operating systems and data management systems. Information resources relevant to the significant business processes also include files, datasets, libraries, and other information resources critical to achieving information security or information processing objectives.<br>Consider whether the following event types have been selected for logging: | NIST SP 800-53, AU-02<br>NIST SP 800-53, SA-20 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • remote access (dial-up or broadband) to relevant information systems (see AC.01.01.04);<br>• wireless access to entity networks, network components, information systems, and information system components (see AC.01.01.05);<br>• consecutive attempts to log on with invalid passwords within a certain period (see AC.02.01.11);<br>• concurrent sessions (see AC.02.02.06);<br>• emergency and temporary access to relevant information systems (see AC.02.03.06);<br>• access to shared file systems (see AC.02.03.07);<br>• access control parameters (see AC.02.03.09);<br>• the use of privileged accounts (see AC.02.04.02);<br>• logical access to maintenance tools and utilities (see AC.02.04.03);<br>• logical access to authenticators and authentication services and directories (see AC.02.04.05); and<br>• physical access to facilities where systems reside, as well as sensitive areas within such facilities (see AC.04.01.08).<br>Consider whether the event types selected for logging that are applicable to the relevant information systems, including related operating systems and data management systems, are adequate to support appropriate incident response.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Note: An event is an observable occurrence. The types of events that require logging are those events that are significant and relevant to the 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, Personal Identity Verification (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.<br>*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.05.01.04, AC.05.01.05, AC.05.01.06, AC.05.01.07, AC.05.02.01, AC.05.02.02, and AC.05.02.03* | Obtain an understanding of the entity's processes and methods to reasonably assure that all event types selected for logging are logged through<br>• 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<br>• 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 management reviews.<br>Inspect audit records for the event types selected for logging that are applicable to the relevant information systems, including related operating systems and data management systems. Consider the appropriateness of the documentation obtained, including any reports that log management software produces and management reviews. | NIST SP 800-53, AU-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Determine whether all event types selected for logging that are applicable to relevant information systems are appropriately logged.<br>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 can generate 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.<br>*Related control: AC.05.01.02, AC.05.01.03, and AC.05.02.03* | Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems.<br>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.<br>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. System-generated time stamps 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-03<br>NIST SP 800-53, AU-08<br>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 | 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<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and | NIST SP 800-53, AU-04<br>NIST SP 800-53, AU-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| appropriate personnel and personnel take timely, appropriate action.<br>*Related controls: AC.05.01.02 and AC.05.01.03* | • 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.<br>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.<br>Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. Consider whether all required audit records associated with such events are available for inspection.<br>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.<br>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.<br>*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<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and<br>• inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing | NIST SP 800-53, AU-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | log management tools and software, as well as implemented access control parameters.<br>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 are able to access, modify, or delete corresponding audit records or change configuration settings for applicable audit logging tools.<br>Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. Consider whether all required audit records associated with such events are available for inspection.<br>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.<br>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.<br>Note: Audit information includes all information needed to successfully audit information system activity, such as audit records, audit log settings, reports that log management software produce, and PII 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 | Obtain an understanding of the entity's processes and methods to reasonably assure that audit records are retained long enough to | NIST SP 800-53, AU-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| investigations of security incidents and to meet legal and entity information retention requirements.<br>*Related controls: AC.05.01.02 and AC.05.01.03* | provide support for after-the-fact investigations of security incidents and to meet legal and regulatory requirements and entity policies on information retention through<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's log management tools and software, and<br>• 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.<br>Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. Consider whether all required audit records associated with such events are available for inspection.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether such processes and methods<br>• adequately define the situations for which session auditing may be employed, | NIST SP 800-53, AU-14 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | • adequately address the use of PII, and<br>• are suitably designed and properly implemented based on risk.<br>Determine whether the process established for session auditing is designed, implemented, and operating effectively and appropriately based on risk.<br>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.<br>*Related controls: AC.05.01.02, AC.05.01.03, and AC.05.02.02* | Obtain an understanding of the entity's processes and methods for regularly reviewing and analyzing audit records through<br>• inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials;<br>• inspection of relevant policies and procedures for logging, monitoring, and managing log management tools and software;<br>• observation of the processes for regularly reviewing and analyzing audit records; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. 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 | NIST SP 800-53, AC-02<br>NIST SP 800-53, AU-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | 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. Consider the appropriateness of the documentation obtained, including any reports that log management software produces, when performing control tests.<br>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.<br>*Related control: AC.05.02.01* | Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. Consider whether any investigation results, as applicable, were reported to appropriate personnel. Consider whether any disciplinary actions taken, as applicable, were appropriate.<br>Determine whether investigation results are reported to appropriate personnel and disciplinary actions are taken when necessary. | NIST SP 800-53, AU-06<br>NIST SP 800-53, PS-08 |
| 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.<br>*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 relevant information systems.<br>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-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| AC.05.02.04 External and internal security alerts, advisories, and directives are identified and promptly issued to appropriate personnel, who take appropriate action.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether external and internal security alerts, advisories, and directives are identified and promptly issued to appropriate personnel, who take appropriate action. | NIST SP 800-53, SI-05 |
| AC.05.02.05 A coordinated, cross-entity approach to sharing incident information is implemented.<br>*Related control: SM.03.02.01* | Obtain an understanding of the entity's approach for sharing incident information through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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 parties when appropriate.<br>Determine whether a coordinated, cross-entity approach to sharing incident information is implemented. | NIST SP 800-53, AU-16 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | Note: When systems or services of external parties 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. | |
| 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<br>• inquiry of appropriate personnel, including incident response team members, and<br>• inspection of relevant documentation.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably ensure that incidents involving information spills and data losses are properly analyzed and appropriate actions are taken.<br>Determine whether information spills and data losses are properly identified, isolated, and resolved by appropriate personnel.<br>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 | NIST SP 800-53, AU-13<br>NIST SP 800-53, IR-09<br>NIST SP 800-53, SI-20 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev 5) controls |
|---|---|---|
| | proprietary, sensitive, or classified information through data theft (or exfiltration) and data leakage. | |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-26-108633

## 550 FISCAM Framework for Segregation of Duties

550.01 The segregation of duties (SD) category relates to the policies, procedures, and an organizational structure for managing who can control key aspects of computer-related operations and thereby prevent unauthorized actions or 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. 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.

550.02 The FISCAM Framework for Segregation of Duties (see table 12) includes one critical element:

- SD.01 Management designs and implements general controls to appropriately segregate incompatible duties and mitigate risks resulting from incompatible duties that cannot be segregated.

550.03 Assessing segregation of duties controls involves evaluating the entity's efforts to satisfy the critical element. When evaluating management's efforts toward the critical element, the auditor considers whether the associated control objectives (shown in table 12), if achieved, will address IS control risk relevant to the engagement objectives. Ineffective segregation of duties controls may result in erroneous or fraudulent transactions being processed, improper program changes being implemented, and computer resources being damaged or destroyed.

**Table 12: FISCAM Framework for Segregation of Duties (SD)**

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| SD.01 Management designs and implements general controls to appropriately segregate incompatible duties and mitigate risks resulting from incompatible duties that cannot be segregated. | | |
| SD.01.01 Incompatible duties are identified based on risk. | | |
| SD.01.01.01 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 | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation. | NIST SP 800-53, AC-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| • preparation of data for input into the system,<br>• approval of data for input into the system,<br>• data input,<br>• research and resolution of data input errors that the system identified,<br>• research and resolution of data processing errors that the system identified,<br>• reconciliation of interfaced data, and<br>• verification of output data.<br>*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, SM.02.01.03, and AC.05.01.06* | 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:<br>• 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.<br>• 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.<br>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.<br>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.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | and procedures. Incompatible duties are also documented within segregation of duties matrices, which may be developed at the entity, 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<br>• information security management,<br>• IT asset management,<br>• system or application design,<br>• system or application programming,<br>• system or application maintenance,<br>• quality assurance testing,<br>• change authorization,<br>• code migration,<br>• configuration auditing,<br>• media management,<br>• production control and scheduling,<br>• application administration,<br>• database administration; | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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:<br>• 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 changes to relevant information systems and their components, as well as maintaining records and custody of IT assets. For example:<br>○ Programmers should not have the ability to migrate code into the production environment and should not have access to production software or data.<br>○ Security administrators who administer access controls should not also administer changes to | NIST SP 800-53, AC-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| • operating system administration,<br>• system administration,<br>• network administration,<br>• security administration,<br>• log management, and<br>• log monitoring.<br>*Related controls: BP.04.03.07, BP.06.03.05, SM.01.02.03, and SM.02.01.03* | network components, applications, databases, operating systems, or other system resources or components.<br>○ Database administrators should not be involved in any IT management functions beyond the duties of database administration.<br>○ 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.<br>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.<br>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.<br>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 documented within segregation of duties matrices, which may be developed at the entity, organizational unit, IT management function, | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | and system levels. 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.<br>*Related control: BP.04.03.07* | 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<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of personnel performing business process and IT management functions.<br>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 controls and audit procedures within AC.02 and AC.04.<br>Determine whether the segregation of identified incompatible duties relevant to the significant business processes is appropriately enforced by logical and physical access controls.<br>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 users—not IT management personnel—should have the ability to initiate transactions and authorize changes to transaction data. | NIST SP 800-53, AC-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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.<br>*Related controls: BP.04.03.07, BP.06.03.05, AC.02.03.01, AC.02.03.02, AC.02.03.05, AC.02.03.09, AC.02.03.10, 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<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, including policies and procedures for the significant business processes; and<br>• observation of personnel performing significant business processes.<br>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.<br>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.<br>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-05 |
| 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<br>• inquiry of appropriate personnel; | NIST SP 800-53, AC-05<br>NIST SP 800-53, SC-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of relevant documentation, including policies and procedures for the significant business processes; and<br>• observation of personnel performing significant business processes.<br>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.<br>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.<br>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.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, including policies and procedures for the significant business processes; and<br>• observation of personnel performing significant business processes.<br>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.<br>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. | NIST SP 800-53, AC-05<br>NIST SP 800-53, SC-02 |
| SD.01.02.05 The information system isolates security functions from nonsecurity functions.<br>*Related controls: SM.01.04.01, 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<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, including policies and procedures for security functions; and<br>• observation of IT management personnel performing security functions.<br>Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system's processes | NIST SP 800-53, AC-05<br>NIST SP 800-53, AC-06<br>NIST SP 800-53, SC-03<br>NIST SP 800-53, SC-39 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | and methods. Consider whether the information system adequately restricts access to security functions using appropriate access control mechanisms and by implementing least privilege capabilities.<br>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.<br>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 general controls 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 general controls, such as the supervisory review of tasks or the subsequent monitoring of relevant audit records.<br>*Related controls: BP.04.03.07 and BP.06.03.05*<br>*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 general controls to mitigate risks resulting from incompatible duties that cannot be segregated through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inquire of appropriate personnel to obtain an understanding of any approved exceptions to segregation of duties requirements.<br>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 | NIST SP 800-53, AC-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • has been recently reviewed and updated;<br>• describes the status of any mitigating factors or compensating controls cited as part of the entity's approval of the exception;<br>• 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 compensating controls sufficiently reduce risk to an acceptable level; and<br>• demonstrates that the exception was properly approved in accordance with the entity's procedures.<br>Obtain an understanding of any compensating controls or alternative general controls cited as part of the entity's approval of relevant exceptions through<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation, including policies and procedures; and<br>• observation of the entity's application of compensating controls.<br>Determine whether the compensating controls or alternative general controls are designed, implemented, and operating effectively to mitigate the risks associated with incompatible duties that cannot be separated.<br>Determine whether management appropriately considered and accepted any residual risks associated with exceptions to segregation of duties requirements. | |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-26-108633

## 560 FISCAM Framework for Configuration Management

560.01 The configuration management (CM) category relates to identifying and managing operating and security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling 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 the information system and provide reasonable assurance that systems are securely configured and operated as intended. 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. 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.

