100 Introduction

110 Overview of FISCAM

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

Purpose and Applicability

1. 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.
2. 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.[[1]](#footnote-1)

* 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.

1. 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 GAO and Council of the Inspectors General on Integrity and Efficiency’s (CIGIE) *Financial Audit Manual* (FAM) for federal financial statement audits.[[2]](#footnote-2) 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 engagement type. Additionally, FISCAM may be used to assess IS controls over compliance requirements and financial reporting in connection with a single audit.[[3]](#footnote-3)
2. 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.[[4]](#footnote-4)
3. 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.[[5]](#footnote-5) 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

1. 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 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 is 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

Diagram

Description automatically generated

FISCAM Methodology

1. 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.
2. 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.
3. 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.
4. The auditor continues to scope the IS controls assessment by performing a risk assessment. IS control risk, as defined by FISCAM, is the likelihood that conditions or events, related to the areas of audit interest, that could significantly affect the entity’s ability to achieve its information processing objectives, will not be prevented, or detected and corrected, on a timely basis by the entity’s IS controls. The auditor identifies inherent and IS risk factors (section 260) based on an understanding of the entity’s operations (section 230), the entity’s information security management program (section 240), and the significant business processes—including information resources and business process controls (section 250).
5. 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 110.21 for discussion of the FISCAM Framework.
6. 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.
7. 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 audit plan for each area of audit interest.
8. 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).
9. 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

Diagram

Description automatically generated

FISCAM Framework

1. 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

Diagram

Description automatically generated

1. 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.
2. The FISCAM Framework’s control categories are consistent with those included in generally accepted government auditing standards (GAGAS).[[6]](#footnote-6) 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 Governmen*t (Green Book).[[7]](#footnote-7) 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 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*,[[8]](#footnote-8) including the patch release.[[9]](#footnote-9)
3. 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.
4. 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 audit 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

1. 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

1. 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.

120 Fundamental IS Control Concepts

1. 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

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

IS Control Types and Organizational Objectives

1. 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.[[10]](#footnote-10)
* 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. Such 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.

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

1. Indirect general controls, which apply to the information security management program and information systems, are intended to create a suitable environment to support the effective operation of user, application, and direct general controls within the business process. Indirect general controls are generally related to the following organizational 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.[[11]](#footnote-11) 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

1. 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 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.

1. 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

1. 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. 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.
2. 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 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 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 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. 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 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.

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.

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

Figure 4: Fundamental Information System Control Concepts

Graphical user interface

Description automatically generated

130 Applicable Auditing and Attestation Standards and Requirements

1. 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.[[12]](#footnote-12)
2. 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).
3. For federal financial audits, FISCAM is to be used in conjunction with the FAM.[[13]](#footnote-13) 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.
4. 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).[[14]](#footnote-14)
5. 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.

1. 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

1. Criteria identify the required or desired state or expectation with respect to the program or operation of internal controls. Suitable criteria are relevant, reliable, objective, and understandable and do not result in the omission of significant information, as applicable, to the engagement objectives. Criteria may include the statutes, regulations, executive orders, implementing 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

Timeline

Description automatically generated

1. 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

1. The Federal Managers’ Financial Integrity Act of 1982 (FMFIA)[[15]](#footnote-15) 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.[[16]](#footnote-16) 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.
2. 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

1. Under the Federal Information Security Modernization Act of 2014 (FISMA),[[17]](#footnote-17) the Office of Management and Budget (OMB), in coordination with the Department of Homeland Security (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.[[18]](#footnote-18) See paragraphs 140.12 and 140.13 for discussion of DHS. OMB uses circulars, bulletins, and memorandums to provide information and guidance, including in areas applicable to information security. OMB information and guidance are published at [https://www.whitehouse.gov/omb/ information-for-agencies/](https://www.whitehouse.gov/omb/%20information-for-agencies/). The following circulars provide guidance that establishes information security requirements for federal executive entities:

* OMB Circular No. A-123, *Management’s Responsibility for Enterprise Risk Management and Internal Control*, defines management’s responsibilities for enterprise risk management and internal control and requires agencies to integrate these functions.[[19]](#footnote-19)
* 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 resources, and supporting infrastructure and services.[[20]](#footnote-20) 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

1. 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.[[21]](#footnote-21) 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

1. 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.
2. 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.[[22]](#footnote-22) 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.[[23]](#footnote-23) 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.

1. FIPS publications do not apply to national security systems.[[24]](#footnote-24) The Committee on National Security Systems is responsible for providing system security guidance for national security systems.

Special Publications

1. 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.[[25]](#footnote-25) 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.[[26]](#footnote-26) 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*.[[27]](#footnote-27) NIST SP 800-53B contains security and privacy control baselines for federal information systems and organizations and provides guidance for tailoring control baselines and for developing overlays to support the security and privacy requirements of stakeholders and their organizations.
* NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, provides guidance for implementing security controls using security configuration checklists specific to IT products or categories of IT products for an operational environment.[[28]](#footnote-28) 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.[[29]](#footnote-29) 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.

