500 FISCAM Framework

510 Overview of the FISCAM Framework

1. 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).
2. 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).[[1]](#footnote-1) 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).[[2]](#footnote-2) See paragraph 110.19 for additional discussion on the consistency between the FISCAM Framework and the Green Book’s principles and attributes.
3. 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*.[[3]](#footnote-3) 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.[[4]](#footnote-4) 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.

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-24-107026

1. 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.
2. 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 audit 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.
3. 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

A picture containing text

Description automatically generated

520 FISCAM Framework for Business Process Controls

1. 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.
2. 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.

1. 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 National Institute of Standards and Technology (NIST) Special Publication (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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as source documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Observe appropriate personnel as they prepare data for input and inspect any source documentation or additional support prepared.  Observe any reviews of source documentation or additional support prepared.  Through inquiry and inspection, obtain an understanding of the entity’s processes and methods to maintain evidence of input activities for subsequent review or reference.  Inspect a selection of transactions and trace selected data from the information system back to sources from which the data originated. Consider whether any of the selected data have been manipulated from their original form.  Determine whether input data are derived from appropriate sources. | NIST SP 800-53, SI-10 |
| BP.01.01.02 Control totals are employed when practicable. | Obtain an understanding of the entity’s use of control totals within the significant business processes through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of control totals to help ensure the completeness of data as they move through the process.  Inspect a selection of transactions, or a selected batch of transactions, and assess the use of control totals in the processing of such transactions.  Determine whether control totals are appropriately employed when practicable.  Note: A control total is the sum of a numerical field contained in a set of records. Control totals are used to verify the completeness of a set of records as it is processed. Control totals are verified by comparing 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 |
| BP.01.01.03 Sequence checking is employed when practicable. | Obtain an understanding of the entity’s use of sequence checking within the significant business processes through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of sequence checking to help ensure the completeness of data as they move through the process.  Observe a user attempt to subvert the sequence-checking process within the information system. Note any error messages and whether the transaction is suspended or processed.  Inspect a selection of transactions and assess the use of sequence checking in the processing of such transactions.  Determine whether sequence checking is appropriately employed when practicable.  Note: Sequence checking is used to verify the completeness of a set of records. A numerical sequence code is used to uniquely identify records. The absence of a number within a range of sequentially numbered records indicates a missing record. | 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   * inquiry of appropriate personnel and * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and any user-defined processing of data.  Observe appropriate personnel as they perform user-defined processing of data. Observe any reviews of such processing.  Inspect program code to obtain an understanding of the automated processing being performed.  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.  Determine whether user-defined processing of data is appropriately controlled.  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. | NIST SP 800-53, SI-10 |
| BP.01.01.05 Data prepared for system input are independently reviewed and approved (1) prior to entry or upload or (2) as part of the application software workflow for data entry.  *Related control: BP.04.03.09* | Obtain an understanding of the entity’s processes and methods for preparing data for input through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as source documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Observe appropriate personnel as they independently review data prepared for system input. Consider whether such reviews are performed (1) prior to data entry or upload or (2) as part of the application software workflow for data entry. Through inquiry and inspection, obtain an understanding of the entity’s processes and methods to maintain evidence of review activities for subsequent review or reference.  Inspect a selection of transactions and verify that data prepared for system input were independently reviewed and approved in accordance with relevant policies and procedures. Consider whether such reviews appropriately verified the completeness, accuracy, and validity of the input data.  Determine whether data prepared for system input are independently reviewed and properly approved (1) prior to entry or upload or (2) as part of the application software workflow for data entry. | NIST SP 800-53, SI-10 |
| 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.  *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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of data 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.  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.  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.  Determine whether relevant information systems appropriately validate that input data match specified definitions for data format and content and will not accept data that do not satisfy these definitions.  Note: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the entity specifies that numerical values from 1 to 100 are the only acceptable inputs for a field in an application, inputs of “387,” “abc,” or “%K%” are invalid inputs and are not accepted as input to the system. | NIST SP 800-53, SI-10 |
| BP.01.02.02 The system validates that input data have not been entered, uploaded, or accepted in duplicate.  *Related control: BP.01.02.03* | Obtain an understanding of the entity’s use of data input controls within the significant business processes through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of data 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.  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.  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.  Determine whether relevant information systems appropriately validate that input data have not been entered, uploaded, or accepted in duplicate. | NIST SP 800-53, SI-10 |
| BP.01.02.03 The system generates error messages, posts log entries, or produces combinations thereof when input data are not accepted.  *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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process; the format and content of inputs and outputs involved; and the use of 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.  Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems.  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.  Determine whether relevant information systems appropriately generate error messages, post log entries, or produce combinations thereof when input data are not accepted. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-12  NIST SP 800-53, SI-11 |
| BP.01.02.04 Rejected input data are held in suspense and identified on error reports until the errors are researched and resolved. | Obtain an understanding of the entity’s processes and methods for holding rejected input data in suspense until errors are resolved through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as error or suspense reports.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Observe a user attempt to perform an action that would cause input data to be rejected and held in suspense. Consider whether the input data are appropriately held in suspense and identified on an error or suspense report for subsequent review.  Determine whether rejected input data are held in suspense and identified on error reports until the errors are researched and appropriately resolved. | NIST SP 800-53, AU-02  NIST SP 800-53, SI-11 |
| BP.01.03 Data input errors are researched and resolved on a timely basis. | | |
| 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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as error or suspense reports.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  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.  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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as documentation for error resolution.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Inspect a selection of error or suspense reports and consider whether data input errors and rejected input data are being resolved through the entry or upload of corrected input data.  Determine whether data input errors are appropriately resolved through the entry or upload of corrected input data. | NIST SP 800-53, SI-10 |
| BP.01.03.03 Manual overrides of 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.  *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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as documentation for error resolution.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Inspect a selection of error or suspense reports and consider whether manual overrides of data 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.  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.  Note: The use of manual overrides does not on its own indicate that controls are inadequate. However, the auditor needs to examine why manual overrides are being used and whether adequate controls are in place to minimize risks from such actions. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-06  NIST SP 800-53, SI-10 |
| 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.  *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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of data 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.  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.  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. | NIST SP 800-53, SI-10 |
| BP.02.01.02 The system logs data processing events to permit management oversight of business processes that the system performs.  *Related controls: BP.01.02.01, 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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of event logging to permit management oversight of business processes that the information system performs.  Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems.  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.  Determine whether relevant information systems appropriately log data processing events to permit management oversight of business processes that the information system performs. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-12 |
| BP.02.01.03 Management reviews system data processing logs on a timely basis.  *Related control: BP.02.01.02* | Obtain an understanding of the entity’s processes and methods for reviewing information system data processing logs through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as information system data processing logs.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and management’s use of information system data processing logs.  Inspect a selection of information system data processing logs and consider whether any unusual or unauthorized activity identified on the logs was properly investigated and resolved on a timely basis. Through inquiry and inspection, obtain an understanding of the entity’s processes and methods to maintain evidence of such activities for subsequent review or reference.  Determine whether management reviews information system data processing logs relevant to the significant business processes on a timely basis. | NIST SP 800-53, AU-06 |
| BP.02.01.04 The system performs reconciliations to identify potential data processing errors. | Obtain an understanding of the entity’s use of automated reconciliations within the significant business processes through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the use of automated reconciliations to facilitate error identification and resolution.  Determine whether relevant information systems perform appropriate reconciliations to identify potential data processing errors. | NIST SP 800-53, SI-10 |
| BP.02.01.05 The system generates an error message, posts a log entry when data processing errors occur, or both.  *Related controls: BP.01.02.03, BP.02.01.02, BP.04.06.05, BP.05.04.05, BP.06.05.03, AC.05.01.02, 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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as system design documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process; the format and content of inputs and outputs involved; as well as the use of error messages, event logging, or combinations thereof to facilitate error resolution.  Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to relevant information systems.  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.  Determine whether relevant information systems appropriately generate an error message, post a log entry, or produce combinations thereof when data processing errors occur. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-12  NIST SP 800-53, SI-11 |
| BP.02.01.06 Data affected by processing errors are held in suspense and identified on error reports until the errors are researched and resolved. | Obtain an understanding of the entity’s processes and methods for holding data affected by processing errors in suspense until errors are resolved through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as error or suspense reports.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing.  Inspect a selection of error or suspense reports and consider whether data processing errors are identified.  Determine whether data affected by processing errors are held in suspense and identified on error reports until the errors are researched and appropriately resolved. | NIST SP 800-53, AU-02  NIST SP 800-53, SI-11 |
| BP.02.02 Data processing errors are researched and resolved on a timely basis. | | |
| BP.02.02.01 Data processing errors are researched to identify and remediate the cause(s) of the errors. | Obtain an understanding of the entity’s processes and methods for researching and remediating data processing errors through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as error or suspense reports.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing.  Inspect a selection of error or suspense reports and consider whether data processing errors are being researched and resolved on a timely basis. Additionally, consider whether management properly identifies the cause(s) of the errors. Follow up on any unresolved items identified.  Determine whether data processing errors are appropriately researched to properly identify and remediate the cause(s) of the errors. | NIST SP 800-53, SI-10 |
| 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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as documentation for error resolution.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing.  Inspect a selection of error or suspense reports and consider whether data processing errors are being resolved on a timely basis through the correction of data, the correction of coding errors in computer programs, or a combination of such actions.  Determine whether data processing errors are appropriately resolved by correcting data, correcting coding errors in computer programs, or a combination thereof. | NIST SP 800-53, SI-10 |
| BP.02.02.03 Manual overrides of data processing errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.  *Related controls: BP.01.03.03 and BP.03.03.03* | Obtain an understanding of the entity’s processes and methods for performing manual overrides of data processing errors through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as documentation for error resolution.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Inspect a selection of error or suspense reports and consider whether manual overrides of data processing errors were performed to resolve any of the errors identified. If a log of manual overrides exists, inspect the log to validate that manual overrides are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.  Determine whether manual overrides of information system data processing errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.  Note: The use of manual overrides does not on its own indicate that controls are inadequate. However, the auditor needs to examine why manual overrides are being used and whether adequate controls are in place to minimize risks from such actions. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-06  NIST SP 800-53, SI-10 |
| 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.  *Related controls: BP.04.03.11 and BP.04.05.03* | Obtain an understanding of the entity’s processes and methods for preparing data for output through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such outputs involved in the significant business processes.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and management’s definitions for the format and content of output data as well as its distribution.  Observe appropriate personnel as they prepare data for output. Through inquiry and inspection, obtain an understanding of the entity’s processes and methods to verify that the format and content of output data are aligned with management’s definitions.  Determine whether the format and content of output data are aligned with management’s definitions.  Note: Output data may include data files and system-generated reports. | NIST SP 800-53, SI-12  NIST SP 800-53, SI-15 |
| BP.03.02 Output data errors are identified on a timely basis. | | |
| BP.03.02.01 Summarized output data included in reports are reviewed and reconciled to appropriate source data on a timely basis. | Obtain an understanding of the entity’s processes and methods to review and reconcile summarized output data included in reports to appropriate source data through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and management’s definitions for the format and content of output data as well as its distribution.  Inspect available documentation for a selection of reconciliations performed during the audit period. Consider whether such reconciliations were appropriate and performed in accordance with the entity’s policies and procedures for timely reviewing and reconciling summarized output data to appropriate source data.  Determine whether summarized output data included in reports are reviewed and reconciled to appropriate source data on timely basis. | NIST SP 800-53, SI-12  NIST SP 800-53, SI-15 |
| BP.03.03 Output data errors are researched and resolved on a timely basis. | | |
| BP.03.03.01 Output data errors are researched to identify and remediate the cause(s) of the errors. | Obtain an understanding of the entity’s processes and methods for researching and remediating output data errors through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as error or suspense reports.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing.  Inspect a selection of error or suspense reports and consider whether output data errors are being researched and resolved on a timely basis. Additionally, consider whether management properly identifies the cause(s) of the errors. Follow up on any unresolved items identified. Determine whether output data errors are researched to identify and remediate the cause(s) of the errors. | NIST SP 800-53, SI-12  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   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as documentation for error resolution.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and controls over data processing.  Inspect a selection of error or suspense reports and consider whether output data errors are being resolved through the correction of data, the correction of coding errors in computer programs, or a combination of such actions.  Determine whether output data errors are appropriately resolved by correcting data, correcting coding errors in computer programs, or a combination thereof. | NIST SP 800-53, SI-10 |
| BP.03.03.03 Manual overrides of output data errors are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.  *Related controls: BP.01.03.03 and BP.02.02.03* | Obtain an understanding of the entity’s processes and methods for performing manual overrides of output data errors through   * inquiry of appropriate personnel; * inspection of business process documentation, such as process narratives, flowcharts, standard operating procedures, desktop guides, and user manuals; and * inspection of other relevant documentation, such as documentation for error resolution.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the flow of information through each significant business process, the format and content of inputs and outputs involved, and the sources of relevant input data.  Inspect a selection of error or suspense reports and consider whether manual overrides of output data errors were performed to resolve any of the errors identified. If a log of manual overrides exists, inspect the log to validate that manual overrides are (1) used only in limited circumstances that are defined and documented, (2) restricted to authorized personnel, and (3) logged and monitored.  Determine whether manual overrides of information system output data errors are (1) used only in limited circumstances that are defined and documented; (2) restricted to authorized personnel; and (3) logged and monitored.  Note: The use of manual overrides does not on its own indicate that controls are inadequate. However, the auditor needs to examine why manual overrides are being used and whether adequate controls are in place to minimize risks from such actions. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-06  NIST SP 800-53, SI-10 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system security and privacy plans.   Identify the business process application owners for the relevant information systems. Consider whether they are senior management officials and possess appropriate skills and technical expertise to satisfy ownership responsibilities.  Determine whether business process application and information system ownership has been appropriately assigned.  Note: Business process application ownership means the overall responsibility and accountability for management of the business process application, including ensuring that the business process application is properly designed to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information. Thus, any changes to the design of the business process application, modifications to functionality of the business process application through changes to application software or changes to configurable controls within application software, or changes to corresponding access controls generally require the approval of the business process application owner or an authorized delegate of the owner. Depending 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. | NIST SP 800-53, PL-02  NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| BP.04.01.02 Business process application responsibilities are appropriately assigned to information resource owners, users, and security administrators, as well as appropriate authorizing officials.  *Related controls: 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* | Obtain an understanding of the business process application responsibilities for information resource owners, users, and security administrators, as well as appropriate authorizing officials, through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system security and privacy plans.   Identify the information resource owners, users, and security administrators, as well as appropriate authorizing officials, for the relevant information systems. Consider whether they possess appropriate skills and technical expertise to satisfy their assigned responsibilities.  Determine whether business process application responsibilities have been clearly defined and appropriately assigned to information resource owners, users, and security administrators, as well as appropriate authorizing officials.  Note: Senior management officials are assigned as authorizing officials for information systems and common controls that organizational systems may inherit. Business process applications may be separately authorized or included within a larger information system boundary. An information system boundary comprises all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems 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, AC-22  NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  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 applications are developed, documented, approved, and periodically reviewed and updated. Such policies and procedures appropriately   * consider risk; * 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; * address changes to business process application functionality through modifications to application software or changes to configurable controls within application software; * address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external parties, and compliance; * identify and describe the relevant processes; * consider general and application controls; * consider segregation of duties controls; and * help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures for administering and using business process applications through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   Through inquiry, inspection, and observation, identify information system (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   * policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external parties, and compliance; * procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be held accountable for their actions, and appropriately consider general and application controls, as well as segregation of duties controls; and * policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity’s internal control objectives.   Throughout the engagement, determine whether the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures are designed, implemented, and operating effectively.  Note: Audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its system-level and business process-level policies and procedures are intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of 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. | NIST SP 800-53, AC-01  NIST SP 800-53, AT-01  NIST SP 800-53, AU-01  NIST SP 800-53, CA-01  NIST SP 800-53, CM-01  NIST SP 800-53, CP-01  NIST SP 800-53, IA-01  NIST SP 800-53, IR-01  NIST SP 800-53, MA-01  NIST SP 800-53, MP-01  NIST SP 800-53, PE-01  NIST SP 800-53, PL-01  NIST SP 800-53, PM-01  NIST SP 800-53, PS-01  NIST SP 800-53, PT-01  NIST SP 800-53, RA-01  NIST SP 800-53, SA-01  NIST SP 800-53, SC-01  NIST SP 800-53, SI-01  NIST SP 800-53, SR-01 |
| 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.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.  Determine whether business process application characteristics are appropriately defined, implemented, and documented to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information.  Note: Entities are required to define business processes with consideration for information security and determine the information protection requirements arising from the defined business processes. Business process applications supporting critical or essential mission and business functions may be designed as platform independent to support the ability to reconstitute on different platforms in the event of a system disruption.  Additionally, business process applications may be designed to use alternative sources of information to carry out essential functions or services when the primary source of information is corrupted or unavailable. Business process applications and information systems are designed to support specific mission or business functions. Business process application design documentation is maintained to support the entity’s authorization process as well as to facilitate configuration management.  Business process application characteristics include the application boundary, application modules and how they interact with one another, and data conventions. Business process application characteristics also include the automated business processes or subprocesses that the application performs, including any system accounts associated with the performance of such processes.  Application module interaction may be depicted in call graphs, data flow diagrams, and control flow diagrams. A data dictionary or data 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. | NIST SP 800-53, CM-12  NIST SP 800-53, PM-11  NIST SP 800-53, PM-32  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05  NIST SP 800-53, SA-08  NIST SP 800-53, SC-27  NIST SP 800-53, SI-22 |