560.02 The FISCAM Framework for Configuration Management (see table 13) includes three critical elements:

- CM.01 Management designs and implements general controls to develop and maintain secure baseline configurations for information systems.
- CM.02 Management designs and implements general controls to manage changes to entity information systems and information system components.
- CM.03 Management designs and implements general controls to protect information systems and information system components from vulnerabilities, flaws, and threats.

560.03 Assessing configuration management controls involves evaluating the entity's efforts to satisfy each of the critical elements. When evaluating management's efforts for each critical element, the auditor considers whether the associated control objectives (shown in table 13), if achieved, will address IS control risk relevant to the engagement objectives. Ineffective configuration management controls may result in security features being inadvertently or deliberately omitted or turned off or processing irregularities or malicious code being introduced. In addition, users do not have adequate assurance that the system will work as intended and to the extent needed to support their operations.

**Table 13: FISCAM Framework for Configuration Management (CM)**

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| CM.01 Management designs and implements general controls to develop and maintain secure baseline configurations for information systems. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect the system-level configuration management plans for each relevant information system. Consider whether the plans<br>• identify roles and responsibilities;<br>• incorporate or reference current entity-level configuration management policies and procedures;<br>• define configuration items for the information system and place such items under configuration management;<br>• establish a process for identifying configuration items throughout the system development life cycle;<br>• establish processes for managing the configuration of these items for the information system and monitoring implemented configuration settings against baseline configurations;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s);<br>• include required information in accordance with authoritative criteria; and | NIST SP 800-53, CM-02<br>NIST SP 800-53, CM-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • are adequate to address configuration management activities applicable to the information system, including any changes to the baseline configuration of the system.<br>Determine whether the system-level configuration management plans for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, consider whether the system-level configuration management plans for relevant information systems have been implemented.<br>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. | Obtain an understanding of the entity's processes and methods for selecting, testing, and implementing configuration settings for the relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for selecting, testing, and | NIST SP 800-53, CM-06<br>NIST SP 800-53, CM-07<br>NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-08<br>NIST SP 800-53, SA-23<br>NIST SP 800-53, SC-25 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| *Related control: CM.01.01.03* | implementing configuration settings for information systems and information system components.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect the implemented configuration settings for a selection of configuration items for relevant information systems. Consider whether the implemented configuration settings<br>• optimize the system's security features;<br>• minimize available processes and services consistent with operational requirements;<br>• align with entity-level requirements, including any entity-defined common secure configurations; and<br>• are consistent with the corresponding baseline configuration settings.<br>Determine whether the implemented configuration settings for the configuration items selected have been properly selected, tested, and implemented.<br>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.<br>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 | NIST SP 800-53, SC-29<br>NIST SP 800-53, SC-34<br>NIST SP 800-53, SC-51<br>NIST SP 800-53, SI-14<br>NIST SP 800-53, SI-16<br>NIST SP 800-53, SI-21 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) 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. | |
| CM.01.01.03 Baseline configurations of systems are developed, documented, and periodically reviewed and updated.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for maintaining baseline configurations of systems.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect the baseline configurations for the relevant information systems. Consider whether the baseline configurations<br>• are under configuration control;<br>• are adequate to serve as a basis for future builds, releases, or changes to the information systems;<br>• are based on documented configuration change decisions and reflect the existing enterprise architecture;<br>• include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture;<br>• have been recently reviewed and updated, as appropriate; and | NIST SP 800-53, CM-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • have been approved by the appropriate senior official(s).<br>Determine whether the baseline configurations for the relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, consider whether the baseline configurations for relevant information systems have been properly maintained.<br>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.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for maintaining system documentation.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, SA-04<br>NIST SP 800-53, SA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect the system documentation for administrators and users of the relevant information systems. Consider whether the documentation<br>• is appropriately protected commensurate with the security categorization of the information system;<br>• accurately describes for administrators the secure configuration, installation, and operation of the information system and its components, as well as the effective use and maintenance of security and privacy mechanisms and any known vulnerabilities associated with administrative functions;<br>• 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;<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s);<br>• includes required information in accordance with authoritative criteria; and<br>• has been distributed to appropriate personnel.<br>Determine whether system documentation for administrators and users of relevant information systems has been appropriately documented, periodically reviewed and updated, and properly approved.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | mission and business function requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing.<br>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. | |
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for maintaining information system component inventories.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect the inventories of components for relevant information systems. Consider whether each inventory<br>• accurately reflects the information system; | NIST SP 800-53, CM-02<br>NIST SP 800-53, CM-08<br>NIST SP 800-53, PE-22 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • includes records for all components for the information system;<br>• does not include duplicate records for any components;<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s); and<br>• includes required information in accordance with authoritative criteria and in sufficient detail to promote accountability for information system components.<br>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 identify the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.<br>Determine whether the inventories of components for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | situations, entities ensure that the inventories include system-specific information required for component accountability.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for monitoring the baseline configurations for information systems.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Observe appropriate personnel as they perform procedures for detecting and addressing unauthorized information system components.<br>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 | NIST SP 800-53, CM-02<br>NIST SP 800-53, CM-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | and appropriately employed to detect unauthorized system components and alert appropriate personnel.<br>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.<br>Determine whether unauthorized system components are detected and appropriately addressed on a timely basis.<br>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.<br>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.<br>Adequate security is the level of security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. | |
| CM.01.02.03 Counterfeit system components are detected and appropriately addressed on a timely basis.<br>*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<br>• inquiry of appropriate personnel and | NIST SP 800-53, SR-09<br>NIST SP 800-53, SR-10<br>NIST SP 800-53, SR-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • inspection of relevant documentation, such as policies and procedures for determining the authenticity of information system components prior to installation.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Observe appropriate personnel as they perform procedures for detecting and addressing counterfeit information system components.<br>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.<br>Determine whether counterfeit information system components are detected and appropriately addressed on a timely basis.<br>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. | |
| 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 relevant information system, as applicable.<br>Determine whether the types of configuration items for relevant information systems are clearly defined.<br>Note: To properly identify configuration items, it is important that the entity define the configuration items for entity information 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 | NIST SP 800-53, CM-02<br>NIST SP 800-53, CM-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for identifying configuration items and managing the configuration of such items.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that configuration items for information systems are properly identified and placed under configuration management.<br>Inspect listings of configuration items for the relevant information systems.<br>Determine whether configuration items for relevant information systems are properly identified and placed under configuration management. | NIST SP 800-53, CM-02<br>NIST SP 800-53, CM-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 Configuration settings are established and documented for configuration items. | | |
| CM.01.04.01 Configuration settings for configuration items are established, documented, and periodically reviewed and updated.<br>*Related controls: AC.01.01.02, AC.02.03.10, and CM.02.03.01* | Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating configuration settings for configuration items through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for establishing configuration settings for information systems and information system components that align with entity-level requirements.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the established configuration settings for a selection of configuration items for the relevant information systems. Consider whether these settings<br>• reflect the most restrictive mode consistent with operational requirements; | NIST SP 800-53, CM-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • align with entity-level requirements, including any entity-defined common secure configurations;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• are consistent with implemented configuration settings.<br>Determine whether the established configuration settings for the configuration items selected have been appropriately documented, periodically reviewed and updated, and properly approved.<br>Throughout the engagement, consider whether the established configuration settings for the configuration items for relevant information systems have been properly maintained.<br>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.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| CM.02 Management designs and implements general controls to manage changes to entity information systems and information system components. | | |
| CM.02.01 Planned changes to configuration items are formally authorized, analyzed, tested, and approved prior to implementation. | | |
| CM.02.01.01 Entity-level and system-level processes for formally authorizing, testing, and approving planned changes to information systems and information system components are established and implemented.<br>*Related controls: SM.01.04.01 and CM.03.02.01* | Obtain an understanding of the entity-level and system-level processes and methods that the entity employs for formally authorizing, testing, and approving planned changes to information systems and information system components through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity-level and system-level processes. Consider whether the processes<br>• identify roles and responsibilities;<br>• are integrated with the entity's system development life cycle processes;<br>• address each type of change to information systems and information system components that is configuration controlled and subject to the entity-level and system-level processes, as applicable;<br>• specify the processes and methods employed for authorizing, testing, and approving planned changes to information systems and information system | NIST SP 800-53, CM-03<br>NIST SP 800-53, SA-10<br>NIST SP 800-53, SA-11<br>NIST SP 800-53, SA-15<br>NIST SP 800-53, SA-17 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | components, as well as retaining records of such actions for subsequent review and monitoring;<br>• specify the processes and methods for updating baseline configuration documentation as part of the change management process;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• are adequate to facilitate and document controlled modifications to hardware, firmware, and software components of entity information systems.<br>Inspect a selection of changes to configuration items for each relevant information system.<br>Determine whether the entity-level 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.<br>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. | Obtain an understanding of the entity's processes and methods for considering proposed changes to software for the relevant information systems through | NIST SP 800-53, SA-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| *Related control: BP.04.07.01* | • inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>Inspect available documentation for any changes to software for the relevant information systems that were implemented (or are expected to be implemented) during the audit period. Consider whether the documentation<br>• demonstrates that proposed changes are considered and authorized prior to development and<br>• facilitates tracing of source code to the design specifications and functional requirements associated with authorized changes.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect any security or privacy impact analyses conducted in connection with planned changes to the relevant information systems. Consider whether such analyses<br>• have been appropriately documented, approved, and disseminated and<br>• are appropriately considered as part of the processes for formally authorizing, testing, and approving planned | NIST SP 800-53, CM-04<br>NIST SP 800-53, RA-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | changes to information systems and information system components.<br>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.<br>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 the privacy of individuals and the ability of implemented controls to mitigate those risks.<br>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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures. | NIST SP 800-53, SA-11 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect available documentation for any changes to the relevant information systems that were implemented (or are expected to be implemented) during the audit period. Consider whether the documentation<br>• provides sufficient evidence of the approval, execution, and review of test plans and results, as appropriate;<br>• 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;<br>• clearly presents the results of testing, including any flaws identified;<br>• identifies the necessary resources, planned actions, and time frames for flaw remediation; and<br>• 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.