1. 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.

DHS Directives and Defense Information Systems Agency Security Technical Implementation Guides

1. 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.[[30]](#footnote-30) 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 entities. These directives are published at <https://www.cisa.gov/news-events/directives>.
2. 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.[[31]](#footnote-31) 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.[[32]](#footnote-32) 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

1. 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.

1. Engagement objectives relate to the overall objectives of a federal financial audit, attestation engagement, or performance audit. [↑](#footnote-ref-1)
2. GAO and Council of the Inspectors General on Integrity and Efficiency, Financial Audit Manual, vol. 1, [GAO-24-107278](https://www.gao.gov/products/gao-24-107278) (Washington, D.C.: June 2024); Financial Audit Manual, vol. 2, [GAO-24-107279](https://www.gao.gov/products/gao-24-107279) (Washington, D.C.: June 2024); and Financial Audit Manual, vol. 3, [GAO-24-107280](https://www.gao.gov/products/gao-24-107280) (Washington, D.C.: July 2024). [↑](#footnote-ref-2)
3. “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. [↑](#footnote-ref-3)
4. GAO, *Cybersecurity Program Audit Guide*, [GAO-23-104705](https://www.gao.gov/products/gao-23-104705) (Washington, D.C.: September 2023). [↑](#footnote-ref-4)
5. In the context of FISCAM, nonfederal entities include state, local, territorial, and tribal governments; nonprofit organizations; and for-profit organizations. [↑](#footnote-ref-5)
6. GAO, Government Auditing Standards: 2018 Revision, [GAO-21-368G](https://www.gao.gov/products/gao-21-368g) (Washington, D.C.: July 2018, updated April 2021). Early implementation of this revision is permitted. [↑](#footnote-ref-6)
7. GAO, Standards for Internal Control in the Federal Government, [GAO-14-704G](https://www.gao.gov/products/GAO-14-704G) (Washington, D.C.: September 2014). [↑](#footnote-ref-7)
8. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, rev. 5 (Gaithersburg, Md.: September 2020). [↑](#footnote-ref-8)
9. 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>. [↑](#footnote-ref-9)
10. 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). [↑](#footnote-ref-10)
11. 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. [↑](#footnote-ref-11)
12. [GAO-21-368G](https://www.gao.gov/products/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. [↑](#footnote-ref-12)
13. [GAO-24-107278](https://www.gao.gov/products/gao-24-107278), [GAO-24-107279](https://www.gao.gov/products/gao-24-107279), and [GAO-24-107280](https://www.gao.gov/products/gao-24-107280). [↑](#footnote-ref-13)
14. ISACA, IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit, 4th ed. (Schaumburg, Ill.: 2020). [↑](#footnote-ref-14)
15. 31 U.S.C. § 3512(c), (d), commonly known as the Federal Managers’ Financial Integrity Act. [↑](#footnote-ref-15)
16. [GAO-14-704G](https://www.gao.gov/products/GAO-14-704G). [↑](#footnote-ref-16)
17. Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (codified at 44 U.S.C. §§ 3551–3558). This 2014 statute largely superseded the similar Federal Information Security Management Act of 2002, Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (Dec. 17, 2002). 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. [↑](#footnote-ref-17)
18. 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. [↑](#footnote-ref-18)
19. Office of Management and Budget, Management's Responsibility for Enterprise Risk Management and Internal Control, OMB Circular No. A-123 (Washington, D.C.: July 15, 2016). [↑](#footnote-ref-19)
20. Office of Management and Budget, Managing Information as a Strategic Resource, OMB Circular No. A-130 (Washington, D.C.: July 15, 2016). [↑](#footnote-ref-20)
21. OMB Circular No. A-130, *Managing Information as a Strategic Resource*, p. 18, app. I-4. [↑](#footnote-ref-21)
22. National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems, FIPS 199 (Gaithersburg, Md.: March 2004). [↑](#footnote-ref-22)
23. National Institute of Standards and Technology, Minimum Security Requirements for Federal Information and Information Systems, FIPS 200 (Gaithersburg, Md.: March 2006). [↑](#footnote-ref-23)
24. 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. [↑](#footnote-ref-24)
25. 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). [↑](#footnote-ref-25)
26. National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, SP 800-53, rev. 5 (Gaithersburg, Md.: September 2020). [↑](#footnote-ref-26)
27. National Institute of Standards and Technology, Control Baselines for Information Systems and Organizations, SP 800-53B (Gaithersburg, Md.: December 2020). [↑](#footnote-ref-27)
28. National Institute of Standards and Technology, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, SP 800-70, rev. 4 (Gaithersburg, Md.: December 2018). [↑](#footnote-ref-28)
29. National Institute of Standards and Technology, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, SP 800-137 (Gaithersburg, Md.: September 2011). [↑](#footnote-ref-29)
30. 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. [↑](#footnote-ref-30)
31. 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. [↑](#footnote-ref-31)
32. DOD Instruction 8500.01, “Cybersecurity” (rev. Oct. 7, 2019). [↑](#footnote-ref-32)