| BP.04.03.02 Business processes are standardized and automated when practicable. | Perform walk-throughs of the significant business processes. Consider the extent to which such business processes are standardized and automated. Consider whether further standardization or automation would reduce control risk.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.  Determine whether the significant business processes are standardized and automated as practicable. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  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.  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.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that transactions are complete, accurate, and valid.  Note: When suitably designed and properly implemented, automated business processes and corresponding application controls provide reasonable assurance that only valid management-approved transactions are input into the application, accepted for processing, processed once and only once by the application, accurately recorded on a timely basis, and properly included in output files or reports. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| BP.04.03.04 Automated business processes and corresponding application controls are designed to help ensure that master and transaction data records maintained in data management systems are complete, accurate, and valid. | Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to help ensure that master and transaction data records maintained in the applicable data management systems are complete, accurate, and valid. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. When appropriate, inspect program code to assess the design of the automated business processes and corresponding application controls.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that master and transaction data records maintained in data management systems are complete, accurate, and valid.  Note: Automated business processes and corresponding application controls (e.g., duplicate checks and system warnings) are often configured into the business process application to prevent or identify potential duplicate master data records as well as to detect data anomalies. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| BP.04.03.05 Automated business processes and corresponding application controls are designed to help ensure that transaction data are in balance across business process application modules. | Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to help ensure that transaction data are in balance across business process application modules. Consider whether additional controls, including manual controls, are needed to mitigate inherent risk.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls. When appropriate, inspect program code to assess the design of the automated business processes and corresponding application controls.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that transaction data are in balance across business process application modules.  Note: For general ledger systems, automated business processes and corresponding application controls are designed to help ensure that data from subsidiary ledgers are in balance with the general ledger. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| 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.  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.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that master data are consistent between business process application modules and among other information systems using the same master data. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| BP.04.03.07 Access controls are incorporated into the design of automated business processes and corresponding application controls to prevent users from executing incompatible transactions within the business process application through menus, screens, or other user interfaces.  *Related controls: SD.01.01.01, SD.01.01.02, SD.01.02.01, SD.01.02.02, and SD.01.03.01* | Perform walk-throughs of the significant business processes. Consider whether access controls are incorporated into the design of automated business processes and corresponding application controls to prevent users from executing incompatible transactions.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.  Determine whether access controls are incorporated into the design of automated business processes and corresponding application controls to prevent users from executing incompatible transactions within the business process application through menus, screens, or other user interfaces. | NIST SP 800-53, AC-05  NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  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.  *Related control: BP.04.06.02*  *Related control objective: AC.02.03* | Perform walk-throughs of significant business processes. Consider whether transaction processing roles are appropriately aligned with management’s authorizations for users and processes acting on behalf of users.  Inspect system design documentation, system security and privacy plans, role permission matrices, and policies and procedures demonstrating the design of transaction processing roles and criteria for role membership.  Inspect a system-generated list of accounts for each of the business process applications and information systems relevant to the significant business processes. Consider the 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.  Determine whether transaction processing roles are aligned with management’s authorizations for users and processes acting on behalf of users. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-06 |
| BP.04.03.09 Approval workflows within the business process application are aligned with management’s authorizations for users and appropriately controlled.  *Related controls: BP.01.01.05 and BP.04.06.02* | Obtain an understanding of the entity’s processes and methods to control approval workflows. Consider whether such processes and methods adequately address access restrictions for workflow development or modification.  Inspect system design documentation, system security and privacy plans, role 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.  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.  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  NIST SP 800-53, AC-05  NIST SP 800-53, AC-06  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.  *Related controls: BP.01.02.01, BP.02.01.01, BP.04.05.01, BP.04.05.02, BP.04.05.03, and BP.06.03.04* | Inspect system design documentation, system security and privacy plans, applicable system configuration files, and policies and procedures demonstrating the defined parameters and tolerances for data input, processing, and output, as well as error conditions and messages. Consider whether parameters and tolerances for data input, processing, and output are appropriately defined, implemented, and documented. Consider whether the parameters and tolerances that management identified are appropriate.  Determine whether parameters and tolerances for data input, processing, and output, as well as error conditions and messages, are defined, implemented, and documented to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information.  Note: Data input, processing, and output parameters and tolerances can be configured based on limits on transaction amounts or based on the nature of transactions. Such parameters and tolerances are aligned with management’s definitions for data format and content. | NIST SP 800-53, SI-10  NIST SP 800-53, SI-11  NIST SP 800-53, SI-12  NIST SP 800-53, SI-15 |
| BP.04.03.11 Management defines the format and content of output data and their distribution based on end user needs and in accordance with applicable guidelines that the entity’s data governance body established to maintain and use data in accordance with applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.  *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 applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the format and content of output data and their distribution.  Determine whether the format and content of output data and their distribution are based on end user needs and in accordance with applicable guidelines that the entity’s data governance body established for maintaining and using data in accordance with applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria relevant to data governance.  Note: Management may have procedures in place to monitor the replication of output data within or outside the entity. | NIST SP 800-53, SI-12  NIST SP 800-53, SI-15 |
| BP.04.03.12 Management establishes, documents, and periodically reviews and updates user training that focuses on the correct use of the business process application. This includes the operation of information processing, information security, and privacy controls. Management monitors the completion status of applicable mandatory training courses for information system users.  *Related controls: SM.02.03.01, SM.02.03.02, and SM.02.03.03* | Obtain an understanding of the entity’s processes and methods for establishing, documenting, and periodically reviewing and updating training on the correct use of the business process applications and information systems relevant to the significant business processes through   * inquiry of appropriate personnel, including any senior officials responsible for the training, and * inspection of relevant documentation, such as training course materials.   Consider whether   * training course materials have been recently reviewed and updated, as appropriate; * mandatory training courses are identified and communicated to information system users as a condition for system access, as applicable; and * management adequately monitors the completion status of applicable mandatory training courses for information system users.   Determine whether management has established, documented, maintained, and monitored user training that focuses on the correct use of the business process application.  Note: System developers are required to provide training on the correct use and operation of information systems, including the operation of information processing, information security, and privacy controls. Developer-provided training applies to external and internal (in-house) developers. Training personnel contributes to ensuring the effectiveness of the controls implemented within business process applications and information systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Entities can also request training materials from developers to conduct in-house training or offer self-training to entity personnel. Entities determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms. | NIST SP 800-53, AT-03  NIST SP 800-53, AT-04  NIST SP 800-53, SA-16 |
| BP.04.04 Business process applications are designed to facilitate the protection of personally identifiable information. | | |
| BP.04.04.01 Business process application characteristics are defined, implemented, and documented with consideration for privacy. | Perform walk-throughs of the significant business processes. Consider whether the automated business processes and corresponding general and application controls observed in walk-throughs of the significant business processes are consistent with those documented in system documentation and align with prescribed personally identifiable information processing needs for the business process applications and information systems.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.  Determine whether business process application characteristics are defined, implemented, and documented with appropriate consideration for privacy.  Note: Entities are required to define business processes with consideration for privacy and determine the personally identifiable information processing needs arising from the defined business processes. The Privacy Act of 1974 (codified, as amended, at 5 U.S.C. § 552a) (PRIVACT) requires that each federal agency publish a system of records notice in the *Federal Register* when 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) guidance, the notice describes the existence and character of the system and identifies   * the system of records, the purpose of the system, * the authority for maintenance of the records, * the categories of records maintained in the system, * the categories of individuals about whom records are maintained, * the routine uses to which the records are subject, and * additional details about the system as described in OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.   Additionally, PRIVACT and implementing guidance establish requirements for federal and nonfederal agencies if they engage in a matching program. In general, a matching program is a computerized comparison of (1) two or more automated PRIVACT systems of records or (2) an automated PRIVACT system of records with automated nonfederal records that a nonfederal agency (or agent thereof) maintains. A PRIVACT matching program pertains either to federal benefit programs or to federal personnel or payroll records. A federal benefit match is performed to determine or verify eligibility for payments under federal benefit programs or to recoup payments or delinquent debts under federal benefit programs. A PRIVACT matching program involves not just the matching activity itself but also the investigative follow-up and ultimate action, if any. | NIST SP 800-53, PM-11  NIST SP 800-53, PT-06  NIST SP 800-53, PT-08 |
| BP.04.04.02 Automated business processes and corresponding application controls are designed to provide notice to information system users about the processing of personally identifiable information. When appropriate, the processes and controls also allow information system users to consent to the processing of their personally identifiable information. | Perform walk-throughs of the significant business processes. Consider the extent to which automated business processes and corresponding application controls are designed to provide notice to information system users about the processing of personally identifiable information and, when appropriate, allow information system users to consent to the processing of their personally identifiable information.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Confirm whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that notice is provided to information system users about the processing of personally identifiable information and, when appropriate, information system users to consent to the processing of their personally identifiable information.  Note: When suitably designed and properly implemented, automated business processes and corresponding application controls provide reasonable assurance that notice is provided to information system users about the processing of personally identifiable information and, when appropriate, information system users to consent to the processing of their personally identifiable information. | NIST SP 800-53, PT-04  NIST SP 800-53, PT-05 |
| BP.04.04.03 Automated business process and corresponding application controls are designed to apply processing conditions for specific categories of personally identifiable information 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 personally identifiable information based on risk.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of automated business processes and corresponding application controls.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Confirm whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that processing conditions for specific categories of personally identifiable information are based on risk.  Note: Entities apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, or guidelines. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any requirements that apply. | NIST SP 800-53, PT-07 |
| BP.04.04.04 Management develops, documents, and periodically reviews and updates a map of system data actions that process personally identifiable information. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating a map of system data actions that process personally identifiable information through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the map of system data actions for each of the business process applications and information systems. Consider whether the map of system data actions identifies   * discrete data actions, * elements of personally identifiable information being processed in the data actions, * system components involved in the data actions, and * the owners or operators of those system components.   Determine whether a map of system data actions has been appropriately documented, periodically reviewed and updated, and properly approved for each of the business process applications and information systems relevant to the significant business processes.  Note: Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. Understanding what personally identifiable information is being processed (e.g., the sensitivity of the personally identifiable information), how personally identifiable information is being processed (e.g., if the data action is visible to the individual or is processed in another part of the system), and by whom (e.g., individuals may have different privacy perceptions based on the entity that is processing the personally identifiable information) provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system.  Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the entity is using. Developing this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system. | NIST SP 800-53, CM-13 |
| 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 controls against specified definitions for input data format and content.  *Related control: BP.01.02.01* 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings, parameters, and tolerances for data input controls during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures. Inspect implemented configuration settings, parameters, and tolerances for data input controls to independently assess whether such are consistent with management’s specified definitions for input data.  Determine whether the entity’s processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for data input controls are designed, implemented, and operating effectively. | NIST SP 800-53, CA-02  NIST SP 800-53, CM-06 |
| BP.04.05.02 Management periodically reviews implemented configuration settings, parameters, and tolerances for data processing events and related logging against specified definitions for in-process data format and content.  *Related control: BP.02.01.01 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings, parameters, and tolerances for in-process data input controls during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures. Inspect implemented configuration settings, parameters, and tolerances for in-process data input controls to independently assess whether such are consistent with management’s specified definitions for in-process data.  Determine whether the entity’s processes and methods for periodically reviewing implemented configuration settings, parameters, and tolerances for in-process data input controls are designed, implemented, and operating effectively. | NIST SP 800-53, CA-02  NIST SP 800-53, CM-06 |
| BP.04.05.03 Management periodically reviews implemented configuration settings and parameters for output data against specified definitions for output.  *Related controls: BP.03.01.01, 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed implemented configuration settings and parameters for output data during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures. Inspect implemented configuration settings and parameters for output data to independently assess whether such are consistent with management’s specified definitions for output.  Determine whether the entity’s processes and methods for periodically reviewing implemented configuration settings and parameters for output data are designed, implemented, and operating effectively. | NIST SP 800-53, CA-02  NIST SP 800-53, CM-06 |
| BP.04.05.04 Management periodically determines whether business processes, as well as related logging, that the business process application performs are functioning as intended. It does so through a combination of observing and inspecting output data and manually reperforming automated business processes on a subset of authoritative source data, including approved input data. | Obtain an understanding of the entity’s processes and methods for periodically reviewing the adequacy of automated business processes and related logging through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed the adequacy of automated business processes and related logging during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures.  Determine whether the entity’s processes and methods for periodically reviewing the adequacy of automated business processes and related logging are designed, implemented, and operating effectively. | NIST SP 800-53, CA-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).  *Related control: BP.06.05.01*  *Related control objective: AC.02.03* | Inspect a system-generated list of accounts for each of the business process applications and information systems relevant to the significant business processes. Consider the 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.  Determine whether business process application roles and corresponding access privileges are appropriately authorized and assigned to users with a valid business purpose (least privilege).  Note: The access privileges authorized and assigned to user accounts are aligned with the transaction processing and approval responsibilities delegated to users and are consistent with management’s design of data input, processing, and output procedures. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-06 |
| BP.04.06.02 The execution of sensitive transactions and the approval of transactions initiated by other users are appropriately controlled.  *Related controls: BP.04.03.08, BP.04.03.09, and SD.01.01.01* | Perform walk-throughs of the significant business processes. Obtain an understanding of any sensitive transactions, as well as the processes and methods by which transactions are initiated, recorded, processed, and reported using the business process applications and information systems relevant to the significant business processes.  Observe the execution of sensitive transactions. Consider whether the users involved in this process are appropriately authorized to perform such actions.  Observe the approval of transactions and inspect any documentary evidence related to such approvals. Consider whether the users involved approving transactions that others initiated are appropriately authorized to perform such actions.  Determine whether the execution of sensitive transactions and the approval of transactions initiated by other users are appropriately controlled.  Note: 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  NIST SP 800-53, AC-05  NIST SP 800-53, AC-06 |
| BP.04.06.03 System accounts are identified for each automated business process or subprocess, and appropriate access privileges are authorized and assigned to such accounts.  *Related control objective: AC.02.03* | Through inquiry, inspection, and observation, identify the system accounts for each automated business process or subprocess involved in the significant business processes.  Inspect system design documentation, system security and privacy plans, role permission matrices, and policies and procedures demonstrating the design of transaction processing roles and criteria for role membership.  Inspect a system-generated list of accounts for each of the business process applications and information systems relevant to the significant business processes. Consider the 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.  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  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.  Obtain an understanding of the entity’s processes and methods to extract key output data and generate key reports relevant to the significant business processes. Consider whether such processes and methods adequately address access restrictions for such output data and reports. Consider whether the users involved in the processes are appropriately authorized to perform such actions.  Determine whether key output data, including key reports generated by the business process applications and information systems relevant to the significant business processes, are appropriately restricted to authorized users and other individuals for authorized purposes.  Note: User access to output data is aligned with the user’s role and the sensitivity of information. User access to reports is aligned with authorization, including the appropriate level of security clearance, where applicable. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-06  NIST SP 800-53, SI-12  NIST SP 800-53, SI-15 |
| BP.04.06.05 The business process application logs events associated with failed user attempts to perform unauthorized data input, processing, or output procedures.  *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.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the entity’s processes and methods for logging and monitoring events at the business process level.  Determine whether the business process applications relevant to the significant business processes properly log events associated with failed user attempts to perform unauthorized data input, processing, or output procedures.  Note: Logging and monitoring controls are implemented at the business process level to help ensure that incidents are identified, analyzed, and resolved in an appropriate and timely manner based on risk. Logical and physical access controls are designed to enforce management’s authorizations for users. Users’ attempts to bypass such controls are logged to facilitate the identification of security violations and incidents. Potential security violations are identified on a timely basis. Logging and other mechanisms may be established to notify management of potential security violations immediately as they occur. Additionally, appropriate personnel generate and review exception reports on a timely basis. Exceptions are properly analyzed, and appropriate actions are taken to respond to potential security violations based on the nature of exceptions. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-03  NIST SP 800-53, AU-12 |
| BP.04.07 Modifications to business process applications and changes to configurable controls within application software are appropriately controlled. | | |
| BP.04.07.01 Modifications to application software are authorized, tested, and approved.  *Related control: CM.02.01.02*  *Related control objectives: CM.02.01 and CM.02.02* | Obtain an understanding of the entity’s processes and methods to modify application software through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to modify application software. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that modifications to application software are appropriately authorized, tested, and approved.   Inspect available documentation for a selection of modifications to application software that occurred during the audit period. Consider whether adequate documentation exists to support such modifications, including evidence demonstrating that the modifications were appropriately authorized, tested, and approved by management. Consider whether the individuals involved in the modifications are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized modifications to application software.  Determine whether modifications to application software are authorized, tested, and approved. | NIST SP 800-53, SA-10 |
| BP.04.07.02 Changes to configurable controls within application software are appropriately controlled.  *Related control objectives: CM.02.01 and CM.02.02* | Perform walk-throughs of the significant business processes. Through inquiry, inspection, and observation, identify configurable controls within application software relevant to the significant business processes.  Obtain an understanding of the entity’s processes and methods to change configurable controls within application software through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to change configurable controls. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that changes to configurable controls within application software are appropriately controlled.   Inspect available documentation for a selection of changes to configurable controls within application software that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that the changes were properly verified and approved by management. Consider whether the individuals involved in the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to configurable controls within application software.  Determine whether changes to configurable controls within application software are appropriately controlled.  Note: Configurable controls are those controls that have been designed into the business process application or information system during system development. These controls address the features most 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. | NIST SP 800-53, CM-03 |
| BP.04.07.03 Management employs integrity verification processes or tools to detect unauthorized changes to application software.  *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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s integrity verification tools, and * inspection of relevant documentation, such as policies and procedures for using and managing the entity’s integrity verification tools, as well as implemented configuration settings, found in system configuration files for the tools employed.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed the output of the entity’s integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether such output was properly reviewed by appropriate personnel and whether appropriate action was taken on a timely basis to address any unauthorized changes detected.  Inspect the implemented configuration settings for the integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether the implemented configuration settings are appropriate for detecting unauthorized changes to application software.  Determine whether management properly employs integrity verification tools to detect unauthorized changes to application software.  Note: Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications. | NIST SP 800-53, CM-06  NIST SP 800-53, SI-07 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system security and privacy plans.   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.  Determine whether system interface ownership has been appropriately assigned.  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 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. | NIST SP 800-53, PL-02  NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.   See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether assigned individuals possess appropriate skills and technical expertise to satisfy their responsibilities.  Determine whether the responsibilities for system interface processing and correcting any errors have been clearly defined and assigned to appropriate personnel.  Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. 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  NIST SP 800-53, PM-23  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 reviewed and updated. Such policies and procedures appropriately   * consider risk; * 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; * address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external parties, and compliance; * identify and describe the relevant processes; * consider general and application controls; * consider segregation of duties controls; and * help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities. | 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   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   * 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; * 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 * policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purposes and support achieving the entity’s internal control objectives.   Throughout the engagement, determine whether the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures are designed, implemented, and operating effectively.  Note: Audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its system-level and business process-level policies and procedures are intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of 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. | NIST SP 800-53, AC-01  NIST SP 800-53, AT-01  NIST SP 800-53, AU-01  NIST SP 800-53, CA-01  NIST SP 800-53, CM-01  NIST SP 800-53, CP-01  NIST SP 800-53, IA-01  NIST SP 800-53, IR-01  NIST SP 800-53, MA-01  NIST SP 800-53, MP-01  NIST SP 800-53, PE-01  NIST SP 800-53, PL-01  NIST SP 800-53, PM-01  NIST SP 800-53, PS-01  NIST SP 800-53, PT-01  NIST SP 800-53, RA-01  NIST SP 800-53, SA-01  NIST SP 800-53, SC-01  NIST SP 800-53, SI-01  NIST SP 800-53, SR-01 |