<br>Inspect available documentation for flaw remediation. Consider whether all flaws identified through testing are remediated or tracked for remediation.<br>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.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 that the entity employs to support the system development and configuration management processes applicable to the relevant information systems through<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's system development and configuration management tools and software, and<br>• inspection of relevant documentation, such as policies and procedures for using and managing the entity's system development and configuration management tools and software, as well as implemented configuration settings, found in system configuration files for the tools and software employed.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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. | NIST SP 800-53, SA-15 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>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 systems and information system components are established and implemented.<br>*Related controls: SM.01.04.01, AC.02.03.06, and CM.03.02.01* | Obtain an understanding of the entity-level and system-level processes and methods that the entity employs for documenting, analyzing, and reviewing emergency changes to information systems and information system components through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, CM-03<br>NIST SP 800-53, SA-10<br>NIST SP 800-53, SA-11<br>NIST SP 800-53, SA-15<br>NIST SP 800-53, SA-17 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect documentation demonstrating the design and implementation of the entity-level and system-level processes. Consider whether the processes<br>• identify roles and responsibilities;<br>• are integrated with the entity's system development life cycle processes;<br>• define emergency changes and address each type of change to information systems and information system components that is subject to the entity-level and system-level processes for implementing emergency changes, as applicable;<br>• 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;<br>• specify the processes and methods for updating baseline configuration documentation as part of the change management process;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• 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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect a selection of emergency changes to configuration items for each relevant information system.<br>Determine whether the entity-level 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.<br>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.<br>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 established configuration settings and unauthorized changes. | | |
| CM.02.03.01 Deviations from established configuration settings are properly identified and appropriately addressed on a timely basis.<br>*Related control: CM.01.04.01* | Obtain an understanding of the entity's processes and methods for identifying and addressing deviations from established configuration settings through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as comparing policies and procedures for monitoring implemented configuration settings for information systems and information system components against | NIST SP 800-53, CM-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | established configuration settings, including any such settings derived from entity-defined common secure configurations.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Observe appropriate personnel as they perform procedures for identifying and addressing deviations from established configuration settings.<br>Obtain an understanding of any automated tools the entity uses to facilitate compliance with established 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 established configuration settings and alert appropriate personnel.<br>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<br>• changing implemented configuration settings for configuration items through a formal configuration management process,<br>• 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<br>• approving the deviation and accepting the risk associated with it.<br>Inspect implemented configuration settings for a selection of configuration items for the relevant information systems. Consider | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | whether the implemented settings align with the established configuration settings for the configuration items.<br>Determine whether deviations from established configuration settings are properly identified and appropriately addressed on a timely basis.<br>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.<br>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<br>• inquiry of appropriate personnel and<br>• 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.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, SI-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 start-up, restart, shutdown, and abort.<br>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.<br>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.<br>*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<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's integrity verification tools, and<br>• 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.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, SI-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 systems and their components. Consider whether appropriate personnel properly reviewed such output and took appropriate, timely action to address any unauthorized changes detected.<br>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.<br>Determine whether management properly employs integrity verification tools to detect unauthorized changes to systems and their components.<br>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.<br>*Related controls: SD.01.02.02 and AC.02.03.06* | 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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as system design documentation, system security and privacy plans, and system-level configuration management plans. | NIST SP 800-53, SA-03<br>NIST SP 800-53, SC-32<br>NIST SP 800-53, SC-49<br>NIST SP 800-53, SC-50 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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<br>• are suitably designed and properly implemented based on risk;<br>• facilitate segregation of duties for program development and implementation, including the movement of programs between environments; and<br>• reasonably assure that the development, test, integration, and production environments are sufficiently separated and appropriately controlled.<br>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.<br>Determine whether the development, test, integration, and production environments for relevant information systems are sufficiently separated and appropriately controlled.<br>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. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as system design documentation, system security and privacy plans, and system-level configuration management plans.<br>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<br>• are suitably designed and properly implemented based on risk and<br>• reasonably assure that source code repositories and program libraries are sufficiently separated and appropriately controlled.<br>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.<br>Determine whether source code repositories and program libraries for relevant information systems are sufficiently separated and appropriately controlled.<br>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 | NIST SP 800-53, CM-05<br>NIST SP 800-53, SA-08<br>NIST SP 800-53, SA-10 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's system development and configuration management tools and software, and<br>• inspection of relevant documentation, such as policies and procedures for the entity's system development and configuration management processes.<br>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.<br>Determine whether logical access to the tools and software that support the entity's system development and configuration management processes is appropriately controlled. | NIST SP 800-53, CM-05<br>NIST SP 800-53, SA-03 |
| CM.03 Management designs and implements general controls to protect information systems and information system components from vulnerabilities, flaws, and threats. | | |
| CM.03.01 Vulnerability monitoring is routinely conducted. | | |
| CM.03.01.01 Entity-level and system-level processes for vulnerability monitoring and scanning are established and implemented. | Obtain an understanding of the entity-level and system-level processes and methods that the entity employs for conducting | NIST SP 800-53, RA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| *Related controls: SM.04.01.01, SM.04.01.02, SM.06.01.01, and AC.02.03.10* | vulnerability monitoring and scanning for relevant information systems and their components through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity and system-level processes. Consider whether the processes<br>• identify roles and responsibilities;<br>• are integrated with the entity-level risk management strategy, as well as the entity-level and system-level continuous monitoring strategies, as applicable;<br>• specify the processes and methods employed for vulnerability monitoring and scanning and for analyzing their results;<br>• 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;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • are adequate to facilitate the proper identification and timely remediation of control deficiencies and vulnerabilities.<br>Determine whether the entity-level and system-level processes for vulnerability monitoring and scanning for relevant information systems and their components are designed, implemented, and operating effectively.<br>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.<br>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 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.<br>*Related control: SM.04.02.03* | Obtain an understanding of the tools and software that the entity employs to support the vulnerability monitoring and scanning processes applicable to the relevant information systems through<br>• inquiry of appropriate personnel, including IT management personnel responsible for the entity's vulnerability monitoring and scanning tools and software, and<br>• inspection of relevant documentation, such as policies and procedures for using and managing the entity's | NIST SP 800-53, RA-05 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | vulnerability monitoring and scanning tools and software, as well as implemented configuration settings, found in system configuration files for the tools and software employed.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether management properly employs appropriate tools and software to support the entity's vulnerability monitoring and scanning processes applicable to relevant information systems.<br>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 ensure that potential vulnerabilities in information systems and information system components are identified and addressed as quickly as possible.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>*Related controls: SM.04.01.01, SM.04.01.02, SM.06.01.01, CM.02.01.01, and CM.02.02.01* | Obtain an understanding of the entity-level and system-level processes and methods that the entity employs for flaw remediation, including patch management, for relevant information systems and their components through<br>• inquiry of appropriate personnel,<br>• inspection of relevant policies and procedures, and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity-level and system-level processes. Consider whether the processes<br>• identify roles and responsibilities;<br>• are integrated with the entity-level risk management strategy, as well as the entity-level and system-level continuous monitoring strategies, as applicable;<br>• are incorporated into 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; | NIST SP 800-53, SI-02 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • specify the processes and methods employed for timely flaw remediation, including patch management;<br>• have been recently reviewed and updated, as appropriate;<br>• have been approved by the appropriate senior official(s); and<br>• are adequate to facilitate the proper identification and timely remediation of control deficiencies and vulnerabilities.<br>Inspect a selection of vendor-recommended patches and compare them to those installed on relevant information systems. Consider whether all available patches have been installed and conduct follow-up with management on any exceptions.<br>Determine whether the entity-level and system-level processes for flaw remediation, including patch management, for relevant information systems and their components are designed, implemented, and operating effectively.<br>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.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | tolerance, the mission or business functions that the information system supports, or the threat environment.<br>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-level and system-level processes for managing planned and emergency changes to information systems and information system components. In some situations, entities may determine that 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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>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. Consider whether such components are scheduled for replacement or supported by other means through alternative sources.<br>Determine whether unsupported system components are replaced or alternative sources for continued support are identified and employed on a timely basis. | NIST SP 800-53, SA-22 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>Determine whether the spam and malicious code protection mechanisms selected for use in connection with relevant information systems and their components are appropriate based on risk.<br>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 | NIST SP 800-53, SC-35<br>NIST SP 800-53, SI-03<br>NIST SP 800-53, SI-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>*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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Consider whether the policies and procedures<br>• identify roles and responsibilities;<br>• 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;<br>• 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;<br>• have been recently reviewed and updated;<br>• have been approved by the appropriate senior officials; and | NIST SP 800-53, CM-14 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • are adequate to prevent unsigned software and firmware components from being installed.<br>Inspect a selection of software and firmware components for the relevant information systems. Consider whether such components are signed with an entity-approved certificate.<br>Determine whether management adequately prevents the installation of software and firmware components lacking recognized and approved digital signature certificates for relevant information systems.<br>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. | |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-26-108633

## 570 FISCAM Framework for Contingency Planning

570.01 The contingency planning (CP) category provides 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 resources and minimizing the risk of unplanned interruptions. It also involves having a plan to recover and reconstitute information systems should system disruptions occur.

570.02 The FISCAM Framework for Contingency Planning (see table 14) includes two critical elements:

- CP.01 Management designs and implements controls to achieve continuity of operations and prioritize the recovery and reconstitution of information systems that support critical or essential mission and business functions in the event of a system disruption, compromise, or failure.
- CP.02 Management designs and implements general controls to prevent or minimize system disruption and potential damage to information resources and facilities due to natural disasters, structural failures, hostile attacks, or errors.

570.03 Assessing contingency planning controls involves evaluating management's efforts to satisfy each of these critical elements. When evaluating management's efforts for each critical element, the auditor considers whether the associated control objectives (shown in table 14), if achieved, will address IS control risk relevant to the engagement objectives. Ineffective contingency planning controls may result in lost or incorrectly processed data caused by a system disruption, compromise, or failure, which can result in financial losses, expensive recovery efforts, and inaccurate or incomplete information.

**Table 14: FISCAM Framework for Contingency Planning (CP)**

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| CP.01 Management designs and implements general controls to achieve continuity of operations and prioritize the recovery and reconstitution of information systems that support critical or essential mission and business functions in the event of a system disruption, compromise, or failure. | | |
| CP.01.01 Criticality analyses are performed to prioritize mission and business functions and determine the criticality of information systems, information system components, and information system services. | | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| 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<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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.<br>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 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. | NIST SP 800-53, RA-09<br>NIST SP 800-53, SA-20 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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.<br>*Related control: CP.01.04.02* | Obtain an understanding of the entity's processes and methods for developing, documenting, and periodically reviewing and updating system-level contingency plans through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation, such as policies and procedures for developing contingency plans.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect the contingency plans for each relevant information system, as applicable. Consider whether the plans<br>• 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;<br>• are based on current information and reflect current conditions, including contingency roles, responsibilities, and assigned individuals with contact information;<br>• have been recently reviewed and updated;<br>• have been approved by the appropriate senior officials; | NIST SP 800-53, CP-02<br>NIST SP 800-53, CP-10<br>NIST SP 800-53, CP-12<br>NIST SP 800-53, SC-24 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • are integrated with the risk management and system development life cycle processes;<br>• 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;<br>• address information system interdependencies;<br>• include required information in accordance with authoritative criteria;<br>• identify and allocate appropriate resources to support achieving continuity of operations and prioritize recovery and reconstitution procedures;<br>• address the failure and timely recovery and reconstitution of the information system and system components to a known state;<br>• 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<br>• are adequate to address eventual, full-system restoration and implementation of alternative mission or business processes without deterioration of the controls originally planned and implemented. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether the contingency plans for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.<br>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.<br>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<br>• inquiry of appropriate personnel and<br>• inspection of relevant entity documentation.<br>Inspect the critical infrastructure and key resources protection plan. Consider whether the plan<br>• has been recently reviewed and updated, as appropriate;<br>• has been approved by the appropriate senior official(s);<br>• includes required information in accordance with authoritative criteria; | NIST SP 800-53, PM-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • is consistent with relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, and guidelines;<br>• 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;<br>• 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<br>• addresses the relevant information systems.<br>Determine whether the crucial infrastructure and key resources protection plan has been appropriately developed, documented, disseminated, and periodically reviewed and updated.<br>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 | 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-02<br>NIST SP 800-53, CP-03<br>NIST SP 800-53, SI-17 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| contingency plan testing or actual system 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<br>• inspection of relevant documentation.<br>Inspect documentation for contingency training for each relevant information system, as applicable. Consider whether<br>• 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;<br>• lessons learned from contingency plan testing or actual system disruptions are incorporated into course materials and training techniques;<br>• mandatory training courses are identified and communicated to information system users as a condition for system access, as applicable; and<br>• management monitors and maintains records of the completion status of applicable mandatory training courses for information system users.<br>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.<br>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.<br>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 | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | specific instructions on subsequent steps to take. Subsequent steps 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 relevant information systems through<br>• inquiry of appropriate personnel, including users and authorizing officials;<br>• inspection of relevant policies and procedures for contingency plan testing; and<br>• inspection of other relevant documentation demonstrating the design and implementation of the processes.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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.<br>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. | NIST SP 800-53, CP-04 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 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.<br>*Related control: CP.01.02.01* | Inspect contingency plan test results documented for the relevant information systems.<br>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-02<br>NIST SP 800-53, CP-04 |
| CP.02 Management designs and implements general controls to prevent or minimize system disruption and potential damage to information resources and facilities due to natural disasters, structural failures, hostile attacks, or errors. | | |
| CP.02.01 Environmental controls are appropriately selected and employed based on risk. | | |
| CP.02.01.01 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 that the entity employs for the facilities where relevant information resources reside through<br>• inquiry of appropriate personnel;<br>• inspection of relevant documentation; and<br>• observation of the entity's use of climate controls to maintain and monitor temperature, humidity, and other environmental factors.<br>Perform walk-throughs of the facilities where relevant information resources reside. Identify the climate controls that the entity employs. Consider whether the selection and employment of climate controls to maintain and monitor temperature, humidity, and other environmental factors are appropriate based on risk. | NIST SP 800-53, PE-14 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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 relevant information systems reside.<br>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 information resources from water damage. | Obtain an understanding of any master shutoff or isolation valves that the entity employs for the facilities where relevant information resources reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the location of any master shutoff or isolation valves within the facilities.<br>Perform walk-throughs of the facilities where relevant information resources reside. Identify any master shutoff or isolation valves that the entity employs. Consider whether the location of such valves would facilitate timely access during an emergency to prevent or minimize water damage to relevant information resources.<br>Determine whether the master shutoff or isolation valves identified are accessible, functional, and known to appropriate personnel to adequately protect relevant information resources from water damage.<br>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 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| CP.02.01.03 Emergency shutoff switches are accessible, functional, and known to appropriate personnel to provide the capability of shutting off power to information systems in the event of an emergency. Access to emergency shutoff switches is appropriately controlled. | Obtain an understanding of any emergency shutoff switches that the entity employs for the facilities where relevant information systems reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the location of any emergency shutoff switches within the facilities.<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify any emergency shutoff switches that the entity employs. 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.<br>Determine whether the emergency shutoff switches are accessible, functional, and known to appropriate personnel to provide the capability of shutting off power to relevant information systems in the event of an emergency. Determine whether access to emergency shutoff switches is appropriately controlled. | NIST SP 800-53, PE-10 |
| CP.02.01.04 Management maintains and monitors fire detection and suppression systems for facilities where information systems reside. | Obtain an understanding of the fire detection and suppression systems that the entity employs for the facilities where relevant information systems reside through<br>• inquiry of appropriate personnel,<br>• inspection of relevant documentation, and<br>• observation of the entity's use of fire detection and suppression systems.<br>Perform walk-throughs of the facilities where relevant information systems reside. Identify the fire detection and suppression systems | NIST SP 800-53, PE-13 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | that the entity employs. Consider whether an independent power source supports the fire detection and suppression systems.<br>Determine whether management adequately maintains and monitors fire detection and suppression systems for the facilities where relevant information systems reside.<br>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 if the primary processing or storage sites are unavailable. | Obtain an understanding of any alternate processing or storage sites that the entity employs for the relevant information systems through<br>• inquiry of appropriate personnel;<br>• 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, if the primary processing or storage sites are unavailable; and<br>• observations of alternate processing and storage sites.<br>Perform walk-throughs of the alternate processing and storage sites where relevant information systems 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 whether the controls at the alternate processing and storage sites are | NIST SP 800-53, CP-06<br>NIST SP 800-53, CP-07<br>NIST SP 800-53, PE-17 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | equivalent or commensurate to those at the primary processing and storage sites.<br>Determine whether sufficiently separated alternate processing and storage sites are maintained for the relevant information systems to provide and support processing capabilities when the primary processing or storage sites are unavailable.<br>Note: While distinct from alternate processing sites, alternate worksites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate worksites or types of sites depending on the work-related activities conducted at the sites. Alternate worksites 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 if the primary telecommunications services are unavailable. | Obtain an understanding of any alternate telecommunications services that the entity employs for the relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>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.<br>Determine whether alternate telecommunication services are available for relevant information systems. | NIST SP 800-53, CP-08 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| CP.02.02.03 Alternate security mechanisms for critical security functions are established to control access if the primary security mechanisms are unavailable or compromised. | Obtain an understanding of any alternate security mechanisms that the entity employs for the relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect documentation demonstrating the design and implementation of any alternate security mechanisms that the entity employs for relevant information systems.<br>Determine whether alternate security mechanisms for critical security functions are available and appropriate for the relevant information systems.<br>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<br>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 relevant information systems reside through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Perform walk-throughs of the facilities where relevant information systems reside.<br>Inspect the results of any recent tests of the entity's uninterruptible power supply. Consider whether the uninterruptible power supply 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. | NIST SP 800-53, PE-11<br>NIST SP 800-53, PE-12 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether, in the event of a loss of the primary power source at the facilities where relevant information systems 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 relevant information resources reside through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Perform walk-throughs of the facilities where relevant information resources reside.<br>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.<br>Determine whether, in the event of a loss of the primary power source at the facilities where relevant information 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 that the entity employs to support continuity of operations in the event of a system disruption through<br>• inquiry of appropriate personnel and<br>• inspection of relevant documentation.<br>Inspect documentation demonstrating the design and implementation of any alternate communications protocols or alternate | NIST SP 800-53, CP-11<br>NIST SP 800-53, SC-47 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | communications paths that the entity employs for the relevant information systems.<br>Determine whether alternate communications mechanisms are available and appropriate for relevant information systems.<br>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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of system-level contingency plans for each relevant information system, as applicable.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity's processes for conducting system backups for relevant information systems. Consider whether<br>• the frequency at which system backups are conducted is adequate, | NIST SP 800-53, CP-09 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • access to system backups is appropriately controlled, and<br>• the retention periods for system backups are aligned with entity-level policies.<br>See also AC.03.02.01 and AC.03.02.02.<br>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.<br>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 are 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<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of system-level contingency plans for each relevant information system, as applicable.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>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<br>• the locations of the alternate processing or storage sites are appropriate to minimize disruption and | NIST SP 800-53, CP-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | • the methods used to transport, receive, and replace system backups permit them to be tracked throughout the process.<br>See also AC.03.01.03, AC.03.01.04, and AC.03.01.05.<br>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.<br>Determine whether system media containing backup data and software are 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 relevant information systems through<br>• inquiry of appropriate personnel;<br>• inspection of relevant policies and procedures; and<br>• inspection of maintenance contracts or service agreements with external parties, as applicable.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.<br>Inspect documentation demonstrating the design and implementation of the entity's processes for approving, controlling, and monitoring the use of system maintenance tools.<br>Inspect documentation demonstrating the design and implementation of the entity's processes for obtaining maintenance support, as well as | NIST SP 800-53, MA-03<br>NIST SP 800-53, MA-05<br>NIST SP 800-53, MA-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | any spare parts or replacement hardware needed to perform system component maintenance on a timely basis. Consider whether<br>• the entity has established a process for authorizing access for external personnel engaged to perform system component maintenance,<br>• maintenance contracts or service agreements include provisions to define timeliness and specify requirements for completing timely maintenance,<br>• requirements for the performance of system component maintenance in accordance with vendor specifications are included in the entity's policies and procedures, and<br>• the entity maintains an inventory of spare parts or replacement hardware for system components that support critical or essential mission and business functions.<br>Inspect available documentation for a selection of system components to assess whether maintenance has been performed for such components in accordance with vendor specifications.<br>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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, MA-06 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | 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<br>• flexibility exists in operations, including processing for critical or essential mission and business functions, to accommodate regularly scheduled maintenance and a reasonable amount of unscheduled maintenance;<br>• management has established goals for the availability of services and processing capabilities;<br>• 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<br>• performance measures and compliance metrics are periodically evaluated and appropriately employed to measure the effectiveness or efficiency of system component maintenance.<br>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 relevant information systems through<br>• inquiry of appropriate personnel and<br>• inspection of relevant policies and procedures.<br>See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures. | NIST SP 800-53, MA-02<br>NIST SP 800-53, MA-04<br>NIST SP 800-53, MA-05<br>NIST SP 800-53, MA-07 |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Inspect documentation demonstrating the design and implementation of the entity's processes for controlling system component maintenance for relevant information systems. Consider whether<br>• management reviews and approves maintenance activities, regardless of whether such activities are performed locally or remotely;<br>• the removal of a system component from an entity facility for maintenance, repair, or replacement requires explicit approval from management;<br>• affected, or potentially affected controls, are tested to determine whether such controls operate as intended following system component maintenance;<br>• records, which provide evidence for all maintenance actions and approvals, are properly prepared and maintained;<br>• 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;<br>• strong authentication methods and appropriate session-level controls are employed in connection with remote maintenance and diagnostic activities;<br>• field maintenance is appropriately controlled;<br>• entity personnel with adequate technical competence supervise or oversee the performance of maintenance activities; and<br>• maintenance activities are appropriately logged and adequately monitored. | |

| Illustrative controls | Illustrative audit procedures | Reference(s) to NIST SP 800-53 (rev. 5) controls |
|---|---|---|
| | Determine whether management performs system component maintenance for relevant information systems in a controlled manner. | |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-26-108633