| 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.  *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.  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.  Determine whether system interfaces are defined, implemented, and documented to reasonably assure the confidentiality, integrity, and availability of information.  Note: System interface design documentation is maintained to support the entity’s authorization process and to facilitate configuration 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. | NIST SP 800-53, CA-03  NIST SP 800-53, CA-09  NIST SP 800-53, CM-12  NIST SP 800-53, PM-11  NIST SP 800-53, SA-05  NIST SP 800-53, SA-08 |
| 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.  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.  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.  *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 design of each system interface includes appropriate encryption techniques based on relevant business requirements.  Inspect system design documentation, system security and privacy plans, and applicable exchange agreements, as well as policies and procedures demonstrating the design of system interfaces involved in the significant business processes.  Determine whether encryption techniques are employed to protect the confidentiality of interfaced data when appropriate. | NIST SP 800-53, SC-08 |
| 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.  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.  Through inquiry, inspection, and observation, identify the general controls applied at the entity, system, or business process levels that support the operating effectiveness of the automated business processes and corresponding application controls. Consider whether the associated general controls are effective.  Determine whether the automated business processes and corresponding application controls are suitably designed and properly implemented to reasonably assure that interfaced data are processed once and only once.  Note: When suitably designed and properly implemented, automated business processes and corresponding application controls provide reasonable assurance that interfaced data are processed once and only once. To help ensure this, system interface files may be automatically archived or deleted from the production environment after processing. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-05 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.   See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Observe the use of any mechanisms that the entity employs to notify users when files sent from a source system are received by the target system.  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.  Note: A positive acknowledgment scheme or “handshake” between the systems helps ensure that files are not skipped or lost. | NIST SP 800-53, SI-10  NIST SP 800-53, SI-11 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.   See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Observe the use of any mechanisms that the entity employs to notify users when a system interface fails or specific data are rejected.  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  NIST SP 800-53, SI-11 |
| BP.05.04.03 Appropriate personnel monitor the status of system interfaces processed through job scheduling software.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.   See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of system interfaces processed through job scheduling software.  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.  Determine whether appropriate personnel monitor the status of system interfaces processed through job scheduling software.  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. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-06 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to reconcile interfaced data from the source and target systems. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure the integrity of interfaced data.   Inspect available documentation for a selection of reconciliations performed during the audit period. Consider whether such reconciliations were appropriate and performed in accordance with the entity’s policies and procedures for reconciling interfaced data.  Determine whether reconciliations of interfaced data from the source and target systems are appropriately performed to verify the integrity of interfaced data.  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. | NIST SP 800-53, SI-10  NIST SP 800-53, SI-11 |
| BP.05.04.05 System interface processing events are logged to permit management oversight.  *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.   See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of 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.  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  NIST SP 800-53, AU-12 |
| BP.05.04.06 Management reviews system interface processing logs on a timely basis.  *Related control objectives: AC.05.02 and AC.05.03* | Obtain an understanding of the entity’s processes and methods to monitor the status of system interfaces involved in the significant business processes through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution and system security and privacy plans.   See BP.05.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Perform walk-throughs of the significant business processes. Obtain an understanding of the tools and techniques employed for monitoring the status of system interfaces.  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.  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 methods to identify and remediate the causes of system interface processing errors through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to identify and remediate the causes of system interface processing errors. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that system interface processing errors are adequately researched to timely identify and remediate their causes.   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.  Determine whether system interface processing errors are appropriately researched to identify and remediate their causes.  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. | NIST SP 800-53, SI-10  NIST SP 800-53, SI-12  NIST SP 800-53, SI-15 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to identify and remediate the causes of system interface processing errors. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that system interface processing errors are properly resolved.   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.  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. | | |
| BP.05.06.01 User-defined processing of data prior to system interface processing is appropriately controlled.  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.  Observe the performance of user-defined processing. Consider whether the users who perform this processing are appropriately authorized to perform such actions. Through a combination of inspection and reperformance, consider whether the results of user-defined processing are complete, accurate, and valid.  Observe any approvals of the results of user-defined processing and inspect any documentary evidence related to such approvals. Consider whether the users who approve such results are appropriately authorized to perform such actions and whether such users take adequate steps to assess the completeness, accuracy, and validity of the results.  Determine whether user-defined processing of data prior to system interface processing is appropriately controlled.  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  NIST SP 800-53, AC-05  NIST SP 800-53, AC-06 |
| BP.05.06.02 The execution of system interfaces is appropriately controlled.  *Related controls: BP.05.01.02 and BP.05.04.03* | Perform walk-throughs of the significant business processes. Obtain an understanding of the processes and methods by which system interfaces involved in the significant business processes are executed.  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.  Determine whether the execution of system interfaces is appropriately controlled. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-05  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.  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.  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  NIST SP 800-53, AC-06  NIST SP 800-53, SI-12  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.  Obtain an understanding of the entity’s processes and methods to automatically archive or delete key data files generated through system interface processing from the production environment after processing.  Determine whether key data files generated during system interface processing are automatically archived or deleted from the production environment after processing. | NIST SP 800-53, SI-12 |
| 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.  *Related control: BP.05.04.03*  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to modify the tools and techniques for system interface processing. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that modifications to the tools and techniques for system interface processing are appropriately controlled.   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 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.  Determine whether modifications to the tools and techniques for system interface processing, including any job-scheduling software employed, are appropriately controlled. | NIST SP 800-53, CM-03 |
| BP.05.07.02 Changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled.  *Related control objectives: CM.02.01 and CM.02.02* | For the 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for system interface processing and error resolution.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to change mapping tables. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled.   Inspect available documentation for a selection of changes to mapping tables for the system interfaces involved in 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 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.  Determine whether changes to mapping tables used to convert data from the source system for input to the target system are appropriately controlled.  Note: When mapping tables are used, it is important that controls are designed and implemented to reasonably assure that 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. | NIST SP 800-53, CM-03 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system security and privacy plans.   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.  Determine whether data ownership has been appropriately assigned.  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. | NIST SP 800-53, PL-02  NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| BP.06.01.02 Responsibilities for requesting, authorizing, and implementing changes to the schema or structure of the database are assigned to appropriate personnel.  *Related controls: 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether assigned individuals possess appropriate skills and technical expertise to satisfy their responsibilities.  Determine whether the responsibilities for requesting, authorizing, and implementing changes to the schema or structure of the database have been clearly defined and assigned to appropriate personnel.  Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. 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  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| BP.06.01.03 Responsibilities for requesting, authorizing, and implementing changes to transaction and master data through the database management software are assigned to appropriate personnel.  *Related controls: 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities.  Determine whether the responsibilities for requesting, authorizing, and implementing changes to transaction and master data have been clearly defined and assigned to appropriate personnel.  Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure. | NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| BP.06.01.04 Responsibilities for database table maintenance are assigned to appropriate personnel.  *Related controls: 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities.  Determine whether the responsibilities for database table maintenance have been clearly defined and assigned to appropriate personnel.  Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure. | NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for data management and system security and privacy plans.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities.  Determine whether the responsibilities for monitoring changes to the database have been clearly defined and assigned to appropriate personnel.  Note: As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure. | NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| BP.06.02 Policies and procedures for managing data management systems are developed and implemented. | | |
| BP.06.02.01 Policies and procedures applied at the system and business process levels for administering data management systems are developed, documented, approved, and periodically reviewed and updated. Such policies and procedures appropriately   * consider risk; * address changes to the schema or structure of the database, including any required approvals or authorizations; * address changes to transaction and master data made outside the business process application through the database management software; * address database table maintenance; * address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as with external parties, and compliance; * identify and describe the relevant processes; * consider general and application controls; * consider segregation of duties controls; and * help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures for administering data management systems through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   Through inquiry, inspection, and observation, identify 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   * 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; * 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 * policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity’s internal control objectives.   Throughout the engagement, determine whether the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level and business process-level policies and procedures are designed, implemented, and operating effectively.  Note: Audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its system-level and business process-level policies and procedures are intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of 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, AC-01  NIST SP 800-53, AT-01  NIST SP 800-53, AU-01  NIST SP 800-53, CA-01  NIST SP 800-53, CM-01  NIST SP 800-53, CP-01  NIST SP 800-53, IA-01  NIST SP 800-53, IR-01  NIST SP 800-53, MA-01  NIST SP 800-53, MP-01  NIST SP 800-53, PE-01  NIST SP 800-53, PL-01  NIST SP 800-53, PM-01  NIST SP 800-53, PS-01  NIST SP 800-53, PT-01  NIST SP 800-53, RA-01  NIST SP 800-53, SA-01  NIST SP 800-53, SC-01  NIST SP 800-53, SI-01  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 requirements for the business process applications and information systems. Consider whether the design of the schema or structure of the database includes appropriate specifications based on relevant business requirements.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of data management systems involved in the significant business processes.  Determine whether data management system characteristics, including the schema or structure of the database, are appropriately defined, implemented, and documented to reasonably assure the completeness, accuracy, and validity of transactions and data, as well as the confidentiality, integrity, and availability of information.  Note: Applications that handle significant volumes of data often employ data management systems to perform certain data-processing functions within an application. Data management systems use specialized software that may operate on specialized hardware. Many of the configurable controls, such as data 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, CM-12  NIST SP 800-53, PM-11  NIST SP 800-53, SA-05  NIST SP 800-53, SA-08  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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of data management systems involved in the significant business processes.  Determine whether master data requirements are appropriately established and properly implemented into the database design to help ensure that master data are complete, accurate, and valid. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-05  NIST SP 800-53, SI-10 |
| BP.06.03.03 Transaction data requirements are established and implemented into the database design to help ensure that transaction data are complete, accurate, and valid. | Obtain an understanding of any transaction data requirements established and implemented into the database design through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of data management systems involved in the significant business processes.  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  NIST SP 800-53, SA-05  NIST SP 800-53, SI-10 |
| BP.06.03.04 Null values or invalid values are not accepted in key fields.  *Related controls: BP.01.02.01, BP.02.01.01, and BP.04.03.10* | Perform walk-throughs of the significant business processes. Observe appropriate personnel as they input data into key fields, noting any data input errors that occur when null values or invalid values are entered.  Inspect system design documentation, system security and privacy plans, applicable system configuration files, and policies and procedures demonstrating the defined parameters for key fields.  Determine whether the management-identified parameters for key fields are appropriate to reasonably assure that null values or invalid values are not accepted. | NIST SP 800-53, PM-11  NIST SP 800-53, SA-05  NIST SP 800-53, SI-10 |
| BP.06.03.05 Access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data.  *Related controls: SD.01.01.01, SD.01.01.02, SD.01.02.02, and SD.01.03.01* | Perform walk-throughs of the significant business processes. Consider whether access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database.  Determine whether access controls are incorporated into the database design to prevent unauthorized users from accessing, updating, or deleting application data.  Note: Access controls in a data management system include consideration for the access paths to the database. The access paths are clearly documented and updated as changes are made. Generally, access to a database can be obtained in three ways: (1) directly through the database, (2) through access paths facilitated by the business process application, or (3) through the operating system(s) underlying the database.  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. | NIST SP 800-53, AC-05  NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| BP.06.03.06 The schema or structure of the database is aligned with management’s authorizations for users.  *Related control objective: AC.02.03* | Obtain an understanding of the database schema or structure through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Identify the access paths to data and the processes and methods for controlling data management system administrative functions.  Consider whether the database schema or structure is consistent with access control requirements such that the organization of data and database-hosted functions correspond to the access restrictions that need to be imposed on different groups of users.  Determine whether the schema or structure of the database is aligned with management’s authorizations for users.  Note: Data management systems have built-in privileged accounts that are often used for data management system administrative functions. Such accounts may be controlled through a combination of (1) strong passwords or other authentication mechanisms, (2) highly restrictive assignment of personnel to the accounts, (3) enforcement of unique identification and authentication for each administrator, and (4) effective logging and monitoring of privileged account usage. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-06 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the data management system, as well as implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced using access control software.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the processes and methods the relevant information systems perform to control logical access to sensitive application data. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems, business process applications, and data management systems; * employ encryption techniques when appropriate based on risk; * are suitably designed and properly implemented based on risk; and * reasonably assure that access to sensitive application data is restricted to authorized individuals for authorized purposes.   Determine whether sensitive application data are appropriately controlled and encrypted when appropriate.  Note: Entities may employ data-mining protection and detection techniques to protect sensitive application data from unauthorized data mining. | NIST SP 800-53, AC-23  NIST SP 800-53, SC-13  NIST SP 800-53, SC-28 |
| BP.06.03.08 Access controls are incorporated into the design of the data management system to help ensure that the physical and logical (in terms of connectivity) locations of the data storage and retrieval functions are appropriate. | Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database.  Determine whether access controls are incorporated into the design of the data management system to help ensure that the physical and logical (in terms of connectivity) locations of the data storage and retrieval functions are appropriate. | NIST SP 800-53, AC-05  NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| BP.06.03.09 Access controls are incorporated into the design of the data management system to help ensure that production data are separated from nonproduction systems (such as testing and development) and other production systems with lesser control requirements. | Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the database.  Determine whether access controls are incorporated into the design of the data management system to help ensure that production data are separated from nonproduction systems (such as testing and development) and other production systems with lesser control requirements. | NIST SP 800-53, AC-05  NIST SP 800-53, PM-11  NIST SP 800-53, SA-04  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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed master data records to verify that master data are complete, accurate, and valid. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures.  Determine whether the entity’s processes and methods for periodically reviewing master data records are designed, implemented, and operating effectively. | NIST SP 800-53, SI-10  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 among other information systems using the same master data. | Obtain an understanding of the entity’s processes and methods for periodically reviewing master data records through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.04.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed master data records to help ensure that master data are consistent between business process application modules and among other information systems using the same master data. Consider whether such actions were appropriate and were performed in accordance with the entity’s policies and procedures.  Determine whether the entity’s processes and methods for periodically reviewing master data records are designed, implemented, and operating effectively. | NIST SP 800-53, SI-10  NIST SP 800-53, SI-18 |
| BP.06.05 Access to data management systems is appropriately controlled. | | |
| BP.06.05.01 Data management system roles and corresponding access privileges are authorized and assigned to users with a valid business purpose (least privilege).  *Related control: BP.04.06.01*  *Related control objective: AC.02.03* | Inspect a system-generated list of accounts for each of the data management systems relevant to the significant business processes. Consider the 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.  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  NIST SP 800-53, AC-05  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 not integrated into the applications (such as ad hoc reporting) are consistent with access control requirements for the business process applications, data management systems, and other systems that may be affected. | Perform walk-throughs of the significant business processes. Consider whether access control requirements for specialized data management processes used to facilitate interoperability between business process applications and functions not integrated into the applications (such as ad hoc reporting) are consistent with access control requirements for the business process applications, data management systems, and other systems that may be affected.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the access control requirements for any specialized data management processes.  Determine whether access control requirements for specialized data management processes used to facilitate interoperability between business process applications and functions not integrated into the applications (such as ad hoc reporting) are consistent with access control requirements for the business process applications, data management systems, and other systems that may be affected. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-05  NIST SP 800-53, AC-06 |
| BP.06.05.03 The data management system logs events associated with changes to business process application data, including master data.  *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, 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.  Inspect system design documentation, system security and privacy plans, and policies and procedures demonstrating the design of the entity’s processes and methods for logging and monitoring events at the business process level.  Determine whether the data management systems relevant to the significant business processes properly log events associated with changes to business process application data, including master data. | NIST SP 800-53, AU-02  NIST SP 800-53, AU-03  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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to change the schema or structure of databases. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that changes to the schema or structure of the database are appropriately controlled.   Inspect available documentation for a selection of changes to the schema or structure of databases relevant to the significant business processes that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that management properly verified and approved changes. Consider whether the individuals involved in the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to the schema or structure of databases relevant to the significant business processes.  Determine whether changes to the schema or structure of the database are appropriately controlled. | NIST SP 800-53, CM-03 |
| BP.06.06.02 Changes to transaction and master data made through the database management software are appropriately controlled. | Obtain an understanding of the entity’s processes and methods to change transaction and master data through the database management software through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to change transaction and master data through the database management software. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk; * address the entity’s approach for de-identification, if applicable; and * reasonably assure that changes to transaction and master data made through the database management software are appropriately controlled.   Inspect available documentation for a selection of changes to transaction and master data relevant to the significant business processes that occurred during the audit period. Consider whether adequate documentation exists to support such changes, including evidence demonstrating that management properly verified and approved the changes. Consider whether the individuals involved in the changes are appropriately authorized to perform such actions. Consider whether effective access controls are employed to prevent or detect unauthorized changes to transaction and master data through the database management software.  Determine whether changes to transaction and master data made through the database management software are appropriately controlled.  Note: De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many 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 personally identifiable information from datasets when it is not (or no longer) necessary to satisfy the requirements envisioned for the data. | NIST SP 800-53, CM-03  NIST SP 800-53, SI-19 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Observe personnel as they perform procedures for monitoring changes to the schema or structure of the database, as well as changes to transaction and master data made through the database management software. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Consider whether the procedures observed are consistent with those the entity documented.  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  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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Observe personnel as they perform database table maintenance. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned responsibilities. Consider whether the procedures observed are consistent with those documented by the entity.  Determine whether management regularly performs database table maintenance. | NIST SP 800-53, SC-28 |
| BP.06.06.05 Management employs integrity verification tools to detect unauthorized changes to data management systems and data maintained in these systems.  *Related controls: 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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s integrity verification tools, and * inspection of relevant documentation, such as policies and procedures for using and managing the entity’s integrity verification tools, as well as implemented configuration settings found in system configuration files for the tools employed.   See BP.06.02.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed the output of the entity’s integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether such output was properly reviewed by appropriate personnel and whether appropriate action was taken on a timely basis to address any unauthorized changes detected.  Inspect the implemented configuration settings for the integrity verification tools employed in connection with the business process applications and information systems relevant to the significant business processes. Consider whether the implemented configuration settings are appropriate for detecting unauthorized changes to data management systems and data maintained in these systems.  Determine whether management properly employs integrity verification tools to detect unauthorized changes to data management systems and data maintained in these systems. | NIST SP 800-53, CM-06  NIST SP 800-53, SC-28  NIST SP 800-53, SI-07 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-24-107026