# SECTION 600

## Appendixes

## Appendix 600A Glossary

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 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 control category within the FISCAM Framework that relates to limiting access or detecting inappropriate access to information resources (e.g., data and information technology) and facilities, thereby protecting these resources against unauthorized modification, disclosure, or destruction; and intentional or unintentional loss or impairment. See also logical access control and physical access control. |
| **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 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. |
| **accuracy** | An information processing objective that aims to provide reasonable assurance that data relating to transactions, events, and balances are properly and timely recorded. |
| **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 worksite** | 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** | One of the three types of information system controls that are incorporated directly into application software to control the input, processing, and output of data. These controls are designed to achieve three information processing objectives: completeness, accuracy, and validity of transactions and 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, timing, and extent of audit procedures applied to the significant business processes and areas of audit interest based on the relevant control objectives and the relevant information system (IS) controls. |
| **appropriateness** | The measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the engagement objectives and supporting findings and conclusions. |
| **areas of audit interest** | A subset of the entity's information systems that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. At the business process level, areas of audit interest may include business process applications, process automation software, system interfaces, data management systems, specific data files, and system-generated reports. At the system level, areas of audit interest may |

| | |
|---|---|
| | include operating systems, access control software, and hardware devices used for information processing, data storage, and network communications. |
| **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. |
| **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 period. |
| **audit plan** | Audit documentation that describes (1) the nature and extent of planned audit procedures for the planning phase of the IS controls assessment; (2) the nature, timing, and extent of planned audit procedures for the testing of relevant IS controls for each area of audit interest; and (3) other planned audit procedures that are required to be carried out so that the engagement complies with generally accepted government auditing standards. |
| **audit procedure** | The specific steps and tests auditors perform to address the engagement objectives. Specific tests include inquiry, observation, and inspection. See also walk-through. |
| **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 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 that agency information systems inherit. Authorization is also known as authorization to operate and accreditation. |
| **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. Authorization boundary is also known as accreditation boundary. |
| **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 an entity achieves its operating, reporting, and compliance objectives. Business processes transform inputs into outputs through a series of transactions or activities. 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 classes of transactions. |
| **business process application** | An application that helps the entity perform a specific business process or related business processes within a business function. |
| **business process controls** | A control category within the FISCAM Framework that relates to the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions. Business process controls include direct general controls that support information processing objectives. |

| | |
|---|---|
| **business process level** | The level at which user, application, and general controls relevant to specific business processes are implemented. These controls are specific to a business process and often correspond to information resources employed by the business process—business process applications, process automation software, system-generated reports, system interfaces, and data management systems. |
| **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 several 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<br>(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 entity in a manner consistent with statutes, regulations, executive orders, directives, implementing guidance, policies, and priorities established by the head of the entity;<br>(2) developing, maintaining, and facilitating the implementation of a sound, secure, and integrated IT architecture for the entity; and<br>(3) promoting the effective and efficient design and operation of all major information |

| | |
|---|---|
| | resources management processes for the executive entity, including improvements to the entity's work processes. |
| **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 in 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. |
| **complementary user entity controls** | Controls that management of the service organization assumes, in the design of its service, will be implemented by entities that use its service and are necessary to achieve control objectives stated in management's description of the service organization's system. |
| **completeness** | An information processing objective that aims to provide reasonable assurance that all valid transactions, events, and balances have been properly recorded. |

| | |
|---|---|
| **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 regarding 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 control category within the FISCAM Framework that relates to 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. |
| **contingency planning** | A control category within the FISCAM Framework that provides 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 actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels. |

| | |
|---|---|
| **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** | Broad groupings of controls based on similar types of risk. Control categories consist of the following: business process controls, security management, access controls, configuration management, segregation of duties, and contingency planning. |
| **control deficiency** | A condition when the design, implementation, or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct errors in information processing on a timely basis. The definition of control deficiency may differ by engagement type. For federal 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 depends on the effectiveness of other controls. |
| **control environment** | One of the five components of internal control. The control environment is the foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives. |
| **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 to achieving the critical elements. |
| **criteria** | The relevant provisions in statutes, regulations, executive orders, implementing guidance, directives, policies, contracts, grant |

| | |
|---|---|
| | agreements, standards, measures, expected performance, defined business practices, defined benchmarks, or other guidance against which performance is compared or evaluated. 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. |
| **critical elements** | Components of a control category that are necessary for maintaining 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 these. |
| **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 is used initially to set up and periodically change the operations performed in cryptographic equipment to encrypt or decrypt electronic signals, 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, which is fundamental to an efficient, effective transaction processing function. |
| **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 cyberthreat 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. |
| **detailed test plan** | Audit documentation that (1) identifies the area of audit interest; (2) explains the relationship of the area of audit interest to the significant business processes and any other areas of audit interest, as applicable; (3) identifies the relevant control objectives; (4) identifies the relevant IS controls selected for testing that are likely to achieve the relevant control objectives; (5) describes the nature, timing, and extent of IS control tests for each relevant IS control; (6) documents the results of completed IS control tests; and (7) provide links to supporting documentation. |
| **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. |
| **direct general controls** | Those controls that apply to information systems used within the business process and directly support the effective operation of user and application controls. See also general controls and indirect general controls. |
| **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** | The level at which general controls relevant to the entire entity or component are implemented. These controls are broader than those applied at the system level and often correspond to the entity’s information security management program or most of its information systems. |
| **entity risk assessment** | One of the five components of internal control. Entity risk assessment is the identification and analysis of risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. |
| **entry points** | Access points to the entity’s information systems. These may include remote access |

| | |
|---|---|
| | through dial-up, wireless devices, or the internet. |
| **environmental controls** | A subset of contingency planning general 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, the 2014 statute amended the U.S. Code to establish a new subchapter on information security (*codified, as amended, at* 44 U.S.C. §§ 3551-3559). In FISCAM, "FISMA" sometimes refers to both the 2014 statute and its 2002 predecessor collectively. |
| **field** | A location in a record in which a particular type of data are 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 file name. |
| **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. |
| **flowchart** | 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** | An intentional 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 or GAGAS, standards that 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.<br><br>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. |
| **general controls** | One of the three types of information system controls that establish actions through 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 mitigate information security risks and maintain a suitable environment to support the effective operation of user and application controls. See also direct general controls and indirect general 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 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. |
| **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. |
| **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. |
| **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 multiple 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. |
| **indirect general controls** | Those controls that apply to the information security management program and information systems. These controls maintain a suitable environment to support the effective operation of user, application, and direct general controls within the business process. See also general controls and direct general controls. |
| **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 and communication** | One of the five components of internal control. Information and communication consists of the quality information management and other personnel communicate and use to support the internal control system. |
| **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 resources** | The people, processes, data, and information technology used to collect, process, store, maintain, use, share, disseminate, or dispose of information. |
| **information security** | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. |
| **information security management program** | A program designed, implemented, and operated to reasonably assure that adequate |

| | |
|---|---|
| | information security is provided for all information collected, processed, transmitted, stored, or disseminated by an entity's information systems. |
| **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 security objectives** | Requirements for effective information security, including confidentiality, integrity, and availability. |
| **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 systems comprise the entity's IT applications and supporting IT infrastructure. |
| **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** | Internal controls that depend on information system processing. They include user controls, application controls, and general controls. |
| **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 using information technology. |
| **information system control risk** | The likelihood that conditions or events related to the areas of audit interest (1) could significantly affect the entity's ability to achieve its information processing objectives (completeness, accuracy, and validity), and (2) will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls. |
| **information system control risk factors** | Conditions or events that affect the susceptibility of the area of audit interest to information system processing errors due to ineffective general controls. |
| **information technology (IT)** | The hardware, software, firmware, equipment, media, and services used for information system processing. |
| **information technology environment** | The entity's IT operations and the IT applications and supporting IT infrastructure that an entity uses to support its operations and achieve strategic objectives. |
| **infrastructure** | The physical information system resources necessary to run software that 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. |
| **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 common boundary between information systems and information system components where interactions take place. Interfaces include system interconnections and system information exchanges. Interface also refers to the portion of a program that interacts with the user. The terms system interface and user interface may also be used in FISCAM. |
| **interface design** | Uses guidelines set by the system interface strategy and provides specific information for each of the characteristics defined in the system interface strategy. |
| **interface strategy** | Describes at the highest level how the system 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, ongoing system balancing requirements, and security requirements. |
| **internal control** | A process effected by an entity's oversight body, management, and other personnel designed to provide reasonable assurance that the entity's objectives will be achieved. Oversight body is equivalent to "those charged with governance" in financial audits. |
| **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 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 it needs to perform its function. |
| **library** | A collection of similar files, such as datasets 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 datasets.<br><br>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** | Involves requiring users to authenticate themselves, limiting their access to files and other resources, and limiting the actions that they can execute. Such controls are also referred to as logical security. See also access controls. |
| **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. |
| **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 engagement 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. |
| **monitoring** | One of the five components of internal control. Monitoring 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. |
| **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. |
| **nonstatistical selection** | A method of selecting items from a population to reach a conclusion only on the items selected. This selection method is not representative of the population and not projectable to the portion of the population that was not selected. To determine whether sufficient evidence has been obtained to conclude on the effectiveness of the controls tested, the auditor considers the results of the nonstatistical selection in conjunction with other sources of evidence. |
| **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 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 resources and facilities. See also access controls. |
| **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<br>(1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;<br>(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<br>(3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy concerns.<br>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 program, the role of the privacy officer and other privacy officials and staff, the strategic goals and objectives of the 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 relevant provisions in 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 functions, including those relevant to security, 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** | Technology that is privately owned, based on trade secrets, or privately developed, 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. |
| **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 information system controls** | Those user, application, and general controls that are suitably designed and are necessary to achieve relevant control objectives and that the auditor plans to test for implementation and operating effectiveness. |
| **relevant control objectives** | Those control objectives pertaining to areas of audit interest that are necessary to achieve the engagement objectives. |
| **relevant information systems** | A subset of the entity's information systems that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. See also areas of audit interest. |
| **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 factor** | A characteristic used in a risk model as an input to determine 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. |
| **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. The term 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 IS controls assessment that is directly tied to the engagement objectives. |
| **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 Instruction 1253 for national security systems and in Federal Information Processing Standard 199 for other than national security systems. |
| **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. A security configuration checklist may also be referred to as a lockdown guide, a hardening guide, a security guide, secure configuration, security |

| | |
|---|---|
| | technical implementation guide (STIG), or a benchmark. |
| **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 control category within the FISCAM Framework that provides the foundation of a security-control structure and reflects senior management's commitment to addressing security risks. |
| **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 control category within the FISCAM Framework that relates to the 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** | An organization or segment of an organization that provides services to other entities. 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 audits. |
| **significant business process** | Business processes that are significant to the engagement objectives. |
| **simple random selection** | A method of selecting a sample of items from a population in which each item of the population has an equal probability of selection. |
| **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 facilitates 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. |
| **sufficiency** | The measure of the quantity of evidence used to support the findings and conclusions related to the engagement objectives. |
| **switch** | A network component that filters and forwards packets between local area network segments. |
| **system** | See information system. |
| **systematic random selection** | A method of selecting a sample of items from a population in which a uniform interval is determined, a starting point is randomly selected in the first interval, and then every kth unit is selected. |
| **system administrator** | An individual, group, or organization responsible for setting up and maintaining a system or specific system elements, implementing approved secure baseline configurations, incorporating secure configuration settings for information system components, and conducting or assisting 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, maintenance, and ultimately its disposal. |
| **system information exchange** | Access to or the transfer of data outside of system authorization boundaries to accomplish a mission or business function. This includes 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 hosted services by external parties; 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** | The level at which general controls relevant to an information system are implemented. These controls are specific to certain information systems 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. |
| **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 rate of 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 communications 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 controls** | One of the three types of information system controls that are performed by people interacting with information systems. These controls are designed to achieve three information processing objectives: completeness, accuracy, and validity of transactions and data. A user control is an information system control if its effectiveness depends on information system processing. |
| **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 scan** | 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. |
| **walk-through** | A combination of observation, inspection, and inquiry audit procedures that helps the auditor understand (1) the steps and information resources involved in a significant business process from beginning to end and (2) the design and implementation of the controls involved. When performing walk-throughs to obtain an understanding of a significant business process, the auditor generally traces one or more transactions, activities, or events from initiation through all processing, observing the processing in operation, inspecting relevant documentation, and making inquiries of entity staff. |
| **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 600B 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 audit documentation 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 audit documentation 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 audit documentation 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 and Review

| | | | |
|---|---|---|---|
| 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? | FISCAM, 220.03<br>GAGAS (2018), 4.02 | | |
| 2. If the auditor used the work of an IT specialist, did the auditor<br>• determine whether the specialist is competent in their area of specialization;<br>• obtain evidence concerning the specialist's qualifications and independence; and<br>• evaluate the adequacy of the work for the auditor's purposes, including<br>○ evaluating the findings and conclusions,<br>○ understanding and evaluating assumptions and methods, and<br>○ evaluating the relevance, completeness, and accuracy | FISCAM, 220.06, 220.10<br>GAGAS (2018), 4.12, 8.82 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| of source data that are significant to the work? | | | |
| 3. Did the auditor determine whether<br>• other auditors have completed or are completing IS controls work that is relevant to the engagement objectives, and if so<br>• the scope, quality, and timing of the audit work can be relied on in the context of current engagement objectives? | FISCAM, 220.08<br>GAGAS (2018), 8.80, 8.81 | | |
| 4. If the auditor used the work of other auditors, did the auditor<br>• obtain evidence concerning qualifications and independence of the other auditors and<br>• perform procedures that provided a sufficient basis for using the work? | FISCAM, 220.10<br>GAGAS (2018), 8.81 | | |
| 5. If the auditor determined that the work of the IT specialist was not adequate for the auditor's purposes, did the auditor ensure additional audit procedures appropriate to the circumstances were performed? | FISCAM, 220.11 | | |
| 6. If the engagement is a financial audit and the auditor used the work of an IT specialist or | FISCAM, 220.12 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| other auditors, did the auditor comply with the requirements in FAM 600? | | | |
| 7. Did the auditor obtain an understanding of the entity's IT environment sufficient to plan the engagement? | FISCAM, 230.02 | | |
| 8. Did the auditor ask management to identify previous audits, attestation engagements, and other studies that directly relate to the engagement objectives? | FISCAM, 230.03<br>GAGAS (2018), 6.11, 7.13, 8.30 | | |
| 9. Did the auditor evaluate whether the entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant to the engagement objectives? | FISCAM, 230.03<br>GAGAS (2018), 6.11, 7.13, 8.30 | | |
| 10. Did the auditor obtain an understanding of inherent risk factors related to the entity's IT environment? | FISCAM, 230.05 | | |
| 11. Did the auditor obtain an understanding of the entity's information security management program using the FISCAM Framework for Security Management? | FISCAM, 240.05, 240.07 | | |
| 12. Did the auditor identify business processes that are significant to the engagement objectives? | FISCAM, 250.06 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| 13. Did the auditor obtain an understanding of significant business processes by performing walk-throughs or alternative audit procedures? | FISCAM, 250.07 | | |
| 14. Did the auditor inspect available system 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, 250.13 | | |
| 15. Did the auditor identify and obtain a sufficient understanding of the business process controls designed to achieve information processing objectives (completeness, accuracy, and validity) based on the auditor's understanding of the significant business processes? | FISCAM, 250.15 | | |
| 16. Did the auditor appropriately identify relevant business process control objectives and the controls intended to achieve those objectives using the FISCAM Framework for Business Process Controls? | FISCAM, 250.16 | | |
| 17. If external parties performed any business process controls on behalf of the entity that were intended to achieve the relevant business process control objectives, did the auditor obtain an understanding of such controls sufficient to assess IS control risk on | FISCAM, 250.19, 250.20 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| a preliminary basis and design further audit procedures in response to those risks? | | | |
| 18. Did the auditor appropriately identify areas of audit interest at the business process and system levels? | FISCAM, 250.22 | | |
| 19. Did the auditor adequately identify IS control risk factors related to the areas of audit interest? | FISCAM, 260.07 | | |
| 20. Did the engagement team members adequately discuss fraud risk factors and appropriately assess the risk of fraud occurring that is significant to the engagement objectives? | FISCAM, 260.08<br>GAGAS (2018), 8.71 | | |
| 21. Did the auditor appropriately involve senior members of the engagement team in assessing IS control risk and determining the nature, timing, and extent of IS control tests in response to assessed risks? | FISCAM, 260.14, 260.16 | | |
| 22. Did the auditor adequately assess the level of IS control risk for each area of audit interest on a preliminary basis based on the auditor's<br>• understanding of inherent risk factors related to the IT environment, IS control risk factors, fraud risk factors, and any other factors or compensating controls that may | FISCAM, 260.14 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| mitigate the effects of identified risk factors; and<br>• consideration of information gathered to evaluate whether the entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant to the engagement objectives? | | | |
| 23. Did the auditor appropriately identify relevant general control objectives for each area of audit interest at the system and entity levels? | FISCAM, 270.02 | | |
| 24. Did the auditor use the FISCAM Framework (sections 530 through 570) to identify general control objectives relevant to the areas of audit interest? | FISCAM, 270.03, 270.06, 270.07, 270.08, 270.09 | | |
| 25. 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, and approach of the IS controls assessment? | FISCAM, 280.01<br>GAGAS (2018), 7.34, 8.132 | | |
| 26. Did the auditor adequately prepare a written description of each significant business process—including relevant information systems—sufficient to clearly identify the | FISCAM, 250.14, 280.02 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| areas of audit interest involved at the business process level, as well as business process controls applied to the significant business processes? | | | |
| 27. Did the auditor adequately prepare a written preliminary assessment of IS control risk for each area of audit interest that identifies the inherent risk factors, IS control risk factors, fraud risk factors, and results of previous engagements that significantly increase or decrease the auditor's assessed level of IS control risk? | FISCAM, 260.05, 280.03 | | |
| 28. Did the auditor adequately prepare and update a written planning memo for the IS controls assessment, including<br>• the identification of significant business processes;<br>• the identification of areas of audit interest at the business process and system levels;<br>• key decisions related to the areas of audit interest;<br>• the identification of relevant user, application, and general control objectives for each area of audit interest, as applicable; and | FISCAM, 280.04 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| • the auditor's basis for such scoping decisions? | | | |
| 29. Did the auditor adequately prepare, update, and complete, as appropriate, a written audit plan, including detailed test plans, for the IS controls assessment, that describes<br>• the nature and extent of planned audit procedures for the planning phase;<br>• the nature, timing, and extent of planned audit procedures for relevant control objectives for each area of audit interest; and<br>• other planned audit procedures that are required to be carried out so that the engagement complies with GAGAS? | FISCAM, 280.05, 280.06<br>GAGAS (2018), 8.03, 8.33 | | |
| 30. Did the auditor adequately complete the planning phase portion of this assessment completion checklist? | FISCAM, 280.07 | | |
| Section 2: Testing Phase | | | |
| 31. Did the auditor appropriately<br>• obtain a sufficient understanding of the design of the entity's IS controls that are likely to achieve the relevant | FISCAM 320.02, 320.03 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| control objectives for each area of audit interest, if implemented and operating effectively, and<br>• identify those controls that achieve the relevant control objectives and improve the efficiency of the auditor's IS control tests? | | | |
| 32. Did the auditor appropriately determine the nature of IS control tests for relevant IS controls? | FISCAM, 330.04, 330.05 | | |
| 33. If the auditor used entity-produced information as evidence, did the auditor perform audit procedures to assess the appropriateness of the information prior to performing IS control tests? | FISCAM, 330.07<br>GAGAS (2018), 8.93 | | |
| 34. If the auditor performed inquiries regarding the implementation and operating effectiveness of IS controls, did the auditor appropriately perform other audit procedures in combination with inquiry to obtain sufficient, appropriate evidence? | FISCAM, 330.10<br>GAGAS (2018), 8.94 | | |
| 35. Did the auditor appropriately determine the timing of IS control tests for relevant IS controls? | FISCAM, 330.04, 330.11 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| 36. Did the auditor appropriately determine the extent of IS control tests for relevant IS controls, including the use of statistical sampling or nonstatistical selection to identify items for control testing? | FISCAM, 330.04, 330.12, 330.16 | | |
| 37. If the auditor used statistical sampling to identify items within a population for control testing, did the auditor appropriately define and determine<br>• the objectives of the control test (including what constitutes a deviation),<br>• the population (including the sampling unit and time frame),<br>• the method of selecting the sample, and<br>• sample design and resulting sample size? | FISCAM, 330.18, 330.19, 330.20 | | |
| 38. If the auditor used statistical sampling to identify items within a population for control testing, did the team appropriately<br>• use attribute sampling;<br>• determine whether to stratify the population prior to sampling; and<br>• determine a sample size sufficient to obtain sufficient, appropriate audit evidence about the operating | FISCAM, 330.17, 330.18, 330.21, 330.24 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| effectiveness of relevant IS controls and reduce sampling risk to an acceptably low level? | | | |
| 39. If the auditor used automated audit tools, did the auditor adequately understand the following for each:<br>• what are the associated risks,<br>• when to use the tool,<br>• how to operate the tool,<br>• how to analyze the data, and<br>• how to interpret results? | FISCAM, 330.31 | | |
| 40. If the auditor used automated audit tools, did the auditor perform a technical review to verify that<br>• the use and operation of the automated audit tool is appropriate,<br>• the results the tool produces are complete and accurate, and<br>• that the conclusions are supported? | FISCAM, 330.32 | | |
| 41. If the auditor used a service organization report as evidence to support the effective design, implementation, and operation of IS controls, did the auditor determine whether the report provides sufficient, appropriate | FISCAM, 330.36 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| evidence about the design, implementation, and operating effectiveness of IS controls by<br>• assessing the adequacy of the standards under which the service auditor's report was issued;<br>• evaluating whether the report is for a period that is appropriate for the auditor's purpose;<br>• evaluating the adequacy of the relevant IS controls that the service organization performed, as described in the service auditor's report, to achieve relevant control objectives and the relevance and adequacy of the service auditor's tests of such controls;<br>• evaluating the adequacy of the period covered by the service auditor's tests of the IS controls the service organization performed and the time elapsed since performance of such tests;<br>• evaluating whether the results of the service auditor's tests of the IS controls the service organization performed, as described in the service auditor's report, provide | | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| sufficient, appropriate evidence to support the auditor's conclusions;<br>• determining whether complementary user entity controls that the service organization identified as necessary to support the effectiveness of relevant IS controls the service organization performed are designed, implemented, and operating effectively; and<br>• if applicable, evaluating the adequacy of any IS controls a subservice organization performed that are necessary to support the effectiveness of relevant IS controls that the service organization performed? | | | |
| 42. 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, 330.40 | | |
| 43. 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 controls, | FISCAM, 330.37 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| did the auditor comply with the requirements in FAM 640? | | | |
| 44. Did the auditor use suitable criteria to perform control tests of relevant IS controls? | FISCAM, 340.04<br>GAGAS 2018, 8.07 | | |
| 45. If the engagement is a financial audit, did the auditor comply with requirements for documenting IS controls that are included on the specific control evaluation worksheet as discussed in FAM 390? | FISCAM, 340.05 | | |
| 46. Did the auditor adequately evaluate the results of control tests to determine whether IS controls are implemented and operating effectively to achieve the relevant control objectives for each area of audit interest? | FISCAM, 340.06 | | |
| 47. 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 determining whether<br>• a control deficiency exists and<br>• the related control objective is achieved? | FISCAM, 340.07 | | |
| 48. Did the auditor appropriately determine whether there are specific compensating | FISCAM, 340.08 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| controls that could mitigate each potential IS control deficiency? | | | |
| 49. If compensating controls could adequately mitigate a potential IS control deficiency and achieve the related control objective, did the auditor obtain evidence that the compensating controls are designed, implemented, and operating effectively? | FISCAM, 340.08 | | |
| 50. Did the auditor appropriately communicate to management the criteria, condition, cause, and effect of the IS control deficiencies identified through the IS controls assessment? | FISCAM, 340.09<br>GAGAS (2018), 6.17, 7.19, 8.116 | | |
| 51. Did the auditor adequately evaluate and sufficiently document the significance of identified IS control deficiencies? | FISCAM, 340.10<br>GAGAS (2018), 8.54 | | |
| 52. Did the auditor adequately reassess, based on the audit procedures performed and the collective evidence obtained, the level of IS control risk for each area of audit interest? | FISCAM, 340.11 | | |
| 53. If IS control risk is assessed at moderate or high for one or more of the areas of audit interest, did the auditor appropriately determine the impact of the underlying control deficiencies on the effectiveness of relevant business process controls? | FISCAM, 340.11 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| 54. 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, 340.15<br>GAGAS (2018), 8.108 | | |
| 55. 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, 340.16<br>GAGAS (2018), 8.109 | | |
| 56. 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<br>GAGAS (2018), 7.34, 8.132 | | |
| 57. 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<br>• a completed written audit plan reflecting the results of the audit procedures performed,<br>• a written results memo describing the overall assessment of the collective | FISCAM, 350.02, 350.03, 350.04, 350.05<br>GAGAS (2018), 8.133, 8.134, 8.135 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| evidence obtained as well as the auditor's final determinations regarding IS control risk and audit risk, and<br>• detailed test plans documenting the approach for testing controls for the relevant control objectives for each area of audit interest? | | | |
| 58. If the auditor used statistical sampling to perform IS control tests, did the auditor prepare written sampling plans that include<br>• the objectives of each test (including what constitutes a deviation),<br>• the population (including sampling unit and time frame),<br>• the method of selecting the sample, and<br>• the sample design and resulting sample size? | FISCAM, 350.08 | | |
| 59. If the auditor used automated audit tools, 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<br>• the use and operation of the automated audit tool is appropriate, | FISCAM, 350.09 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| • the results produced by the automated audit tool are complete and accurate, and<br>• any conclusions are supported? | | | |
| 60. Did the auditor adequately complete the testing phase portion of this assessment completion checklist? | FISCAM, 350.10 | | |
| Section 3: Reporting Phase | | | |
| 61. Did the auditor adequately determine whether they followed the FISCAM methodology? | FISCAM, 420.01 | | |
| 62. For financial audit reports, did the overall engagement auditor comply with the reporting requirements, including requirements for classifying control weaknesses, as discussed in FAM 580? | FISCAM, 430.07 | | |
| 63. For examination-level attestation engagements, did the overall engagement auditor properly include in the examination report all internal control deficiencies that are considered significant deficiencies or material weaknesses that the auditor identified based on the engagement work performed? | FISCAM, 430.08<br>GAGAS (2018), 7.42 | | |
| 64. For performance audits, did the overall engagement auditor properly include in the | FISCAM, 430.09 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| audit report any deficiencies in internal control that are significant to the engagement objectives and based upon the audit work performed? | GAGAS (2018), 9.29, 9.30 | | |
| 65. 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<br>• include those deficiencies in the report or<br>• communicate those deficiencies in writing to audited entity officials and refer to that written communication in the audit report? | FISCAM, 430.10<br>GAGAS (2018), 9.31 | | |
| 66. 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, 430.11<br>GAGAS (2018), 6.50, 7.48, 9.18 | | |
| 67. When presenting findings in the report, did the overall engagement auditor<br>• 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; | FISCAM, 430.13<br>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 |
|---|---|---|---|
| • 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<br>• if the results cannot be projected, limit conclusions appropriately? | | | |
| 68. For performance audits, did the overall engagement auditor 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 engagement objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions? | FISCAM, 430.13<br>GAGAS (2018), 9.20 | | |
| 69. Did the overall engagement auditor<br>• disclose significant facts relevant to the objectives of the work and known to the team that if not disclosed could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices; | FISCAM, 430.14, 430.15, 430.16<br>GAGAS (2018), 9.19, 9.22, 9.23 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| • report conclusions based on the engagement objectives and findings;<br>• provide recommendations for corrective action for any sufficiently developed findings that are significant to the engagement objectives;<br>• 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<br>• 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? | | | |
| 70. For reports that contain, or may contain, information prohibited from public disclosure because of its confidential or sensitive nature, did the overall engagement auditor appropriately<br>• request that the source agency perform a classification, security, or sensitivity review of the draft report; | FISCAM, 430.17, 430.18, 430.19, 430.20<br>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 |
|---|---|---|---|
| • evaluate entity concerns and make appropriate report revisions or redactions, considering legal or regulatory requirements;<br>• 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;<br>• 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<br>• 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? | | | |
| 71. Did the auditor prepare reporting phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand | FISCAM, 440.01<br>GAGAS (2018), 7.34, 8.132 | | |