530 FISCAM Framework for Security Management

1. The 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.
2. 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 fraud risk, and significant changes related to the entity’s information security management program.
* SM.05 Management designs and implements policies and procedures to achieve the entity’s information security and privacy objectives and respond to risks.
* 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.

1. 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 National Institute of Standards and Technology (NIST) Special Publication (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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as applicable organizational charts, business or organizational unit descriptions, and staffing plans.   Determine whether the organizational structure supporting the entity’s information security management program has adequate independence, authority, expertise, and resources to achieve the entity’s information security objectives. | NIST SP-800-53, PL-09  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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as applicable organizational charts, business or organizational unit descriptions, and staffing plans.   Determine whether the organizational structure supporting the entity’s privacy management program has adequate independence, authority, expertise, and resources to achieve the entity’s privacy objectives. | NIST SP 800-53, PL-09  NIST SP 800-53, SA-02 |
| SM.01.01.03 A supply chain risk 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 supply chain risk management activities through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Determine whether the organizational structure supporting the entity’s supply chain risk management activities has adequate independence, authority, expertise, and resources. | NIST SP 800-53, PL-09  NIST SP 800-53, SA-02 |
| SM.01.02 Responsibilities are assigned to senior management positions within the information security and privacy functions. | | |
| SM.01.02.01 An information security officer is appointed and given the authority and resources to coordinate, develop, implement, and maintain the entity’s information security management program. | Obtain an understanding of the responsibilities of the information security officer through   * inquiry of appropriate personnel and * inspection of information security management program documentation.   Determine whether an information security officer has been appointed and given appropriate authority and resources. Consider whether the appointed information security officer possesses appropriate skills and technical expertise to satisfy the responsibilities of the position. | NIST SP 800-53, PM-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.  *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.  Obtain an understanding of the tasks senior management officials perform to satisfy their responsibilities as authorizing officials through   * inquiry of appropriate personnel, including the authorizing officials, and * inspection of information security management program documentation.   Determine whether senior management officials have been assigned as authorizing officials for the relevant information systems and the common controls that such systems inherit.  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. | NIST SP 800-53, CA-06  NIST SP 800-53, PM-10  NIST SP 800-53, SA-09 |
| SM.01.02.03 In coordination with the data governance body and data integrity board, information security responsibilities are defined and assigned to (1) senior management, (2) information resource owners and users, (3) IT management personnel, and (4) security administrators.  *Related controls: BP.04.01.01, BP.04.01.02, BP.05.01.01, BP.05.01.02, BP.06.01.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, SD.01.01.01, and SD.01.01.02* | Obtain an understanding of the information security responsibilities of senior management, information resource owners and users, IT management personnel, and security administrators through   * inquiry of appropriate personnel and * inspection of information security management program documentation.   Determine whether information security responsibilities have been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned information security responsibilities.  Note: To achieve the entity’s objectives, management assigns responsibility and delegates authority to key roles throughout the entity. To do so, management considers the overall responsibilities assigned to each business or organizational unit, determines what key roles are needed to fulfill the assigned responsibilities, and establishes the key roles. Management also determines what level of authority each key role needs to fulfill a responsibility. As part of delegating authority, management evaluates the delegation for proper segregation of duties within the business or organizational units and in the organizational structure overall. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure. | NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| SM.01.02.04 A privacy officer is appointed and given the authority and resources to coordinate, develop, implement, and maintain the entity's privacy management program. | Obtain an understanding the responsibilities of the privacy officer through   * inquiry of appropriate personnel and * inspection of privacy management program documentation.   Determine whether a privacy officer has been appointed and given appropriate authority and resources. Consider whether the appointed privacy officer possesses appropriate skills and technical expertise to satisfy the responsibilities of the position. | NIST SP 800-53, PM-19 |
| SM.01.02.05 In coordination with the data governance body and data integrity board, privacy responsibilities are defined and assigned to (1) senior management, (2) information resource owners and users, (3) IT management personnel, and (4) security administrators. | Obtain an understanding of the privacy responsibilities of senior management, information resource owners and users, IT management personnel, and security administrators through   * inquiry of appropriate personnel and * inspection of privacy management program documentation.   Determine whether privacy responsibilities have been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators. Consider whether such individuals possess appropriate skills and technical expertise to satisfy their assigned information security responsibilities. | NIST SP 800-53, PM-03  NIST SP 800-53, PM-23  NIST SP 800-53, PM-24 |
| SM.01.02.06 A chief risk officer is appointed and given the authority and resources to align information security and privacy management processes with strategic, operational, and budgetary planning processes and to reasonably assure consistent risk management practices across the organization. | Obtain an understanding of the responsibilities of the chief risk officer, or senior accountable official for risk management, through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Determine whether a chief risk officer has been appointed and given appropriate authority and resources. Consider whether the appointed risk management officer possesses appropriate skills and technical expertise to satisfy the responsibilities of the position. | NIST SP 800-53, PM-29 |
| SM.01.03 Planning documentation related to the entity’s information security management program is developed and maintained. | | |
| SM.01.03.01 Management develops, documents, and periodically reviews and updates an entity-level information security management program plan that is aligned with the entity-level strategic plan. This program plan includes   * approval by a senior official with responsibility and accountability for the risk being incurred; * requirements of the entity’s information security management program, including the coordination among organizational entities responsible for information security; * descriptions of the program management controls and common controls for meeting requirements; and * assignment of roles and responsibilities for the information security management program. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level information security management program plan through   * inquiry of appropriate personnel, including the senior official responsible for the plan, and * inspection of relevant documentation.   Inspect the entity-level information security management program plan. Consider whether the plan   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); * is aligned with the entity-level strategic plan; * includes required information in accordance with authoritative criteria; and * is adequate to guide the implementation of the entity’s information security management program and achieve the entity’s information security objectives.   Determine whether the entity-level information security management program plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the entity-level information security management program plan has been implemented. | NIST SP 800-53, PM-01  NIST SP 800-53, PM-02 |
| SM.01.03.02 Management develops, documents, and periodically reviews and updates an entity-level privacy management program plan. This program plan includes   * approval by a senior official with responsibility and accountability for the risk being incurred; * descriptions of the privacy management program strategic goals and objectives; * descriptions of the requirements of a privacy management program, including the coordination among organizational entities responsible for information security; * descriptions of the privacy controls for meeting those requirements; and * assignment of roles and responsibilities for the privacy management program. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level privacy management program plan through   * inquiry of appropriate personnel, including the senior official responsible for the plan, and * inspection of relevant documentation.   Inspect the entity-level privacy management program plan. Consider whether the plan   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); * includes required information in accordance with authoritative criteria; and * is adequate to guide the implementation of the entity’s privacy management program and achieve the entity’s privacy objectives.   Determine whether the entity-level privacy management program plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the entity-level privacy management program plan has been implemented. | NIST SP 800-53, PM-18  NIST SP 800-53, PM-19  NIST SP 800-53, PM-20  NIST SP 800-53, PM-21  NIST SP 800-53, PM-22  NIST SP 800-53, PM-25  NIST SP 800-53, PM-26  NIST SP 800-53, PM-27  NIST SP 800-53, PT-02  NIST SP 800-53, PT-03 |
| SM.01.04 System development life cycle processes that incorporate information security and privacy considerations are established. | | |
| SM.01.04.01 System development life cycle processes are developed, documented, and periodically reviewed and updated.  *Related controls: SD.01.02.05, CM.02.01.01, and CM.02.02.01* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating its system development life cycle processes through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the entity’s system development life cycle processes. Consider whether the processes   * identify roles and responsibilities; * are integrated with the entity’s risk management processes; * address the entity’s application of security and privacy engineering principles in the specification, design, development, implementation, and modification of information systems and information system components; * incorporate operations security controls; * require developers to design information systems, information system components, and information system services to align with the system-level security and privacy architectures and the enterprise architecture of the entity; * facilitate tracing of source code to design specifications and functional requirements during testing; * establish the standards, tools, and tool configurations used in source code development; * provide for validation, verification, and flaw remediation used in source code development; * facilitate replacing or providing alternative support for system components that the developer, vendor, or manufacturer no longer supports; * establish system documentation requirements; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are adequate to provide a foundation for the successful development, implementation, and operation of entity information systems.   Determine whether the system development life cycle processes have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, consider whether the system development life cycle processes have been implemented.  Note: Effective system development life cycle processes provide a foundation for the successful development, implementation, and operation of entity information systems. Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control 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. | NIST SP 800-53, SA-03  NIST SP 800-53, SA-08  NIST SP 800-53, SA-10  NIST SP 800-53, SA-11  NIST SP 800-53, SA-15  NIST SP 800-53, SA-17  NIST SP 800-53, SA-22  NIST SP 800-53, SC-04  NIST SP 800-53, SC-31  NIST SP 800-53, SC-36  NIST SP 800-53, SC-38  NIST SP 800-53, SI-23  NIST SP 800-53, SR-07 |
| SM.01.04.02 An enterprise architecture that addresses security and privacy considerations is developed, documented, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating an enterprise architecture that addresses security and privacy considerations through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the enterprise architecture of the entity. Consider whether the enterprise architecture   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); * is integrated with the entity’s risk management processes; and * adequately addresses security and privacy considerations for the entity.   Determine whether the enterprise architecture has been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the enterprise architecture has been implemented.  Note: The effective integration of security and privacy requirements into the enterprise architecture helps ensure that important security and privacy considerations are addressed throughout the system development life cycle and that those considerations are directly 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. | | |
| SM.01.05.01 The entity has developed and documented and periodically reviews and updates an entity-level incident response plan that   * provides the entity with a road map for implementing its incident response capability; * describes the structure and organization of the incident response capability; * provides a high-level approach for how the incident response capability fits into the entity’s organizational structure; * meets the unique requirements of the entity, which relate to mission, size, structure, and functions; * defines reportable incidents; * provides metrics for measuring the incident response capability within the entity; * defines the resources and management support needed to effectively maintain and mature an incident response capability; * addresses the sharing of incident information; * is reviewed and approved by management; and * explicitly designates responsibility for incident response to appropriate personnel.   *Related controls: SM.04.01.01, SM.04.01.02, and AC.05.01.02* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level incident response plan through   * inquiry of appropriate personnel, including the senior officials responsible for the plan, and * inspection of relevant documentation.   Inspect the entity-level incident response plan. Consider whether the plan   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); * includes required information in accordance with authoritative criteria; and * is adequate to guide the implementation of the entity’s incident response program and achieve the entity’s information security and privacy objectives.   Determine whether the entity-level incident response plan is effectively designed and has been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the entity-level incident response plan has been implemented. | NIST SP 800-53, IR-08  NIST SP 800-53, SR-08 |
| SM.01.05.02 An incident response program is implemented in accordance with the entity-level incident response plan. The program includes   * incident response training to system users consistent with their assigned roles and responsibilities; * documented testing of the entity’s incident response capabilities and follow-up on findings; * appropriate incident-handling activities supported by automated mechanisms and incident response team members with the necessary knowledge, skills, and abilities; * appropriate incident-monitoring mechanisms to track and document incidents; * a means for reporting incident information; * appropriate incident response assistance; * a process for gathering forensic evidence and conducting forensic analysis; * links to other relevant security and privacy groups and associations; * monitoring, generating, and disseminating security alerts, advisories, and directives, as applicable; and * protection against denial-of-service attacks.   *Related controls: SM.02.03.01, SM.02.03.02, and AC.05.02.04* | Obtain an understanding of the entity’s incident response program through   * inquiry of appropriate personnel, including the senior officials responsible for the plan, and * inspection of relevant documentation.   Inspect documentation for the entity’s incident response program. Consider whether   * incident response training is associated with the assigned roles and responsibilities of entity personnel to reasonably assure that the appropriate content and level of detail are included in such training; * the entity tests its incident response capabilities to determine their effectiveness and identifies potential weaknesses or deficiencies for follow-up; * incident-handling activities are consistent with the incident response plan and supported by automated mechanisms and incident response team members with the necessary knowledge, skills, and abilities to perform preparation, detection and analysis, containment, eradication, and recovery procedures; * incident-monitoring mechanisms maintain records about each incident, the status of the incident, and other pertinent information necessary for forensic analysis, as well as the evaluation of incident details, trends, and handling activities; * incidents are reported in accordance with applicable statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, and guidelines; * incident information is used to inform risk assessments or control assessments; * incident response support resources are adequate; * forensic evidence is gathered and forensic analysis is performed when appropriate; * there are links to other relevant security and privacy groups and associations; * security alerts, advisories, and directives are monitored, generated, and disseminated, as applicable; * techniques are employed to prevent adversarial attacks based on risks; and * denial-of-service attacks can be limited or eliminated.   Inspect the results of the entity’s incident response testing. Consider whether tests of the entity’s incident response capabilities were coordinated with business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, and other relevant plans, as applicable. Consider whether appropriate follow-up was performed for potential findings, weaknesses, or deficiencies related to the entity’s incident response capabilities.  Inspect available documentation for a selection of incident records for incidents that occurred during the audit period and verify whether the incidents were tracked and documented in accordance with the entity’s policies and procedures. Also, determine whether any associated forensic analysis or reporting was performed as appropriate. Consider whether adequate information was available for the entity to perform appropriate forensic analysis.  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. | NIST SP 800-53, IR-02  NIST SP 800-53, IR-03  NIST SP 800-53, IR-04  NIST SP 800-53, IR-05  NIST SP 800-53, IR-06  NIST SP 800-53, IR-07  NIST SP 800-53, PE-20  NIST SP 800-53, PM-15  NIST SP 800-53, SC-05  NIST SP 800-53, SC-06  NIST SP 800-53, SC-26  NIST SP 800-53, SC-30  NIST SP 800-53, SC-40  NIST SP 800-53, SC-42  NIST SP 800-53, SC-44  NIST SP 800-53, SC-48  NIST SP 800-53, SI-05  NIST SP 800-53, SR-08 |
| SM.01.06 System-level and entity-level processes for implementing and operating the entity’s information security management program are developed and maintained. | | |
| SM.01.06.01 An entity-level inventory of major information systems (i.e., all major applications and general support systems) is developed, documented, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level inventory of major information systems through   * inquiry of appropriate personnel and * inspection of relevant documentation, including management’s criteria for designating information systems as major information systems.   Inspect the entity-level inventory of major information systems. Consider whether   * the relevant information systems are appropriately included in the inventory, * management’s criteria for designating information systems as major information systems are suitable and consistently applied, and * the inventory has been recently reviewed and updated and is complete.   Determine whether the entity-level inventory of major information systems has been appropriately documented, periodically reviewed and updated, and properly approved. | NIST SP 800-53, PM-05 |
| 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.  *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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the control baseline for each relevant information system. Consider whether each control baseline has been selected and tailored based on   * the impact level of the corresponding system and * the entity-level process for selecting and implementing security controls.   Determine whether the entity-level process for selecting and implementing security controls is effectively designed and implemented to reasonably assure that minimum security requirements for information and information systems are satisfied.  Throughout the engagement, determine whether the security controls included in the control baselines for relevant information systems are designed, implemented, and operating effectively.  Note: Control baselines are predefined sets of controls that represent a starting point for protecting information and information systems. Subsequent tailoring of selected control baselines allows for management of risk in accordance with mission, business, or other constraints. Federal information system control baselines are provided in NIST SP 800-53B, which states that its security and privacy control baselines are based on the requirements in the Federal Information Security Modernization Act of 2014 (Public Law 113-283) (FISMA) and the Privacy Act of 1974 (codified, as amended, at 5 U.S.C. § 552a) (PRIVACT).  To prepare for selecting and tailoring the appropriate control baseline for an information system and its respective environment of operation, the entity first determines the criticality and sensitivity of the information the system is to process, store, or transmit. The process of determining information criticality and sensitivity is known as security 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.  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 security objectives are low. A moderate-impact system is a system in which at least one of the security objectives is moderate and no security objective is high. Finally, a high-impact system is a system in which at least one security objective is high. | NIST SP 800-53, PL-10  NIST SP 800-53, PL-11 |
| SM.01.06.03 System-level concept of operations (CONOPS) documents that describe the operation of the information system from the perspective of information security and privacy are developed, documented, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level CONOPS documents through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the system-level CONOPS documents for each relevant information system. Consider whether CONOPS documents   * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are adequate to describe the operation of the information systems from the perspective of information security and privacy.   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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the system-level security and privacy architectures for each relevant information system. Consider whether the security and privacy architectures   * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); * are consistent with the enterprise architecture; * are integrated with the risk management and system development life cycle processes; and * are adequate to describe the structure and behavior of the system’s security and privacy processes.   Determine whether the system-level security and privacy architectures for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the system-level security and privacy architectures for relevant information systems have been implemented.  Note: A security architecture is a set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected. The system-level security and privacy architectures describe the structure and behavior for a system’s security and privacy processes. | NIST SP 800-53, PL-08  NIST SP 800-53, PM-07 |
| SM.01.06.05 System security and privacy plans for each major information system included in the systems inventory are developed, documented, and periodically reviewed and updated.  *Related 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   * inquiry of appropriate personnel and * inspection of relevant documentation, including the entity-level inventory of major information systems.   Inspect the system security and privacy plans for each relevant information system. Consider whether the plans   * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); * include required information in accordance with authoritative criteria; and * are adequate to provide an overview of the security and privacy requirements for the system and describe the controls designed and implemented to satisfy such requirements.   Determine whether the system security and privacy plans for relevant information systems are effectively designed and have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the system security and privacy plans for relevant information systems have been implemented.  Note: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The 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.  System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle. Updates to system security and privacy plans are made to address changes to the system and environment of operation or deficiencies identified through control assessments. The auditor may use system security and privacy plans to obtain an understanding of an information system’s components, security categorization, impact level, operational environment, control dependencies, system interconnections, security and privacy requirements, and the individuals who fulfill system roles and responsibilities. | NIST SP 800-53, AC-14  NIST SP 800-53, PL-02 |
| SM.01.06.06 System-level supply chain risk management plans for information systems are developed, documented, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level supply chain risk management plans for information systems through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the system-level supply chain risk management plan for each relevant information system. Consider whether the plans   * have been recently reviewed and updated, as appropriate; * include required information in accordance with authoritative criteria; and * are adequate to identify, assess, and manage supply chain risks relevant to the system.   Determine whether the system-level supply chain risk management plans for relevant information systems are effectively designed, have been appropriately documented, and are periodically reviewed and updated.  Throughout the engagement, determine whether the system-level supply chain risk management plans for relevant information systems have been implemented.  Note: System-level supply chain risk management plans can be stand-alone plans or part of system security and privacy plans. | NIST SP 800-53, SR-02  NIST SP 800-53, SR-03 |
| 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.  *Related controls: SM.02.03.01 and SM.02.03.02* | Obtain an understanding of the entity’s security and privacy workforce development and improvement program through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Determine whether a security and privacy workforce development and improvement program has been established and documented. | NIST SP 800-53, PM-13 |
| SM.02.01.02 Information security and privacy roles and responsibilities, as well as position risk designation, are included in position descriptions. | Inspect a selection of position descriptions for senior management, information resource owners, IT management personnel, and security administrators.  Determine whether the information security and privacy roles and responsibilities, as well as position risk designation, are accurately identified and included in position descriptions.  Note: Position risk designations reflect the degree of potential damage that could occur from the misconduct of an incumbent of a position. Position risk designations inform the nature, timing, and extent of the entity’s screening activities. | NIST SP 800-53, PS-02  NIST SP 800-53, PS-09 |
| SM.02.01.03 Incompatible duties are included in position descriptions.  *Related controls: SD.01.01.01 and SD.01.01.02* | Inspect a selection of position descriptions for senior management, information resource owners, IT management personnel, and security administrators.  Determine whether incompatible duties are accurately identified and included in position descriptions. | NIST SP 800-53, AC-05 |
| SM.02.02 Screening activities are completed, and access agreements are signed prior to access authorization. | | |
| SM.02.02.01 References for prospective employees are contacted, and background investigations and agency checks are performed based on position risk designations. | Obtain an understanding of the entity’s processes and methods for contacting references for prospective employees and performing background investigations and agency checks through   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect relevant documentation for a selection of recently hired IT management personnel to verify that references have been contacted and background investigations and agency checks have been performed in accordance with the entity’s policies and procedures.  Determine whether references for prospective employees are contacted and background investigations and agency checks are properly performed based on position risk designations.  Note: Position risk designations inform the nature, 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  NIST SP 800-53, PS-03  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 applicable 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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect relevant documentation for a selection of IT management personnel to verify that rescreening activities, including periodic reinvestigations, have been performed in accordance with the entity’s policies and procedures.  Determine whether rescreening activities, including periodic reinvestigations, are performed based on position risk designations as required by applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria. | NIST SP 800-53, PS-02  NIST SP 800-53, PS-03  NIST SP 800-53, SA-21 |
| SM.02.02.03 Individuals sign access agreements prior to being granted access to information and information systems.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect available documentation for a selection of accounts that were created during the audit period.  Determine whether the entity obtains signed access agreements prior to granting access to information and information systems.  Note: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. | NIST SP 800-53, CM-10  NIST SP 800-53, CM-11  NIST SP 800-53, MP-07  NIST SP 800-53, PL-04  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 breaches and awareness techniques is established, documented, and periodically reviewed and updated. The completion status of applicable mandatory training courses for information system users is monitored.  *Related controls: BP.04.03.12, SM.01.05.02, SM.02.01.01, and SM.02.03.02* | Obtain an understanding of the entity’s processes and methods for establishing, documenting, and periodically reviewing and updating information security and privacy literacy training and awareness techniques through   * inquiry of appropriate personnel, including any senior officials responsible for the information security and privacy literacy training and awareness program, and * inspection of relevant documentation, such as literacy training course materials demonstrating the incorporation of lessons learned from internal or external security incidents or breaches.   Inspect documentation for the information security and privacy literacy training and awareness program. Consider whether   * training course materials are consistent with information system user roles and responsibilities and the content has been reviewed and updated when required because of system changes and at an appropriate frequency; * lessons learned from internal or external security incidents or breaches are incorporated into literacy training course materials and awareness techniques; * mandatory training courses are identified and communicated to information system users as a condition of system access, as applicable; and * management monitors and maintains records of the completion status of applicable mandatory training courses for information system users.   Determine whether the information security and privacy literacy training and awareness program is effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses.  Throughout the engagement, determine whether the information security and privacy literacy training and awareness program has been implemented. | NIST SP 800-53, AT-02  NIST SP 800-53, AT-04  NIST SP 800-53, PM-14 |
| SM.02.03.02 A role-based information security and privacy training program that incorporates lessons learned from internal or external security incidents or breaches is established, documented, and periodically reviewed and updated. The completion status of applicable mandatory training courses for information system users is monitored.  *Related controls: BP.04.03.12, SM.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   * inquiry of appropriate personnel, including any senior officials responsible for the role-based information security and privacy training program, and * inspection of relevant documentation, such as role-based training course materials demonstrating the incorporation of lessons learned from internal or external security incidents or breaches.   Inspect documentation for the role-based information security and privacy training program. Consider whether   * training course materials are consistent with information system user roles and responsibilities and the content has been reviewed and updated when required by system changes and at an appropriate frequency; * lessons learned from internal or external security incidents or breaches are incorporated into role-based training content; * mandatory training courses are identified and communicated to information system users as a condition of system or role-based access, as applicable; and * management monitors and maintains records of the completion status of applicable mandatory training courses for information system users.   Determine whether the role-based information security and privacy training program is effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses.  Throughout the engagement, determine whether the role-based information security and privacy training program has been implemented. | NIST SP 800-53, AT-03  NIST SP 800-53, AT-04  NIST SP 800-53, PM-14 |
| SM.02.03.03 Current rules that describe the responsibilities and expected behavior for information and information system usage, security, and privacy have been acknowledged in writing by individuals prior to their being granted access to information and information systems.  *Related controls: BP.04.03.12, 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   * inquiry of appropriate personnel, including information system users, and * inspection of relevant documentation, including access agreements.   Inspect available documentation for a selection of accounts that were created during the audit period.  Determine whether current rules that describe the responsibilities and expected behavior for information and information system usage, security, and privacy have been acknowledged in writing by individuals prior to their being granted access to information and information systems. | NIST SP 800-53, CM-10  NIST SP 800-53, CM-11  NIST SP 800-53, MP-07  NIST SP 800-53, PL-04  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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect relevant documentation for a selection of IT management personnel to verify that employee training records have been documented, monitored, and retained in accordance with the entity’s policies and procedures.  Determine whether employee training records are appropriately documented, monitored, and retained. | NIST SP 800-53, AT-04 |