| Question | Paragraph reference(s) and related GAGAS requirement | Response (yes, no, or N/A) | Explanation and audit documentation reference |
|---|---|---|---|
| the conclusions reached, including evidence that supports the auditor's conclusions? | | | |
| 72. 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 | | |
| 73. Did the auditor adequately complete the reporting phase portion of this assessment completion checklist? | FISCAM, 440.03 | | |

# Appendix 600C FISCAM Security Management Questionnaire

## Purpose

The *Federal Information System Controls Audit Manual* (FISCAM) security management questionnaire includes questions relevant to the information system (IS) controls included in the FISCAM Framework for Security Management. The FISCAM security management questionnaire is intended to assist auditors with obtaining and documenting a preliminary understanding of the entity's information security management program sufficient to (1) assess the design and implementation of the control environment, entity risk assessment, and monitoring components of internal control relevant to the IS controls assessment and (2) assess IS control risk on a preliminary basis. See the FISCAM methodology (section 240) for additional guidance. The questionnaire does not include all procedures necessary to evaluate the design, implementation, and operating effectiveness of IS controls to achieve the engagement objectives overall.

## Instructions

The FISCAM security management questionnaire contains detailed questions that are organized by critical element. A response to each question is noted by either "yes," "no," or "n/a" (not applicable) in the "Response" column. An n/a response indicates that the question is not relevant to the engagement objectives and does not require further explanation. For each yes response, provide a reference to supporting documentation where the auditor's understanding is documented. For each no response, provide a response to whether any compensating controls have been identified in the "If no, have compensating controls been identified?" column. If compensating controls have been identified, provide a description of such controls in the "Comment" column. If compensating controls are not identified, provide an explanation of the potential effect on areas of audit interest in the "Comment" column.

## Preparation and Review

| | | | |
|---|---|---|---|
| Prepared by: | _____ | Date: | _____ |
| Reviewed by: | _____ | Date: | _____ |

## Questionnaire

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| Information security management program structure (SM.01.01) | | | | |
| 1. Does the organizational structure supporting the entity's information security management program have adequate independence, authority, expertise, and resources to achieve the entity's information security objectives? | | | | |
| 2. Does the organizational structure supporting the entity's privacy management program have adequate independence, authority, expertise, and resources to achieve the entity's privacy objectives? | | | | |
| 3. Does the organizational structure supporting the entity's supply chain risk management activities have adequate independence, authority, expertise, and resources? | | | | |
| Assignment of responsibilities for senior management (SM.01.02) | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 4. Has an information security officer been appointed and given the appropriate authority and resources to coordinate, develop, implement, and maintain the entity's information security management program? | | | | |
| 5. Has a senior management official been assigned as the authorizing official for each relevant information system and for the common controls that such systems inherit? | | | | |
| 6. Have information security responsibilities been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators, who possess the appropriate skills and technical expertise to satisfy their assigned responsibilities? | | | | |
| 7. Has a privacy officer been appointed and given the authority and resources to coordinate, develop, implement, and maintain the entity's privacy management program? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 8. Have privacy responsibilities been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators, who possess the appropriate skills and technical expertise to satisfy their assigned responsibilities? | | | | |
| 9. Has a chief risk officer been appointed and given the appropriate authority and resources to align information security and privacy management processes with strategic, operational, budgetary planning, and risk management processes? | | | | |
| Information security management planning documentation (SM.01.03) | | | | |
| 10. Has an entity-level information security management program plan been effectively designed and appropriately documented and periodically reviewed and updated? When determining if the plan has been effectively designed, consider if the plan includes<br>• approval by a senior official with responsibility and accountability for the risk being incurred;<br>• requirements of the entity's information security management | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| program, including the coordination among organizational entities responsible for information security;<br>• descriptions of the program management controls and common controls for meeting requirements; and<br>• assignment of roles and responsibilities for the information security management program. | | | | |
| 11. Has an entity-level information privacy management program plan been effectively designed and appropriately documented and periodically reviewed and updated? When determining if the plan has been effectively designed, consider if the plan includes<br>• approval by a senior official with responsibility and accountability for the risk being incurred;<br>• descriptions of the privacy management program strategic goals and objectives;<br>• descriptions of the requirements of a privacy management program, including the coordination among organizational entities responsible for information security; | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| • descriptions of the privacy controls for meeting those requirements; and<br>• assignment of roles and responsibilities for the privacy management program. | | | | |
| System development life cycle (SM.01.04) | | | | |
| 12. Have system development life cycle processes been appropriately documented, periodically reviewed and updated, and properly approved? | | | | |
| 13. Has an enterprise architecture that addresses security and privacy considerations been appropriately documented, periodically reviewed and updated, and properly approved? | | | | |
| Incident response program (SM.01.05) | | | | |
| 14. Has an entity-level incident response plan been effectively designed, appropriately documented, periodically reviewed and updated, and properly approved? When determining if the plan has been effectively designed, consider if the plan | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| • provides the entity with a road map for implementing its incident response capability;<br>• describes the structure and organization of the incident response capability;<br>• provides a high-level approach for how the incident response capability fits into the entity's organizational structure;<br>• meets the unique requirements of the entity, which relate to mission, size, structure, and functions;<br>• defines reportable incidents;<br>• provides metrics for measuring the incident response capability within the entity;<br>• defines the resources and management support needed to effectively maintain and mature an incident response capability;<br>• addresses the sharing of incident information;<br>• is reviewed and approved by management; and<br>• explicitly designates responsibility for incident response to appropriate personnel. | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 15. Has an incident response program been effectively designed and properly implemented in accordance with the entity-level incident response plan? When determining if the program has been effectively designed, consider if the program includes<br>• incident response training to system users consistent with their assigned roles and responsibilities;<br>• documented testing of the entity's incident response capabilities and follow-up on findings;<br>• appropriate incident-handling activities supported by automated mechanisms and incident response team members with the necessary knowledge, skills, and abilities;<br>• appropriate incident monitoring mechanisms to track and document incidents;<br>• a means for reporting incident information;<br>• appropriate incident response assistance;<br>• a process for gathering forensic evidence and conducting forensic analysis;<br>• links to other relevant security and privacy groups and associations; | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| • monitoring, generating, and disseminating security alerts, advisories, and directives, as applicable; and<br>• protection against denial-of-service attacks. | | | | |
| System-level and Entity-level processes (SM.01.06) | | | | |
| 16. Has the entity-level inventory of major information systems (i.e., all major applications and general support systems) been appropriately documented, periodically reviewed and updated, and properly approved? | | | | |
| 17. Is the entity-level process for selecting and implementing security controls effectively designed and implemented? When determining if the process has been effectively designed, consider if minimum security requirements for information and information systems are satisfied. | | | | |
| 18. Has the system-level concept of operations document for each relevant information system been appropriately documented, periodically reviewed and updated, and properly approved? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 19. Has the system-level security and privacy architecture for each relevant information system been appropriately documented, periodically reviewed and updated, and properly approved? | | | | |
| 20. Have the system security and privacy plans for each relevant information system included in the systems inventory been effectively designed, appropriately documented, periodically reviewed and updated, and properly approved? | | | | |
| 21. Has the system-level supply chain risk management plan for each relevant information system been effectively designed, appropriately documented, and periodically reviewed and updated? | | | | |
| Information security and privacy workforce and roles (SM.02.01) | | | | |
| 22. Has a security and privacy workforce development and improvement program been established and documented? | | | | |
| 23. Are information security and privacy roles, responsibilities, and position risk designation accurately identified and included in position descriptions? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 24. Are incompatible duties accurately identified and included in position descriptions? | | | | |
| Screening activities (SM.02.02) | | | | |
| 25. Are references for prospective employees properly contacted and background investigations and agency checks properly performed based on position risk designations? | | | | |
| 26. Are rescreening activities, including periodic reinvestigations, performed based on position risk designations as required by relevant provisions in statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria? | | | | |
| 27. Does the entity obtain signed access agreements prior to granting access to information and information systems? | | | | |
| Information security and privacy training and awareness program (SM.02.03) | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 28. Has an information security and privacy literacy training and awareness program been effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses? | | | | |
| 29. Has a role-based information security and privacy training program been effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses? | | | | |
| 30. Have current rules that describe the responsibilities and expected behavior for information and information system usage, security, and privacy been acknowledged in writing by individuals prior to their being granted access to information and information systems? | | | | |
| Training activities (SM.02.04) | | | | |
| 31. Have employee training records been appropriately documented, monitored, and retained? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 32. Have the results of employee training been evaluated by appropriate personnel, and have appropriate actions been taken? | | | | |
| Transfer and termination activities (SM.02.05) | | | | |
| 33. Have transfer and termination activities been appropriately completed on a timely basis? Consider the following transfer and termination activities:<br>• Review ongoing need for logical and physical access authorizations.<br>• Modify, disable, or remove accounts when associated access privileges or accounts are no longer needed.<br>• Collect property, equipment, and physical access authorization credentials.<br>• Conduct exit interviews.<br>• Escort terminated employees out of the entity's facilities.<br>• Identify the period during which nondisclosure requirements remain in effect for terminated employees. | | | | |
| Noncompliance with security and privacy policies and procedures (SM.03.01) | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 34. Have the entity's formal sanctions process and methods for individuals failing to comply with information security and privacy policies and procedures been appropriately employed? | | | | |
| External-party accountability (SM.03.02) | | | | |
| 35. Have the terms and conditions for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems been appropriately documented, periodically reviewed and updated, and properly approved? | | | | |
| 36. Has the entity-level process for assessing the effectiveness of information security and privacy controls that external parties design, implement, or operate effectively been designed and implemented to achieve the entity's information security and privacy objectives and hold external parties accountable for their assigned internal control responsibilities? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 37. Has the interorganizational joint authorization process for systems with multiple authorizing officials and at least one authorizing official from an external party been effectively designed and implemented to achieve the entity's information security and privacy objectives and hold external parties accountable for their assigned internal control responsibilities? | | | | |
| Complementary user-entity controls (SM.03.03) | | | | |
| 38. Have complementary user-entity controls related to external parties been identified and implemented and are they operating effectively? | | | | |
| Risk management strategies (SM.04.01) | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 39. Has the entity-level risk management strategy for information security and privacy risks been effectively designed, appropriately documented, and periodically reviewed and updated? When determining if the process has been effectively designed, consider if the strategy includes determination of assumptions and constraints affecting entity risk assessments, organizational risk tolerance, and entity-level priorities to guide and inform risk-based decisions. | | | | |
| 40. Has the entity-level continuous monitoring strategy been effectively designed, appropriately documented, and periodically reviewed and updated? When determining if the process has been effectively designed, consider if the 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. | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 41. Has the entity-level supply chain risk management strategy been effectively designed, appropriately documented, and periodically reviewed and updated? When determining if the process has been effectively designed, consider if the strategy manages risks associated with developing, acquiring, maintaining, and disposing of systems, system components, and system services. | | | | |
| Risk identification, analysis, and response activities (SM.04.02) | | | | |
| 42. Does the security categorization for each relevant information system flow logically from the supporting rationale documented and approved within the respective system security and privacy plan? | | | | |
| 43. Have risk assessments for relevant information systems been conducted and documented in accordance with effectively designed and implemented processes and methods for conducting and documenting such assessments? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 44. Have vulnerability scan reports and results from vulnerability monitoring, including results of penetration testing, been appropriately considered as part of the risk assessments conducted and documented for relevant information systems? | | | | |
| 45. Have risk assessment results for relevant information systems been documented, analyzed, and approved by management in accordance with effectively designed and implemented processes and methods for analyzing and responding to risks? | | | | |
| 46. Are risks reassessed periodically, at an appropriate frequency, to address changes to relevant information systems, the systems' environments of operation, or other conditions that may affect the security or privacy state of the systems? | | | | |
| 47. Have findings from risk assessments, security assessments, privacy assessments, monitoring activities, and audits been addressed within appropriate time frames in accordance with organizational risk tolerance? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| Information security and privacy policies and procedures (SM.05.01) | | | | |
| 48. Does management appropriately develop, document, periodically review and update, and properly approve information security and privacy policies and procedures implemented at the entity and system levels? | | | | |
| System authorization (SM.05.02) | | | | |
| 49. Have common controls been authorized for inheritance before commencing operations and reauthorized on a periodic basis thereafter? | | | | |
| 50. Has the authorizing official(s) appropriately (1) authorized each relevant information system to operate before commencing operations, (2) authorized the use of inherited common controls, and (3) reauthorized relevant information systems to operate and use inherited common controls periodically? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 51. Does the authorization package for each relevant information system include the authorization to operate, executive summary, system security and privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones? | | | | |
| Monitoring activities (SM.06.01) | | | | |
| 52. Has the system-level continuous monitoring strategy for each relevant information system been effectively designed, appropriately documented, and periodically reviewed and updated? | | | | |
| 53. Have system-level control monitoring activities been 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? | | | | |
| 54. Have assessors, with appropriate skills and technical expertise, properly performed security and privacy control assessments for each relevant information system on a periodic basis? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 55. Are control assessment reports shared with appropriate personnel and documented 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? | | | | |
| 56. Are performance measures and compliance metrics periodically evaluated and appropriately employed to measure the effectiveness or efficiency of information security and privacy functions? | | | | |
| Remediation of control deficiencies and vulnerabilities (SM.07.01) | | | | |
| 57. Are plans of action and milestones for relevant information systems appropriately documented and periodically reviewed and updated? | | | | |
| 58. Are control deficiencies and vulnerabilities adequately analyzed in relation to the entire entity and are appropriate corrective actions applied entity-wide? | | | | |

| Question | Response (yes, no, or N/A) | If no, have compensating controls been identified? (yes, no, or N/A) | Reference to supporting documentation | Comment |
|---|---|---|---|---|
| 59. Are remediation tasks and milestones accomplished by scheduled completion dates? | | | | |