| SM.02.04.02 Results of employee training are evaluated by appropriate personnel and appropriate actions are taken. | Obtain an understanding of the entity’s processes and methods for evaluating the results of employee training and taking appropriate action through   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect relevant documentation for a selection of training courses, such as information security and privacy literacy training or role-based information security and privacy training. Consider whether   * results of employee training, including employee feedback, are retained and evaluated by personnel with the authority to take or delegate appropriate actions, and * actions, such as updates to course materials or instruction methods, are taken in response to evaluations of training, as appropriate.   Determine whether the results of employee training are evaluated by appropriate personnel and appropriate actions are taken. | NIST SP 800-53, AT-06 |
| SM.02.05 Transfer and termination activities are completed on a timely basis. | | |
| SM.02.05.01 Where appropriate, the following transfer and termination activities are completed on a timely basis:   * review ongoing need for logical and physical access authorizations; * modify, disable, or remove accounts when associated access privileges or accounts are no longer needed; * collect property, equipment, and physical access authorization credentials; * conduct exit interviews; * escort terminated employees out of the entity’s facilities; and * identify the period during which nondisclosure requirements remain in effect for terminated employees.   *Related control: AC.02.03.04* | Obtain an understanding of the entity’s processes and methods for completing transfer and termination activities through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect relevant documentation for a selection of recently transferred or terminated IT management personnel to verify that appropriate transfer and termination activities were completed on a timely basis.  Consider whether   * logical and physical access authorizations for transferred personnel were reviewed to determine whether an ongoing need for such access exists; * accounts were timely modified, disabled, or removed when associated access privileges or accounts are no longer needed due to transfer or termination; * property, equipment, and physical access authorization credentials were timely collected; * exit interviews were conducted; * terminated employees were escorted out of the entity’s facilities; and * the period during which nondisclosure requirements remain in effect was identified for terminated employees.   Inspect a system-generated list of enabled user accounts and a list of terminated personnel to verify that user accounts for terminated personnel have been promptly disabled after the termination date. Consider the 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.  Determine whether appropriate transfer and termination activities are completed on a timely basis. | NIST SP 800-53, PS-04  NIST SP 800-53, PS-05 |
| 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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in to assessing the adequacy of policies and procedures.  Inspect relevant documentation for a selection of IT management personnel who have recently been subject to the entity’s formal sanctions process.  Determine whether the entity’s formal sanctions process and methods for individuals failing to comply with information security and privacy policies and procedures are appropriately employed. | NIST SP 800-53, PS-08 |
| 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.  *Related controls: BP.05.03.01, AC.01.01.01, and AC.05.02.05* | Obtain an understanding of the entity’s processes and methods for developing, documenting, periodically reviewing and updating, and approving the terms and conditions for protecting controlled unclassified information that is processed, stored, or transmitted on external systems through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, or other exchange agreements.   Inspect the interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, or other exchange agreements for the relevant information systems. Consider whether such documentation   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); and * is adequate to reasonably assure the protection of controlled unclassified information that is processed, stored, or transmitted on external systems.   Inspect the contracts executed between the entity and external parties for the acquisition of information systems, information system components, or information system services. Consider whether the contracts include, either explicitly or by reference to an exchange agreement, the following requirements, descriptions, and criteria:   * security and privacy functional requirements and related controls; * strength of mechanism requirements; * security and privacy assurance requirements; * security and privacy documentation requirements and related controls; * descriptions of the system development environment and the environment in which the system is intended to operate; * roles and responsibilities for information security, privacy, and supply chain risk management; and * acceptance criteria.   Determine whether the terms and conditions for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, determine whether the terms and conditions for the protection of controlled unclassified information have been implemented.  Note: Entities may incorporate provisions related to exchange agreements into formal contracts, especially for 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. | NIST SP 800-53, AC-20  NIST SP 800-53, AC-21  NIST SP 800-53, CA-03  NIST SP 800-53, PM-17  NIST SP 800-53, PS-07  NIST SP 800-53, SA-04  NIST SP 800-53, SA-09 |
| 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.  *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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, * inspection of relevant service organization reports, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Through inquiry, inspection, and observation, identify 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.  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   * is based on current information; * addresses any controls the entity designs, implements, or operates that are necessary to achieve the external parties’ control objectives; and * is adequate to support the entity’s conclusions on the effectiveness of information security and privacy controls that external parties design, implement, or operate.   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 objectives and hold external parties accountable for their assigned internal control responsibilities.  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.  See also section 330 for guidance on using service organization reports.  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.  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.  Monitoring activities related to service organizations may include the use of work performed by external parties, such as service auditors, and reviewed by management. Additionally, if controls that service organizations perform are necessary for the entity to achieve its objectives and address risks related to the assigned operational process, the entity’s internal controls may include complementary user-entity controls that the service organization or its auditors identified that are necessary to achieve the service organization’s control objectives. | NIST SP 800-53, CA-01  NIST SP 800-53, CA-06  NIST SP 800-53, PS-07  NIST SP 800-53, SA-09 |
| 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   * inquiry of appropriate personnel, such as authorizing officials and information system owners; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  See also SM.05.02.01, SM.05.02.02, and SM.05.02.03.  If applicable, determine whether the interorganizational joint authorization process for systems with multiple authorizing officials and at least one authorizing official from an external 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  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.  *Related control: SM.03.02.02* | Obtain an understanding of the entity’s processes and methods for identifying, implementing, and testing complementary user-entity controls through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation, such as service organization reports and internal control testing results.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether management identified all relevant complementary user-entity controls from the external 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.  Perform tests of effectiveness over relevant complementary user-entity controls, as appropriate.  Inspect the external party’s service organization report and consider whether relevant controls at the external party are appropriately designed, implemented, and operating effectively.  Determine whether the complementary user-entity controls related to external parties are identified, implemented, and operating effectively.  Note: Complementary user-entity controls are controls that management of the service organization assumes, in the design of its service, will be implemented by user entities and are necessary to achieve the control objectives stated in management’s description of the service organization’s system. | NIST 800-53, SA-09 |
| SM.04 Management identifies, analyzes, and responds to risks, including fraud risk, and significant changes related to the entity’s information security management program. | | |
| SM.04.01 Risk management strategies are developed, documented, and maintained. | | |
| SM.04.01.01 An entity-level risk management strategy for information security and privacy risks is developed, documented, and periodically reviewed and updated. To guide and inform risk-based decisions, the strategy includes determination of assumptions and constraints affecting entity risk assessments, organizational risk tolerance, and entity-level priorities.  *Related controls: SM.01.05.01, AC.04.01.01, CM.03.01.01, and CM.03.02.01* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level risk management strategy for information security and privacy risks through   * inquiry of appropriate personnel, including the senior officials responsible for the strategy, and * inspection of relevant documentation.   Inspect the entity-level risk management strategy for information security and privacy risks. Consider whether the strategy   * has been recently reviewed and updated, as appropriate; * includes required information in accordance with authoritative criteria; * demonstrates that the entity has determined assumptions and constraints affecting risk assessments, organizational risk tolerance, and priorities to guide and inform risk-based decisions; and * is adequate for prioritizing the entity’s implementation of activities to assess, respond to, and monitor information security and privacy risks, including physical and environmental hazards.   Determine whether the entity-level risk management strategy for information security and privacy risks is effectively designed, has been appropriately documented, and is periodically reviewed and updated.  Throughout the engagement, determine whether the entity-level risk management strategy has been implemented. | NIST SP 800-53, PE-23  NIST SP 800-53, PM-09  NIST SP 800-53, PM-10  NIST SP 800-53, PM-12  NIST SP 800-53, PM-16  NIST SP 800-53, PM-28 |
| SM.04.01.02 An entity-level continuous monitoring strategy that establishes the metrics, frequency, and type(s) of control assessments and monitoring, as well as the process for correlating, analyzing, and responding to control assessment and monitoring results, is developed, documented, and periodically reviewed and updated.  *Related controls: SM.01.05.01, SM.06.01.01, CM.03.01.01, and CM.03.02.01* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level continuous monitoring strategy through   * inquiry of appropriate personnel, including the senior officials responsible for the strategy, and * inspection of relevant documentation.   Inspect the entity-level continuous monitoring strategy. Consider whether the strategy   * has been recently reviewed and updated, as appropriate; * includes required information in accordance with authoritative criteria; * establishes the metrics, frequency, and type(s) of control assessments and the monitoring to be performed; * defines the process for correlating, analyzing, and responding to control assessment and monitoring results; and * is adequate for prioritizing the entity implementing activities that facilitate ongoing awareness of the security and privacy posture across the entity and for supporting entity risk management decisions.   Determine whether the entity-level continuous monitoring strategy is effectively designed, has been appropriately documented, and is periodically reviewed and updated.  Throughout the engagement, determine whether the entity-level continuous monitoring strategy has been implemented. | NIST SP 800-53, PM-14  NIST SP 800-53, PM-31 |
| SM.04.01.03 An entity-level supply chain risk management strategy is developed, documented, and periodically reviewed and updated. The strategy should manage risks associated with developing, acquiring, maintaining, and disposing of systems, system components, and system services. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating the entity-level supply chain risk management strategy through   * inquiry of appropriate personnel, including the senior officials responsible for the strategy, and * inspection of relevant documentation.   Inspect the entity-level supply chain risk management strategy. Consider whether the plan   * has been recently reviewed and updated, as appropriate; * is aligned with the entity-level risk management strategy for information security and privacy risks; * includes required information in accordance with authoritative criteria; * addresses the development, acquisition, maintenance, and disposal of systems, system components, and system services; and * is adequate for prioritizing the entity’s implementation of activities to assess, respond to, and monitor supply chain risks.   Determine whether the entity-level supply chain risk management strategy is effectively designed, has been appropriately documented, and is periodically reviewed and updated.  Throughout the engagement, determine whether the entity-level supply chain risk management strategy has been implemented. | NIST SP 800-53, PM-30  NIST SP 800-53, SR-03  NIST SP 800-53, SR-04  NIST SP 800-53, SR-05  NIST SP 800-53, SR-06 |
| SM.04.02 Risk identification, analysis, and response activities are conducted. | | |
| SM.04.02.01 Security categorization of the information system and the information it processes, stores, and transmits has been completed based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals. The security categorization has been documented and approved.  *Related controls: SM.01.06.02 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   * inquiry of appropriate personnel, including authorizing officials responsible for approving security categorization decisions; * inspection of relevant documentation, including system security and privacy plans; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the system security and privacy plans for each relevant information system. Consider whether the plans   * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * provide an adequate supporting rationale for the security categorization of the information system, based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals.   Determine whether the security categorization for each relevant information system flows logically from the supporting rationale documented within the respective system security and privacy plan. | NIST SP 800-53, RA-02 |
| SM.04.02.02 Risk assessments are conducted and documented to   * identify threats to and vulnerabilities in the system; * determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and * determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.   *Related controls: SM.04.02.03, SM.04.02.04, and SM.04.02.05* | Obtain an understanding of the entity’s processes and methods for conducting and documenting risk assessments through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation, including risk assessments relevant to the significant business processes and areas of audit interest that demonstrate the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the risk assessments relevant to the significant business processes and areas of audit interest, including any risk assessments conducted and documented for the relevant information systems. Consider whether the risk assessments   * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); * identify threats to and vulnerabilities in the respective systems; * determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the respective systems, as well as the information processed, stored, or transmitted by such systems; and * determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.   Determine whether the entity’s processes and methods for conducting and documenting risk assessments are effectively designed and implemented to reasonably assure that risks are properly identified and analyzed.  Determine whether the risk assessments relevant to the significant business processes and areas of audit interest have been conducted and documented in accordance with the entity’s policies and procedures.  Note: Risk assessments may be documented within risk assessment reports, security and privacy plans, or other entity-defined documents detailing the results of entity risk assessments. Reviewing the results of entity risk assessments may be useful in assessing risk and determining the nature, timing, and extent of further audit procedures. | NIST SP 800-53, RA-03  NIST SP 800-53, RA-06  NIST SP 800-53, RA-10 |
| SM.04.02.03 Vulnerability scan reports and results from vulnerability monitoring inform the entity’s risk assessment process. The results of penetration testing, when conducted, also inform the entity’s risk assessment process.  *Related controls: SM.04.02.02, 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.  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  NIST SP 800-53, RA-05 |
| SM.04.02.04 Risk assessment results, including validation and mitigation, are documented, analyzed, and approved by management.  *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   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation, including risk response documentation, demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect risk response documentation for the risk assessments relevant to the significant business processes and areas of audit interest, including any risk assessments conducted and documented for the relevant information systems. Consider whether the risk response documentation   * has been approved by the appropriate senior official(s) and * is adequate to demonstrate that risks identified through the risk assessment process have been appropriately analyzed as part of the risk response process.   Determine whether the entity’s processes and methods for analyzing and responding to risks are effectively designed and implemented to reasonably assure that risks are properly validated and mitigated.  Determine whether the risk response documentation for the risk assessments relevant to the significant business processes and areas of audit interest has been prepared in accordance with the entity’s policies and procedures. | NIST SP 800-53, RA-03  NIST SP 800-53, RA-07 |
| 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.  *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.  Determine whether risks are reassessed periodically or to address changes to relevant information systems, the system’s environments of operation, or other conditions that may affect the security or privacy state of the systems.  Determine whether the frequency of the entity’s reassessment of risks is appropriate. | 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.  *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.  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 achieve the entity’s information security and privacy objectives and respond to risks. | | |
| SM.05.01 Information security and privacy policies and procedures are developed and implemented. | | |
| SM.05.01.01 Management develops, documents, and periodically reviews and updates information security and privacy policies and procedures. These policies and procedures are implemented at the entity and system levels and are approved by management. They also appropriately   * consider risk; * address purpose, scope, roles, responsibilities, coordination among business or organizational units as well as external parties, and compliance; * describe the process; * consider general and application controls; * consider segregation of duties controls; and * ensure that users can be held accountable for their actions.   Note: Information security and privacy policies and procedures may be applicable across multiple FISCAM control categories—business process controls, security management, access controls, segregation of duties, configuration management, and contingency planning. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating entity-level and system-level information security and privacy policies and procedures through   * inquiry of appropriate personnel and * inspection of relevant documentation, including the entity’s policies and procedures relevant to the significant business processes and areas of audit interest.   Throughout the engagement, determine whether the entity’s processes and methods for developing, documenting, and periodically reviewing and updating entity-level and system-level information security and privacy policies and procedures are designed, implemented, and operating effectively.  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   * policies appropriately consider risk and sufficiently address purpose, scope, roles, responsibilities, coordination among business or organizational units and with external parties, and compliance; * procedures adequately describe the process (including standards, criteria, tasks, tools, and techniques), sufficiently address responsibilities so that users can be held accountable for their actions, and appropriately consider general and application controls and segregation of duties controls; and * policies and procedures are accurate, clearly written, and sufficiently detailed to satisfy their intended purpose and support achieving the entity’s internal control objectives.   Note: The auditor performs audit procedures to assess whether the entity appropriately develops, documents, and periodically reviews and updates its entity-level and system-level information security and privacy policies and procedures. Such assessment is intended to be performed in conjunction with audit procedures to assess the design, implementation, and operating effectiveness of 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. | NIST SP 800-53, AC-01  NIST SP 800-53, AT-01  NIST SP 800-53, AU-01  NIST SP 800-53, CA-01  NIST SP 800-53, CM-01  NIST SP 800-53, CP-01  NIST SP 800-53, IA-01  NIST SP 800-53, IR-01  NIST SP 800-53, MA-01  NIST SP 800-53, MP-01  NIST SP 800-53, PE-01  NIST SP 800-53, PL-01  NIST SP 800-53, PM-01  NIST SP 800-53, PS-01  NIST SP 800-53, PT-01  NIST SP 800-53, RA-01  NIST SP 800-53, SA-01  NIST SP 800-53, SC-01  NIST SP 800-53, SI-01  NIST SP 800-53, SR-01 |
| SM.05.02 Information systems are authorized to operate. | | |
| SM.05.02.01 Common controls are authorized for inheritance before commencing operations and are reauthorized on a periodic basis thereafter.  *Related control: SM.01.02.02* | Obtain an understanding of the entity’s processes and methods for authorizing and periodically reauthorizing common controls for inheritance through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; * inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the relevant information systems.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the authorization packages for each relevant information system. Consider whether   * the information contained in the authorization package is updated on an ongoing basis through comprehensive continuous monitoring activities, * authorization decisions flow logically from the supporting rationale documented within the authorization package, * authorization decisions are made on a timely basis in accordance with the entity-defined frequency, and * the entity-defined frequency for reauthorizations is appropriate.   Determine whether the authorizing official(s) for relevant information systems appropriately authorized inherited common controls before commencing operations and has since appropriately reauthorized the inheritance of such controls on a periodic basis.  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.  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 frequency when the system is operating under an ongoing authorization.  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. | NIST SP 800-53, CA-06  NIST SP 800-53, PM-10 |
| SM.05.02.02 The information system is authorized to operate before commencing operations, is authorized to use inherited common controls, and is reauthorized periodically thereafter. | Obtain an understanding of the entity’s processes and methods for authorizing and periodically reauthorizing an information system to operate, including the use of inherited common controls, through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the relevant information systems.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the authorization packages for each of relevant information systems. Consider whether   * the information contained in the authorization package is updated on an ongoing basis through comprehensive continuous monitoring activities, * authorization decisions flow logically from the supporting rationale documented within the authorization package, * authorization decisions are made on a timely basis in accordance with the entity-defined frequency, and * the entity-defined frequency for reauthorizations is appropriate.   Determine whether the authorizing official(s) for relevant information systems appropriately authorized 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. | NIST SP 800-53, CA-06  NIST SP 800-53, PM-10 |
| SM.05.02.03 The authorization to operate is documented within an authorization package, which includes an executive summary, system security and privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones. | Obtain an understanding of the entity’s processes and methods for preparing and assembling authorization packages through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the process, such as authorization packages for the relevant information systems.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the authorization packages for each of relevant information systems. Consider whether each authorization package   * includes required information in accordance with authoritative criteria and * is adequately documented to support the authorization decisions expressed therein.   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.  Note: Reviewing the authorization packages may be useful in assessing risk and determining the nature, timing, and extent of further audit procedures. | NIST SP 800-53, CA-06 |
| 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.  *Related controls: SM.04.01.02, CM.03.01.01, and CM.03.02.01* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level continuous monitoring strategies through   * inquiry of appropriate personnel, including the senior official(s) responsible for the strategies, and * inspection of relevant documentation.   Inspect the system-level continuous monitoring strategy for each relevant information system. Consider whether each of the strategies   * has been recently reviewed and updated, as appropriate; * is aligned with the entity-level continuous monitoring strategy; * includes required information in accordance with authoritative criteria; * establishes the metrics, frequency, and type(s) of control assessments and monitoring to be performed; * defines the process for correlating, analyzing, and responding to control assessment and monitoring results; and * is adequate for prioritizing the entity’s implementation of activities to facilitate ongoing awareness of the security and privacy posture of the information system.   Determine whether the system-level continuous monitoring strategy for each of relevant information systems is effectively designed, has been appropriately documented, and is periodically reviewed and updated.  Throughout the engagement, determine whether the system-level continuous monitoring strategy for each of relevant information systems has been implemented. | NIST SP 800-53, CA-07  NIST SP 800-53, PM-31 |
| SM.06.01.02 System-level control monitoring activities are implemented in accordance with the system-level continuous monitoring strategy to assess controls and identify risks at a frequency sufficient to support risk-based decisions.  *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   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the process, such as relevant system-level control monitoring documentation, the system-level continuous monitoring strategy, and the entity-level continuous monitoring strategy.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect relevant system-level control monitoring documentation for each relevant information system. Consider whether   * system-level control monitoring activities are implemented in accordance with the system-level continuous monitoring strategy and * system-level control monitoring documentation is adequate to facilitate ongoing awareness of the security and privacy posture of the information system.   Determine whether system-level control monitoring activities are implemented in accordance with the system-level continuous monitoring strategy to assess controls and identify risks at a frequency sufficient to support risk-based decisions.  Note: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support entity risk management decisions. “Continuous” implies that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. Control monitoring activities may include a combination of ongoing monitoring activities and separate evaluations. The use of separate evaluations includes entity self-assessments, as well as results of audits, examinations, and other independent assessments performed by internal auditors, external 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. | NIST SP 800-53, CA-07 |
| SM.06.01.03 Assessors with appropriate skills and technical expertise periodically perform security and privacy control assessments.  *Related controls: SM.06.01.02 and SM.06.01.04* | Obtain an understanding of the entity’s processes and methods for conducting security and privacy control assessments through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the process, such as relevant control assessment plans and reports.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect relevant control assessment plans and reports for each relevant information system. Consider whether   * the security and privacy control assessments were performed recently and used current information, * the control assessment plan was reviewed and approved by the authorizing official prior to performing the assessment, * the security and privacy control assessments were performed by assessors with appropriate skills and technical expertise, and * the control assessment report is adequate to facilitate communication of the security and privacy posture of the information system.   Determine whether security and privacy control assessments for the relevant information system are properly performed on a periodic basis by assessors with appropriate skills and technical expertise.  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 development, system security engineering, privacy engineering, and the system development life cycle. | NIST SP 800-53, CA-02 |
| SM.06.01.04 Control assessment reports are shared with appropriate personnel. These reports document the assessment results in sufficient detail to enable such personnel to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements.  *Related control: SM.06.01.03* | Inspect relevant control assessment reports for each relevant information system and inquire with appropriate personnel to obtain an understanding of how control assessment results are documented and shared. Consider whether   * the control assessment reports include sufficient detail to enable personnel to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements and * communication mechanisms exist to facilitate the sharing of control assessment reports with appropriate personnel.   Determine whether control assessment reports are shared with appropriate personnel and document the assessment results in sufficient detail. | NIST SP 800-53, CA-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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the process.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the performance measures and compliance metrics for information security and privacy functions applicable to the relevant information systems. Consider whether   * management periodically evaluates the performance measures and compliance metrics and * management uses the performance measures and compliance metrics appropriately to measure the effectiveness or efficiency of the information security and privacy functions.   Determine whether performance measures and compliance metrics are periodically evaluated and appropriately employed to measure the effectiveness or efficiency of information security and privacy functions. | NIST SP 800-53, PM-06 |
| 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.  *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   * inquiry of appropriate personnel, including the authorizing officials for relevant information systems, and * inspection of relevant documentation, including plans of action and milestones included in the authorization packages for relevant information systems.   Inspect plans of action and milestones for relevant information systems. Consider whether these plans   * have been recently reviewed and updated, as appropriate; * are consistent with the entity-level risk management strategy; * respond to risk; * focus on remediating the root causes of identified deficiencies and vulnerabilities; and * are adequate to assign responsibilities and guide the implementation of corrective actions to fully resolve (or substantially mitigate risks associated with) identified deficiencies and vulnerabilities on a timely basis.   Determine whether the plans of action and milestones for relevant information systems have been appropriately documented and periodically reviewed and updated.  Note: A plan of action and milestones is a document that identifies tasks needing to be accomplished and details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. | NIST SP 800-53, CA-05  NIST SP 800-53, PM-04  NIST SP 800-53, SR-03 |
| SM.07.01.02 Control deficiencies and vulnerabilities are analyzed in relation to the entire entity, and appropriate corrective actions are applied entity-wide.  *Related control: SM.07.01.01* | Inspect plans of action and milestones for the 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   * specify when entity-wide corrective actions are necessary and * are adequate to guide the implementation of entity-wide corrective actions to fully resolve (or substantially mitigate risks associated with) identified deficiencies and vulnerabilities.   Determine whether control deficiencies and vulnerabilities are adequately analyzed in relation to the entire entity and appropriate corrective actions are applied entity-wide. | NIST SP 800-53, PM-04 |
| SM.07.01.03 Remediation tasks and milestones are accomplished by scheduled completion dates.  *Related control: SM.07.01.01* | Inspect plans of action and milestones for the 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   * have been recently reviewed and updated, as appropriate; * reflect reasonable scheduled completion dates; and * are adequate to demonstrate progress the entity made in accomplishing remediation tasks and milestones to fully resolve (or substantially mitigate risks associated with) identified deficiencies and vulnerabilities on a timely basis.   Determine whether remediation tasks and milestones are accomplished by scheduled completion dates. | NIST SP 800-53, CA-05 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-24-107026

540 FISCAM Framework for Access Controls

1. 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 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.
2. 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.

1. 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 National Institute of Standards and Technology (NIST) Special Publication (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.  *Related controls: BP.05.03.01 and SM.03.02.01* | Obtain an understanding of the entity’s processes and methods for establishing, documenting, periodically reviewing and updating, and approving system information exchanges through   * inquiry of appropriate personnel, including authorizing officials, network engineers, system developers, and network and system administrators, and * inspection of relevant documentation, such as network maps, system security and privacy plans, and exchange agreements.   Inquire of appropriate personnel and inspect network maps to obtain an understanding of relevant network and system topologies, including information system boundaries, system interconnections, and key devices, for the 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 system information exchanges relevant to the significant business processes. Determine whether key system information exchanges were appropriately established based on risk.  Inspect system security and privacy plans, interconnection security agreements, information exchange security agreements, memorandums of understanding or agreement, service-level agreements, user agreements, nondisclosure agreements, or other exchange agreements applicable to the key system information exchanges. Consider whether such documentation   * has been recently reviewed and updated, as appropriate; * has been approved by appropriate senior official(s); * includes required information in accordance with authoritative criteria; * accurately describes the key system information exchanges; and * is adequate to communicate and reinforce the entity’s processes and methods to protect the access paths, control the flow of information, and reasonably assure that connectivity to system resources is appropriately controlled.   Determine whether key system information exchanges have been appropriately documented, periodically reviewed and updated, and properly approved.  Note: Authorizing officials determine the risk associated with system information exchanges and the controls needed for appropriate risk mitigation. The type of exchange agreement selected is based on factors such as the impact level of the information being exchanged, the relationship between the entities exchanging information, and the level of access to the organizational system granted to users of the other system. | NIST SP 800-53, AC-04  NIST SP 800-53, CA-03  NIST SP 800-53, CA-09 |
| AC.01.01.02 Networks are appropriately structured and network components are properly configured to protect access paths within and between systems.  *Related control: CM.01.04.01* | Obtain an understanding of the entity’s processes and methods for structuring networks and configuring network components through   * inquiry of appropriate personnel, including network engineers, system developers, and network and system administrators; * inspection of relevant policies and procedures; and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inquire of appropriate personnel and inspect network maps to obtain an understanding of relevant network and system topologies, including information system boundaries, system interconnections, and key devices, for the 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.  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, AC-04  NIST SP 800-53, SC-07  NIST SP 800-53, SC-37  NIST SP 800-53, SC-46  NIST SP 800-53, SC-49  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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to uniquely identify and authenticate devices. Consider whether such processes and methods   * adequately address the access paths within and between the relevant information systems; * adequately address the components of the information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; and * reasonably assure that devices are properly identified and authenticated before connections to relevant information systems, or their components, are established.   Determine whether relevant information systems uniquely identify and authenticate devices before establishing a connection. | NIST SP 800-53, IA-03  NIST SP 800-53, IA-04 |
| AC.01.01.04 Remote access is appropriately controlled and protected.  *Related control: AC.01.01.05* | Obtain an understanding of the processes and methods that relevant information systems employ to control and protect remote access (dial-up or broadband) through   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to control and protect remote access. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; and * reasonably assure that remote access to information systems or their components is appropriately controlled and protected.   Observe appropriate personnel as they obtain remote access to relevant information systems and their components. Consider whether the processes and methods observed to control and protect remote access are consistent with those the entity has documented.  Obtain an understanding of the entity’s processes and methods to log and monitor remote access to relevant information systems and their components through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether remote access is appropriately controlled and protected for relevant information systems.  Note: Remote access is access to organizational systems (or process acting on behalf of user) that communicate through external networks, such as the internet. Types of remote access include dial-up, broadband, and wireless. | NIST SP 800-53, AC-03  NIST SP 800-53, AC-17 |
| AC.01.01.05 Wireless access is appropriately controlled and protected.  *Related control: AC.01.01.04* | Obtain an understanding of the entity’s processes and methods to control and protect wireless access to entity networks, network components, information systems, and information system components through   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to control and protect wireless access to entity networks, network components, information systems, and information system components. Consider whether such processes and methods   * include procedures for identifying and remediating rogue wireless access points; * are suitably designed and properly implemented based on risk; and * reasonably assure that wireless access to entity networks, network components, information systems, and information system components is appropriately controlled and protected.   Observe appropriate personnel as they obtain wireless access to entity networks, network components, information systems, and information system components, as applicable. Consider whether the processes and methods observed to control and protect wireless access are consistent with those the entity has documented.  Observe appropriate personnel as they perform procedures for identifying and remediating rogue wireless access points. Consider whether the procedures observed are consistent with those the entity has documented.  Obtain an understanding of the entity’s processes and methods to log and monitor wireless access to entity networks, network components, information systems, and information system components through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether wireless access to entity networks, network components, information systems, and information system components is appropriately controlled and protected.  Note: A rogue wireless access point is an unauthorized node on a network that connects to a wired network using a wireless network standard. | NIST SP 800-53, AC-18  NIST SP 800-53, SC-43 |
| 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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to enable or prevent the use of mobile devices and personally owned systems, components, or devices. Consider whether such processes and methods   * include entity-level policies on the use of mobile devices and personally owned systems, components, or devices; * include procedures for requesting and approving the use of mobile devices and personally owned systems, components, or devices; * include software update or configuration requirements imposed on individual users to mitigate risks associated with the use of mobile devices and personally owned systems, components, or devices; * include mechanisms to monitor and enforce software update or configuration requirements imposed on individual users; * are suitably designed and properly implemented based on risk; and * reasonably assure that system connectivity using mobile devices and personally owned systems, components, or devices is approved only when appropriate to perform assigned official duties.   Inquire with appropriate personnel to obtain an understanding of the extent to which entity personnel may use mobile devices and personally owned systems, components, or devices when performing significant business processes. If applicable, observe personnel as they use mobile devices and personally owned systems, components, or devices to perform significant business processes.  Determine whether system connectivity using mobile devices and personally owned systems, components, or devices is approved only when appropriate to perform assigned official duties. | NIST SP 800-53, AC-17  NIST SP 800-53, AC-18  NIST SP 800-53, AC-19  NIST SP 800-53, AC-20  NIST SP 800-53, SC-43 |
| AC.01.02 Network sessions are appropriately controlled. | | |
| AC.01.02.01 Where connectivity is not continual, the network connection automatically disconnects at the end of a communications session. | Obtain an understanding of the entity’s processes and methods to automatically disconnect network connections at the end of communications sessions through   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as policies and procedures for managing network connectivity and implemented configuration settings, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to automatically disconnect network connections at the end of communications sessions. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that network connections are appropriately disconnected.   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 using identification and authentication procedures. | Obtain an understanding of the entity’s processes and methods to use device locks to prevent unauthorized access to systems through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for managing device locks and implemented configuration settings for initiating device locks after a specified period of inactivity, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to use device locks to prevent unauthorized access to systems. Consider whether such processes and methods   * include entity-level policies on the use of device locks before leaving systems unattended, * are suitably designed and properly implemented based on risk, and * reasonably assure that device locks are consistently and properly initiated and remain in effect until users reestablish access using identification and authentication procedures.   Observe a user initiate a device lock.  Observe the system to determine whether the system automatically initiates a device lock after a period of inactivity.  Determine whether device locks are properly used to prevent unauthorized access to systems. | NIST SP 800-53, AC-11 |
| AC.01.02.03 A user session is automatically terminated when certain conditions or events occur. | Obtain an understanding of the processes and methods that relevant information systems employ to automatically terminate user sessions when certain conditions or events occur through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for managing user sessions and implemented configuration settings for terminating user sessions when certain conditions or events occur, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to automatically terminate user sessions when certain conditions or events occur. Consider whether such processes and methods   * identify the conditions or events that will prompt the information system to automatically terminate a user session, * are suitably designed and properly implemented based on risk, and * reasonably assure that user sessions are appropriately terminated.   Observe the occurrence of the conditions or events that should prompt an information system to automatically terminate a user session.  Determine whether user sessions for relevant information systems are automatically terminated when certain conditions or events occur. | NIST SP 800-53, AC-12 |
| AC.01.02.04 Appropriate notifications are displayed on screen   * before users log onto a system and until they acknowledge the notifications (for example, U.S. government system, consent to monitoring, penalties for unauthorized use, privacy notices) and * after successful log-on to the system (for example, date and time of last log-on and unsuccessful log-ons). | Inquire of appropriate personnel, including users, to obtain an understanding of the entity’s use of system notifications for the relevant information systems.  Observe appropriate personnel as they obtain access to relevant information systems.  Determine whether appropriate notifications are displayed on screen before users log onto a system and after successful log-on. | NIST SP 800-53, AC-08  NIST SP 800-53, AC-09 |
| 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).  *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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and authentication parameters evidenced by system configuration files and reports produced by access control software.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to reasonably assure that identification and authentication is unique to each user (or process acting on behalf of a user). Consider whether such processes and methods   * include entity-level policies requiring unique identification and authentication of users and processes; * identify (preferably within the entity-level policies) any specific conditions or circumstances in which unique identification and authentication may not be necessary and for which an exception may be requested and approved; * include procedures for requesting and approving exceptions to the requirement for unique identification and authentication of users and processes; * maintain a complete listing of any specially approved instances in which unique identification and authentication is not required, which is shared with authorizing officials and other IT management personnel; * are suitably designed and properly implemented based on risk; and * reasonably assure that identification and authentication is unique to each user (or process acting on behalf of user), except in specially approved instances.   Inquire of appropriate personnel to obtain an understanding of any specially approved instances in which unique identification and authentication is not required.  Inspect documentation for any specially approved instances in which unique identification and authentication is not required. Consider whether the documentation for any specially approved instances   * has been recently reviewed and updated, as appropriate; * describes the status of any mitigating factors or compensating controls cited as part of the entity’s approval of the exception; * accurately describes the impact of the exception on information systems and common controls available for inheritance to enable authorizing officials to assess risk and determine whether the mitigating factors or compensating controls sufficiently reduce risk to an acceptable level; and * demonstrates that the exception was properly approved in accordance with the entity’s procedures.   Identify any specially approved instances that affect the relevant information systems or their components, including related operating systems and data management systems.  Obtain an understanding of any compensating controls cited as part of the entity’s approval of relevant exceptions through   * inquiry of appropriate personnel; * inspection of relevant documentation, such as policies and procedures; and * observation of the entity’s application of compensating controls.   Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated with any specially approved instances affecting relevant information systems or their components.  Determine whether identification and authentication applicable to relevant information systems and their components is unique to each user (or process acting on behalf of a user), except in specially approved instances. | NIST SP 800-53, IA-02  NIST SP 800-53, IA-08  NIST SP 800-53, IA-09  NIST SP 800-53, AC-14 |
| AC.02.01.02 Authenticators (for example, passwords, tokens, biometrics, key cards, Public Key Infrastructure (PKI) certificates, or multifactor authenticator), including strength of mechanism, are selected and employed based on risk.  *Related control: AC.02.04.01* | Obtain an understanding of any entity-level policies or procedures governing the selection of authenticators through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of authenticators selected for use in connection with relevant information systems and their components. Consider whether the authenticators   * have sufficient strength of mechanism for their intended use, * were selected in accordance with the entity’s policies and procedures, and * are suitably designed and properly implemented based on risk.   Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components.  Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components.  Determine whether the authenticators selected for use in connection with the relevant information systems and their components are appropriate based on risk. | NIST SP 800-53, IA-05  NIST SP 800-53, IA-10 |
| 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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as entity-level or system-level policies and procedures for authenticator management, system security and privacy plans, and access control software authentication parameters.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to protect authenticators and authentication information feedback from unauthorized disclosure or modification. Consider whether such processes and methods are suitably designed and properly implemented based on risk.  Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components. Consider whether authentication information feedback is obscured.  Determine whether the authenticators and authentication information feedback applicable to relevant information systems and their components are adequately protected from unauthorized disclosure or modification. | NIST SP 800-53, IA-05  NIST SP 800-53, IA-06 |
| AC.02.01.04 PKI-based authentication validates certificates by constructing a certification path to an accepted trust anchor, establishes user control of the corresponding private key, and maps the authenticated identity to the user account.  *Related control: AC.02.02.02* | Obtain an understanding of any entity-level policies or procedures governing PKI-based authentication methods through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of any PKI-based authentication methods used in connection with relevant information systems and their components. Consider whether the PKI-based authentication methods   * validate certificates by constructing a certification path to an accepted trust anchor, * establish user control over the corresponding private key, * map the authenticated identity to the user account, and * satisfy information security requirements in accordance with authoritative criteria.   Inspect certificate parameters.  Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components.  Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components.  Determine whether any PKI-based authentication methods used in connection with relevant information systems and their components are suitably designed and properly implemented based on risk. | NIST SP 800-53, IA-05 |
| AC.02.01.05 Password-based authenticators   * are not displayed when entered; * are changed periodically (e.g., every 30 to 90 days); * contain alphanumeric and special characters; * are sufficiently complex (e.g., not easily guessed, minimum length, no words, etc.); * have an appropriate life (e.g., automatically expire); * are prohibited from reuse for a specified period (e.g., at least six generations); and * 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of any password-based authenticators used in connection with relevant information systems and their components. Consider whether the password-based authenticators   * are not displayed when entered; * are changed periodically (e.g., every 30 to 90 days); * contain alphanumeric and special characters; * are sufficiently complex (e.g., not easily guessed, minimum length, no words, etc.); * have an appropriate life (e.g., automatically expire); * are prohibited from reuse for a specified period (e.g., at least six generations); * are not the same as the user ID; and * satisfy information security requirements in accordance with authoritative criteria.   Inspect access control software authentication parameters.  Observe appropriate personnel using valid authenticators to obtain access to relevant information systems and their components.  Observe appropriate personnel attempting to use invalid authenticators to obtain access to relevant information systems and their components.  Determine whether any password-based authenticators used in connection with relevant information systems and their components are suitably designed and properly implemented based on risk. | NIST SP 800-53, IA-05  NIST SP 800-53, IA-06 |
| AC.02.01.06 Shared or group authenticators are only used in specially approved instances.  *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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and authentication parameters evidenced by system configuration files and reports produced using access control software.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods for approving shared or group authenticators in special instances. Consider whether such processes and methods   * include entity-level policies requiring unique identification and authentication of users and processes; * identify (preferably within the entity-level policies) any specific conditions or circumstances in which unique identification and authentication may not be necessary and for which an exception may be requested and approved; * include procedures for requesting and approving exceptions to the requirement for unique identification and authentication of users and processes; * maintain a complete listing of any specially approved instances in which unique identification and authentication is not required, which is shared with authorizing officials and other IT management personnel; * are suitably designed and properly implemented based on risk; and * reasonably assure that shared or group authenticators are not used, except in specially approved instances.   Inquire of appropriate personnel to obtain an understanding of any specially approved instances in which shared or group authenticators are permitted.  Inspect documentation for any specially approved instances in which shared or group authenticators are permitted. Consider whether the documentation for any specially approved instances   * has been recently reviewed and updated, as appropriate; * describes the status of any mitigating factors or compensating controls cited as part of the entity’s approval of the exception; * accurately describes the impact of the exception on information systems and common controls available for inheritance to enable authorizing officials to assess risk and determine whether the mitigating factors or compensating controls sufficiently reduce risk to an acceptable level; and * demonstrates that the exception was properly approved in accordance with the entity’s procedures.   Identify any specially approved instances that affect the relevant information systems or their components, including related operating systems and data management systems.  Obtain an understanding of any compensating controls cited as part of the entity’s approval of relevant exceptions through   * inquiry of appropriate personnel; * inspection of relevant documentation, such as policies and procedures; and * observation of the entity’s application of compensating controls.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated with any specially approved instances affecting relevant information systems or their components.  Determine whether shared or group authenticators are only used in specially approved instances.  Note: Unique identification of individuals in group accounts is required for detailed accountability of individual activity. If shared or group authenticators are used, the authenticators should be promptly changed when membership to the shared or group account changes to ensure that former members do not retain access to the shared or group account. Management should only authorize the use of shared or group authenticators for specific shared or group accounts. | NIST SP 800-53, AC-02  NIST SP 800-53, IA-02  NIST SP 800-53, IA-05 |
| AC.02.01.07 Vendor-supplied default passwords are replaced during software or hardware installation. | Obtain an understanding of any entity-level policies or procedures governing the replacement of vendor-supplied default passwords during software or hardware installation through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures for system component installation and configuration.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect password files using audit software to verify whether common vendor-supplied passwords are in use.  Determine whether vendor-supplied default passwords are replaced during installation for relevant 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   * inquiry of appropriate personnel, including network engineers, system developers, and network and system administrators, and * inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and authentication parameters, as well as relevant programs or program source code, as applicable.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to reasonably assure that passwords embedded in programs are not used. Consider whether such processes and methods   * include entity-level policies prohibiting passwords embedded in programs; * identify (preferably within the entity-level policies) any specific conditions or circumstances in which the use of passwords embedded in programs may be necessary and for which an exception may be requested and approved; * include procedures for requesting and approving exceptions to the prohibition for passwords embedded in programs; * maintain a complete listing of any specially approved instances in which the use of passwords embedded in programs is necessary, which is shared with authorizing officials and other IT management personnel; * are suitably designed and properly implemented based on risk; and * reasonably assure that passwords embedded in programs are not used, except in specially approved instances.   Identify any specially approved instances that affect the relevant information systems or their components, including related operating systems and data management systems.  Obtain an understanding of any compensating controls cited as part of the entity’s approval of relevant exceptions through   * inquiry of appropriate personnel; * inspection of relevant documentation, such as policies and procedures; and * observation of the entity’s application of compensating controls.   Determine whether the compensating controls are designed, implemented, and operating effectively to mitigate the risks associated with any specially approved instances affecting relevant information systems or their components.  Determine whether passwords embedded in programs are only used in specially approved instances.  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. | NIST SP 800-53, IA-05 |
| 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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed to prevent improper duplication of authenticators and to administer lost, compromised, or damaged authenticators (e.g., passwords, tokens, biometrics, key cards, or PKI certificates).  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 |
| AC.02.01.10 Account policies (including password, authentication, and lockout policies) are appropriate based on risk and enforced. | Obtain an understanding of the entity’s processes and methods for establishing and implementing account policies through   * inquiry of appropriate personnel, including users, and * inspection of relevant documentation and account policy settings.   Inspect relevant documentation and account policy settings for a selection of account policies (including password, authentication, and lockout policies) applicable to relevant information systems and their components.  Determine whether enabled account policies applicable to relevant information systems and their components are appropriate based on risk and enforced. | NIST SP 800-53, AC-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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to limit consecutive log-on attempts. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; and * reasonably assure that consecutive attempts to log on with invalid passwords within a certain period are limited.   Observe users as they repeatedly attempt to log onto relevant information systems and their components using invalid passwords. Consider whether the processes and methods observed to limit consecutive log-on attempts are consistent with those documented by the entity.  Obtain an understanding of the entity’s processes and methods to log and monitor consecutive log-on attempts to relevant information systems and their components through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether relevant information systems and their components appropriately limit consecutive attempts to log on with invalid passwords within a certain period. | NIST SP 800-53, AC-07 |
| AC.02.02 Information system users, processes, and services are appropriately identified and authenticated before accessing information systems. | | |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   Inspect available documentation for a selection of individuals for whom user credentials were established during the audit period. Consider whether evidence of each individual’s identity was presented, validated, and verified   * based on applicable identity assurance-level requirements and * before the entity provides user credentials for the individual.   Determine whether evidence of an individual’s identity is presented, validated, and verified based on applicable identity assurance-level requirements before the entity provides user credentials. | NIST SP 800-53, IA-12 |
| AC.02.02.02 PKI certificates are issued in accordance with an approved certificate policy or obtained from an approved service provider. Only approved trust anchors are included in trust stores or certificate stores that the entity manages.  *Related control: AC.02.01.04* | Obtain an understanding of the entity’s process and methods for issuing PKI certificates through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect available documentation for a selection of user accounts applicable to relevant information systems and their components for which PKI certificates were issued during the audit period. Consider whether the PKI certificates were either   * issued in accordance with an approved certificate policy or * obtained from an approved service provider.   Determine whether PKI certificates are issued in accordance with an approved certificate policy or obtained from an approved service provider.  Determine whether only approved trust anchors are included in trust stores or certificate stores that the entity manages. | NIST SP 800-53, SC-17 |
| 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of identity providers and authorization servers. Consider whether the identity providers and authorization servers   * are appropriate for their intended use, * were selected in accordance with the entity’s policies and procedures, and * are suitably designed and properly implemented based on risk.   Determine whether 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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as policies and procedures for managing sessions, as well as implemented configuration settings, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to implement session-level controls. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; and * reasonably assure that appropriate session-level controls are implemented.   Consider the adequacy of session-level controls, including name and address resolution service, session authenticity, protection of session-level information held in temporary storage, and other controls to reasonably assure that one session ends before the next session begins (i.e., prevent overlapping sessions).  Determine whether appropriate session-level controls are implemented. | NIST SP 800-53, SC-20  NIST SP 800-53, SC-21  NIST SP 800-53, SC-22  NIST SP 800-53, SC-23 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for managing user reauthentication, as well as implemented configuration settings requiring user reauthentication when specific circumstances or situations occur, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to require user reauthentication when specific circumstances or situations occur. Consider whether such processes and methods   * identify the specific circumstances or situations (e.g., changes in roles, authenticators, or credentials) that will prompt the information system to require a user to reauthenticate; * are suitably designed and properly implemented based on risk; and * reasonably assure that user reauthentication is required as appropriate.   Observe the occurrence of the specific circumstances or situations that should prompt the information system to require a user to reauthenticate.  Determine whether specific circumstances or situations that require the information systems to reauthenticate users are appropriate based on risk. | NIST SP 800-53, IA-11 |
| 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   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as policies and procedures for managing user sessions, as well as implemented configuration settings for controlling concurrent sessions, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to control concurrent sessions. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that concurrent sessions are appropriately controlled.   Observe appropriate personnel as they initiate concurrent sessions on relevant information systems. Consider whether the processes and methods observed to control concurrent sessions are consistent with those the entity has documented. Consider whether concurrent sessions could be used to (1) enable an unauthorized individual to access the information system or (2) enable an authorized user to circumvent information system segregation of duties controls.  Obtain an understanding of the entity’s processes and methods to log and monitor concurrent sessions on relevant information systems through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether concurrent sessions on relevant information systems are appropriately controlled. | NIST SP 800-53, AC-10 |
| 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of digital signatures and other nonrepudiation mechanisms employed in connection with the significant business processes, the relevant information systems, and their components. Consider whether the digital signatures and other nonrepudiation mechanisms   * were selected in accordance with the entity’s policies and procedures and * are suitably designed and properly implemented based on risk.   Observe appropriate personnel as they employ digital signatures and other nonrepudiation mechanisms in connection with the significant business processes, the relevant information systems, and their components.  Determine whether the digital signatures and other nonrepudiation mechanisms are appropriately employed in connection with the significant business processes, the relevant information systems, and their components.  Note: Nonrepudiation mechanisms provide (1) protection when an individual falsely denies having performed a certain action and (2) the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message. | NIST SP 800-53, AU-10 |
| 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.  *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   * inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and * inspection of relevant documentation.   Inspect relevant system documentation identifying the types of accounts allowed and specifically prohibited for use for relevant information systems. Consider whether   * the definitions include usage and restriction conditions and * the criteria for group and role membership are specified.   Determine whether the types of accounts, their usage and restriction conditions, and if applicable criteria for group and role membership have been appropriately documented and are appropriate based on risk.  Inspect a system-generated list of accounts. Consider the appropriateness of system-generated evidence when performing control tests. Consider whether the list includes undefined or prohibited types of accounts. Determine whether the types of accounts established are appropriate.  Note: Account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. | NIST SP 800-53, AC-02 |
| AC.02.03.02 Access authorizations for each type of account are defined, documented, and periodically reviewed and updated.  *Related controls: AC.02.03.05, AC.02.04.01, and SD.01.02.02* | Obtain an understanding of the entity’s processes and methods for defining, documenting, and periodically reviewing and updating the information system users and their authorized access through   * inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and * inspection of relevant documentation.   Inspect relevant policies and procedures for access authorization and account management, system security and privacy plans, and other documentation identifying the account types and their access authorization for the relevant information systems. Consider whether   * privileged and nonprivileged users and their authorized access are accurately identified and * the access that information system users are authorized to have is compatible with segregation of duties requirements.   Determine whether the information system users and their authorized access to relevant information systems are appropriate based on risk and consistent with the concept of least privilege.  Determine whether the information system users and their authorized access to relevant information systems have been appropriately documented and periodically reviewed and updated. | NIST SP 800-53, AC-02 |
| AC.02.03.03 Account management processes are implemented to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed.  *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   * inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; * inspection of relevant policies and procedures for access authorization and account management; and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed.  Inspect available documentation for a selection of accounts that were created, enabled, modified, disabled, or removed during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures for access authorization and account management. Consider whether the administrators responsible for account management actions identify and discuss any questionable authorizations with information resource owners.  Determine whether the account management processes applicable to relevant information systems are designed, implemented, and operating effectively to reasonably assure that accounts are properly created, enabled, modified, disabled, and removed. | NIST SP 800-53, AC-02 |
| 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.  *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   * inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; * inspection of relevant policies and procedures for account management; and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed to reasonably assure that accounts are timely modified, disabled, or removed when associated access privileges or accounts are no longer required.  Inspect available documentation for a selection of accounts that were modified, disabled, or removed during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures for account management.  Inspect access control software parameters for disabling inactive accounts and verify whether such are consistent with the entity’s policies and procedures for account management.  Inquire of the administrators responsible for account management actions and inspect a system-generated list of disabled accounts to determine why the disabled accounts have not been removed. Consider the appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.  Inspect a system-generated list of enabled user accounts and a list of recently separated personnel to determine whether user accounts for recently separated personnel remain enabled after their separation dates. Consider the appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.  Determine whether the account management processes applicable to relevant information systems are designed, implemented, and operating effectively to reasonably assure that accounts are timely modified, disabled, or removed when associated access privileges or accounts are no longer required. | NIST SP 800-53, AC-02 |
| AC.02.03.05 Access to systems and system resources is limited to individuals with a valid business purpose (least privilege).  *Related controls: AC.02.03.02, 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   * inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials, and * inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and other documentation identifying the information system users and their authorized access.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to reasonably assure that system access is limited to individuals with a valid business purpose. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that system access is limited to individuals with a valid business purpose.   Inspect available documentation for a selection of user accounts that were created, enabled, or modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures for account management.  Inspect system-generated listings of user accounts and privileged user accounts to determine whether the access privileges associated with such accounts are consistent with the access privileges defined and documented for such users. Consider the appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.  Determine whether system access is limited to individuals with a valid business purpose (least privilege) for relevant information systems. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-06 |
| AC.02.03.06 Emergency and temporary access to systems and system resources is appropriately controlled.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for the use of emergency and temporary accounts, including firecall IDs.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to control emergency and temporary access to the relevant information systems. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * include entity-level policies governing the use of emergency and temporary accounts, including firecall IDs; * identify (preferably within the entity-level policies) the specific conditions or circumstances in which emergency or temporary accounts may be used, as well as the specific functions or tasks that individuals may perform while using emergency or temporary accounts; * maintain a complete listing of individuals who are authorized to use emergency or temporary accounts, which is shared with authorizing officials and other IT management personnel; * include procedures for requesting and approving the use of emergency and temporary accounts; * include procedures for creating, enabling, modifying, disabling, and removing emergency and temporary accounts; * are suitably designed and properly implemented based on risk; and * reasonably assure that emergency and temporary access to information systems is appropriately controlled and protected.   Obtain an understanding of the entity’s processes and methods to log and monitor emergency and temporary access to the relevant information systems through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  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.  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.  Determine whether emergency and temporary access to the relevant information systems is appropriately controlled.  Note: Temporary and emergency accounts are intended for short-term use. Entities establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Entities establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account management processes. | NIST SP 800-53, AC-02 |
| AC.02.03.07 Access to shared file systems is appropriately restricted. | Obtain an understanding of the entity’s processes and methods to restrict access to shared file systems relevant to the significant business processes through   * inquiry of appropriate personnel, including network and system administrators, and * inspection of relevant documentation, such as policies and procedures for managing access to shared file systems.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to restrict access to shared file systems relevant to the significant business processes. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that access to shared file systems relevant to the significant business processes is appropriately restricted.   Observe appropriate personnel as they obtain access to the shared file systems relevant to the significant business processes. Consider whether the processes and methods observed to restrict access to shared file systems are consistent with those the entity has documented.  Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software to determine whether access to shared file systems relevant to the significant business processes is appropriately restricted to authorized personnel.  Inspect available documentation for a selection of instances in which access to shared file systems relevant to the significant business processes was modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures. Consider the appropriateness of the documentation obtained, including any logs of changes to access control parameters, when performing control tests.  Obtain an understanding of the entity’s processes and methods to log and monitor access to the shared file systems, as well as changes to access control parameters, relevant to the significant business processes through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether access to shared file systems relevant to the significant business processes is appropriately restricted. | NIST SP 800-53, AC-06 |
| 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   * inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; * inspection of relevant policies and procedures for access authorization, account management, and periodic access recertification; and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which access to the 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.  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. | NIST SP 800-53, AC-02 |
| AC.02.03.09 Access control parameters are set to apply access control decisions and enforce access as authorized.  *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   * inquiry of appropriate personnel, including network and system administrators, information resource owners, and authorizing officials, and * inspection of relevant documentation, such as policies and procedures for managing access control software, as well as implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to apply access control decisions and enforce access as authorized. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; and * reasonably assure that access control parameters are properly set to apply access control decisions and enforce access as authorized.   For each 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.  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 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.  Obtain an understanding of the entity’s processes and methods to log and monitor changes to access control parameters through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether access control parameters applicable to relevant information systems are properly set to apply access control decisions and enforce access as authorized.  Note: Access control parameters are set to apply access control decisions to 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. | NIST SP 800-53, AC-03  NIST SP 800-53, AC-24  NIST SP 800-53, AC-25 |
| AC.02.03.10 The system is configured to provide only those functions and services that are necessary to support entity operations through, for example,   * installing only required functions and services based on least functionality, * restricting access to required functions and services based on least privilege, * monitoring the use of functions and services, and * employing appropriate tools and technologies to identify and prevent the use of prohibited functions and services.   *Related controls: SD.01.02.02, CM.01.04.01, and CM.03.01.01* | Obtain an understanding of the entity’s processes and methods for the relevant information systems to reasonably assure that system functions and services are limited to those necessary to support entity operations through   * inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and * inspection of relevant documentation, such as policies and procedures, system security and privacy plans, and other documentation identifying the functions and services each information system is configured to provide.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods for relevant information systems to reasonably assure that system functions and services are limited to those necessary to support entity operations. Consider whether such processes and methods   * include policies and procedures for installing only required functions and services based on least functionality, * include policies and procedures for restricting access to required functions and services based on least privilege, * address monitoring the use of functions and services, * employ appropriate tools and technologies to identify and prevent the use of prohibited functions and services, * are suitably designed and properly implemented based on risk, and * reasonably assure that system functions and services are limited to those that are necessary to support entity operations.   Determine whether relevant information systems are properly configured to provide only those functions and services necessary to support entity operations. | NIST SP 800-53, CM-07  NIST SP 800-53, SC-41 |
| 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   * inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and * inspection of relevant documentation, such as policies and procedures for managing collaborative computing devices and applications, as well as implemented configuration settings, found in applicable system configuration files.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to prohibit remote activation of collaborative computing devices and applications. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that the information systems prohibit remote activation of collaborative computing devices and applications.   Observe appropriate personnel as they use collaborative computing devices and applications. Determine whether the system provides an explicit indication of use of such devices and applications to the local user.  Determine whether relevant information systems prohibit remote activation of collaborative computing devices.  Note: Collaborative computing devices and applications include remote meeting devices and applications, networked whiteboards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated. | NIST SP 800-53, SC-15 |
| 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.  *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   * inquiry of appropriate personnel, including privileged users, network and system administrators, information resource owners, and authorizing officials, and * inspection of relevant documentation, such as relevant policies and procedures for access authorization and account management, system security and privacy plans, and other documentation identifying privileged users and the access they are authorized to have.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to reasonably assure that the use of privileged accounts is appropriately restricted. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * include entity-level policies governing the use of privileged accounts; * identify (preferably within the entity-level policies) the specific functions or tasks that individuals may perform while using privileged accounts; * maintain a complete listing of individuals who are authorized to use privileged accounts, which is shared with authorizing officials and other IT management personnel; * are suitably designed and properly implemented based on risk; and * reasonably assure that privileged access is limited to individuals or processes with a valid business purpose.   Inspect available documentation for a selection of privileged accounts that were created, enabled, or modified during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures for account management.  Inspect system-generated listings of privileged accounts to determine whether the access privileges associated with such accounts are consistent with the access privileges defined and documented for privileged users or processes. Consider the appropriateness of the documentation obtained, including any system-generated listings, when performing control tests.  Determine whether the use of privileged accounts is restricted to individuals or processes with a legitimate need for privileged access to information resources to accomplish valid business functions. | NIST SP 800-53, AC-02  NIST SP 800-53, AC-06 |
| AC.02.04.02 The use of privileged accounts is appropriately logged and adequately monitored. | Obtain an understanding of the entity’s processes and methods to log and monitor the use of privileged accounts through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * 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.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to log and monitor the use of privileged accounts. Consider whether such processes and methods   * adequately address the components of the relevant information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; * reasonably assure that reports that log management software produces and management reviews are complete and accurate; and * reasonably assure that the entity takes appropriate action to identify and address any access anomalies.   Observe the entity’s processes and methods to log and monitor the use of privileged accounts and inspect relevant reports that log management software produces and management reviews. Consider the appropriateness of these reports when performing control tests.  See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether the use of privileged accounts is appropriately logged and adequately monitored. | NIST SP 800-53, AC-02  NIST SP 800-53, AU-06 |
| 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   * inquiry of appropriate personnel, including network and system administrators, information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to control, log, and monitor logical access to maintenance tools and utilities applicable to relevant information systems. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * are suitably designed and properly implemented based on risk; * reasonably assure that logical access to maintenance tools and utilities applicable to relevant information systems is appropriately controlled and logged; * reasonably assure that reports that log management software produces and management reviews are complete and accurate; and * reasonably assure that management takes appropriate action to identify and address any access anomalies.   Observe appropriate personnel as they obtain logical access to maintenance tools and utilities applicable to relevant information systems. Consider whether the processes and methods for controlling logical access are consistent with those documented by the entity.  Observe the entity’s processes and methods to log and monitor logical access to maintenance tools and utilities applicable to relevant information systems and inspect relevant reports that log management software produces and management reviews. Consider the appropriateness of these reports when performing control tests.  See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether logical access to maintenance tools and utilities applicable to relevant information systems is appropriately controlled and logged and adequately monitored. | NIST SP 800-53, AC-02  NIST SP 800-53, MA-02  NIST SP 800-53, MA-03  NIST SP 800-53, MA-04  NIST SP 800-53, MA-05 |
| 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   * inquiry of appropriate personnel, including authorizing officials, system developers, and network and system administrators, and * inspection of relevant documentation, such as policies and procedures for managing authenticators and authentication services and directories, as well as implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports produced by access control software.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to control logical access to authenticators and authentication services and directories. Consider whether such processes and methods   * adequately address the components of the information systems, including related operating systems and data management systems; * employ encryption techniques when appropriate based on risk; * are suitably designed and properly implemented based on risk; and * reasonably assure that access to authenticators and authentication services and directories is restricted to authorized individuals for authorized purposes.   Obtain an understanding of the entity’s processes and methods to log and monitor logical access to authenticators and authentication services and directories applicable to relevant information systems and their components through   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  Determine whether authenticators and authentication services and directories applicable to relevant information systems and their components are appropriately controlled and encrypted when necessary. | NIST SP 800-53, AC-02  NIST SP 800-53, IA-05 |
| AC.02.04.05 Mobile code is appropriately controlled. | Obtain an understanding of the entity’s processes and methods to control mobile code through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to control mobile code. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that mobile code is appropriately controlled.   Determine whether mobile code is appropriately controlled.  Note: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. | NIST SP 800-53, SC-18  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   * inquiry of appropriate personnel, including system developers, system administrators, and authorizing officials, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the processes and methods that relevant information systems employ to establish an isolated, trusted communications path between the user and trusted components of the information system. Consider whether such processes and methods   * identify and adequately address the trusted components of the information systems; * are suitably designed and properly implemented based on risk; and * reasonably assure that an isolated, trusted communications path between the user and trusted components of the information system is established.   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.  Note: Entities employ trusted paths for trustworthy, high-assurance connections between systems’ security functions and users, including during system log-ons. | NIST SP 800-53, SC-11 |
| 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   * inquiry of appropriate personnel, including users, information resource owners, and authorizing officials, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to limit access to printed and digital media containing data removed from relevant information systems. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that only authorized users with a valid business purpose have access to printed and digital media containing data removed from the information systems.   Determine whether access to printed and digital media containing data removed from relevant information systems is appropriately limited to authorized individuals for authorized purposes.  Note: Digital media 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. | NIST SP 800-53, MP-02 |
| 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   * inquiry of appropriate personnel, including system developers, users, information resource owners, and authorizing officials, and * inspection of relevant documentation.   Inspect documentation, such as relevant system output reports and exports of relevant database schemas, demonstrating the design and implementation of the processes and methods that relevant information systems employ to mark output and associate attributes with internal data in storage, process, and transmission. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk; * employ standard practices for marking output, including the use of standard naming conventions; * employ standard practices for associating security and privacy attributes to internal data, including the labeling of data; and * reasonably assure that associated security and privacy attributes are not modified when information is exchanged between information systems and their components.   Determine whether relevant information systems appropriately mark output and associate attributes with internal data in storage, process, and transmission.  Note: The association of attributes to subjects and objects by an information system is referred to as binding and includes setting the attribute value and the attribute type. Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of personally identifiable information, and identification of personal information within data objects.  Entities can define the types of attributes needed for information systems to support mission or business functions. Labeling refers to the association of attributes with the subjects and objects represented by the internal data structures within information systems. This facilitates system-based enforcement of information security and privacy policies. A related term to labeling is marking. Marking refers to the association of attributes with objects in a human-readable form displayed on system output. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. | NIST SP 800-53, AC-16  NIST SP 800-53, MP-03  NIST SP 800-53, SC-16 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Observe the entity’s processes and methods for controlling the collection, transport, and delivery of system media associated with relevant information systems.  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.  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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Observe the entity’s processes and methods for storing system media associated with relevant information systems. Consider whether the processes and methods adequately address the sensitivity of data contained within such media and legal and entity information retention requirements.  Determine whether system media associated with relevant information systems are securely stored according to their sensitivity until destroyed or sanitized. | NIST SP 800-53, MP-04 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Observe the entity’s processes and methods for sanitizing and disposing of data, documentation, tools, or system components associated with relevant information systems. Consider whether the processes and methods adequately address the approved equipment, techniques, and procedures to be used based on the type of digital media, as well as the sensitivity of data contained within such media. Consider whether processes and methods adequately address sanitizing data, documentation, tools, or system components before disposal or release or reuse outside of the entity.  Inspect a selection of recently sanitized digital media and determine whether such have been properly sanitized.  Inspect a selection of disposal records data, documentation, tools, or system components and determine whether such have been properly disposed of.  Determine whether the approved equipment, techniques, and procedures for sanitizing and disposing of data, documentation, tools, or system components associated with relevant information systems are appropriate based on the sensitivity of data. | NIST SP 800-53, MP-06  NIST SP 800-53, MP-08  NIST SP 800-53, SR-12 |
| AC.03.02 Cryptographic controls are appropriately selected and employed based on risk. | | |
| AC.03.02.01 Cryptographic tools are implemented to protect the integrity and confidentiality of data and software when appropriate. | Obtain an understanding of any entity-level policies or procedures governing the selection and use of cryptographic tools through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of cryptographic tools selected for use in connection with relevant information systems and their components. Consider whether the cryptographic tools   * are appropriate for their intended use, * were selected in accordance with the entity’s policies and procedures, and * are suitably designed and properly implemented based on risk.   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  NIST SP 800-53, SC-28 |
| AC.03.02.02 Encryption techniques are implemented to protect data communications when appropriate.  *Related control: BP.05.03.03* | Obtain an understanding of any entity-level policies or procedures governing the selection and use of encryption techniques through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of encryption techniques selected for use in connection with relevant information systems and their components, including related operating systems and data management systems. Consider whether the encryption techniques   * are appropriate for their intended use, * were selected in accordance with the entity’s policies and procedures, and * are suitably designed and properly implemented based on risk.   Determine whether the encryption techniques selected for use in connection with relevant information systems and their components are properly implemented to protect data communications, as applicable. | NIST SP 800-53, SC-08 |
| 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   * are appropriate and * are suitably designed and properly implemented based on risk.   Determine whether appropriate mechanisms are properly employed for authentication to cryptographic modules applicable to relevant information systems.  Note: Authentication mechanisms are hardware- or software-based mechanisms that force users to prove their identities before accessing information. | NIST SP 800-53, IA-07 |
| 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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Through inquiry, inspection, and observation, identify and assess the adequacy of controls employed in connection with cryptographic key generation distribution, storage, access, and destruction.  Determine whether the cryptographic key establishment and management processes applicable to relevant information systems are designed, implemented, and operating effectively. | NIST SP 800-53, SC-12 |
| AC.04 Management designs and implements 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the entity-level risk management strategy for information security and privacy risks.  Determine whether physical and environmental hazards to the facilities where relevant information systems reside are appropriately assessed and included as part of the entity-level risk management strategy.  Note: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. | NIST SP 800-53, PE-23 |
| 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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the position of system components within the applicable facilities.   Inspect a diagram of the physical layout of the facilities where relevant information systems reside. Identify sensitive areas housing critical system components or concentrations of system resources (e.g., data centers and server rooms).  Perform walk-throughs of the facilities where relevant information systems reside. Identify the position of system components comprising relevant information systems within the facilities. Consider whether nonessential support entities residing at the facilities are colocated with the system components. See AC.04.01.06 for considerations related to physical access controls.  Determine whether system components comprising relevant information systems are positioned within applicable facilities to mitigate the risk of unauthorized access and minimize potential damage from physical and environmental hazards.  Note: Entities consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to entity communications. When possible, system components should not be colocated with nonessential support entities (e.g., cafeterias, day cares, bank branches, etc.). | NIST SP 800-53, PE-18  NIST SP 800-53, PE-19  NIST SP 800-53, PE-21 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the list of individuals with authorized access to these facilities. Consider whether the list   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); and * is adequate to clearly identify individuals with authorized access and the individuals authorizing the access.   Inspect the authorized access list and a list of recently separated personnel to verify whether the names of recently separated personnel remained on the authorized access list after their separation dates. Consider the appropriateness of the documentation obtained, including any system-generated listings of recently separated personnel.  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.  Note: Individuals with authorized access to facilities may include employees, contractors, and others who routinely need access to facilities where systems reside. | NIST SP 800-53, PE-02 |
| AC.04.01.04 Physical access authorization credentials are issued to individuals who are authorized to access facilities where systems reside.  *Related control: AC.02.02.01* | Obtain an understanding of the entity’s process and methods for issuing physical access authorizations credentials through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures.   Inspect available documentation for a selection of individuals for whom physical access authorization credentials were issued during the audit period.  Observe practices for safeguarding unissued physical access authorization credentials.  Determine whether physical access authorization credentials are properly issued to individuals who are authorized to access facilities where relevant information systems reside.  Note: Physical access authorization credentials include ID badges, identification cards, and smart cards. | NIST SP 800-53, MA-05  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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures for managing visitor access to applicable facilities.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of individuals who visited the facilities where relevant information systems reside during the audit period. Consider whether   * the visitor screening activities performed, including any background screening requirements completed prior to a visitor accessing the facilities, are appropriate based on risk; * the conditions or circumstances requiring visitors to be escorted are consistently applied and appropriate based on risk; and * the maintenance of records associated with visitor access to the facilities is sufficient to demonstrate the performance of applicable general controls associated with a visitor’s access.   Observe entries to and exits from facilities where relevant information systems reside during and after normal business hours.  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. | NIST SP 800-53, MA-05  NIST SP 800-53, PE-02 |
| 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   * guards and guard posts; * physical access devices and barriers; * physical access logs, including visitor access records, used in conjunction with lists of individuals with authorized access; * requirements for individuals to carry or display ID badges (including visitor badges); and * physical perimeter security checks, patrols, and inspections. | Obtain an understanding of the physical access controls that the entity employs for the facilities where relevant information systems reside through   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the entity’s use of physical access controls.   Inspect a diagram of the physical layout of the facilities where 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).  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.  Observe practices for safeguarding physical access devices, such as keys and combinations, applicable to the key access points.  Determine whether physical access authorizations are adequately enforced at entity-defined entry and exit points, as well as interior access points relevant to sensitive areas, for the facilities where relevant information systems reside.  Note: Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical barriers include doors, gates, fences, bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers. Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and the names and organizations of individuals visited. | NIST SP 800-53, PE-03  NIST SP 800-53, PE-08  NIST SP 800-53, PE-16 |
| AC.04.01.07 Physical access is monitored at entity-defined entry and exit points, as well as interior access points relevant to sensitive areas, for facilities where systems reside through the selection and employment of physical access monitoring controls based on risk, including   * guards and guard posts, * video surveillance equipment, and * physical intrusion alarms. | Obtain an understanding of the physical access monitoring controls that the entity employs for the facilities where relevant information systems reside through   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the entity’s use of physical access monitoring controls.   Inspect a diagram of the physical layout of the facilities where 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).  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.  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.  Note: Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. | NIST SP 800-53, PE-06 |
| 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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to log and monitor physical access to the facilities where 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   * are suitably designed and properly implemented based on risk, * reasonably assure that reports that log management software produce and management reviews are complete and accurate, and * reasonably assure that the entity takes appropriate action to identify and address any physical access anomalies.   Observe the entity’s processes and methods 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.  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.  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.  See AC.05.01 and AC.05.02 for additional general controls and audit procedures related to logging and monitoring.  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.  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. | NIST SP 800-53, PE-06  NIST SP 800-53, PE-08 |
| 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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the entity’s use of security controls applicable to system distribution and transmission lines.   Perform walk-throughs of the facilities where 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.  Determine whether physical access to system distribution and transmission lines is appropriately controlled.  Note: Security controls are applied to system distribution and transmission lines to prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls of physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors. | NIST SP 800-53, PE-04 |
| 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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the entity’s processes and methods for controlling physical access to system output devices.   Perform walk-throughs of the facilities where relevant information systems reside. Identify the controls that the entity employs to manage physical access to system output devices. Consider whether the selection and employment of such controls are appropriate based on risk. Determine whether the entity’s controls for managing physical access to system output devices are designed, implemented, and operating effectively.  Determine whether physical access to system output devices is appropriately controlled.  Note: Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers. Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and limiting access to authorized individuals only, placing output devices in locations that authorized personnel can monitor, installing monitor or screen filters, and using headphones. | NIST SP 800-53, PE-05 |
| 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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the entity’s processes and methods for controlling physical access to power equipment and cabling.   Perform walk-throughs of the facilities where 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.  Determine whether physical access to power equipment and cabling is appropriately controlled.  Note: Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, as well as generators and power cabling outside of buildings. | NIST SP 800-53, PE-09 |
| 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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s intrusion detection tools and software, and * inspection of relevant documentation, such as network maps, policies and procedures for logging, monitoring, and managing the entity’s intrusion detection tools and software, and reports or alerts that intrusion detection software produces and management reviews.   Inspect documentation demonstrating the design and implementation of the entity’s intrusion detection system. Consider whether the entity’s intrusion detection system   * adequately addresses the relevant information systems processes; * adequately addresses the components of relevant information systems; * adequately addresses the placement of intrusion detection sensors and incident thresholds; * is suitably designed and properly implemented based on risk; * reasonably assures that reports or alerts produced by intrusion detection software and reviewed by management are complete and accurate; and * 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.   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. | NIST SP 800-53, SI-04 |
| AC.05.01.02 A process is established to periodically identify and select event types for logging based on risk.  *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the event types selected for logging. Identify the event types selected for logging that are applicable to the 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.  Consider whether the following event types have been selected for logging:   * remote access (dial-up or broadband) to relevant information systems (see AC.01.01.04); * wireless access to entity networks, network components, information systems, and information system components (see AC.01.01.05); * consecutive attempts to log on with invalid passwords within a certain period (see AC.02.01.11); * concurrent sessions (see AC.02.02.06); * emergency and temporary access to relevant information systems (see AC.02.03.06); * access to shared file systems (see AC.02.03.07); * access control parameters (see AC.02.03.09); * the use of privileged accounts (see AC.02.04.02); * logical access to maintenance tools and utilities (see AC.02.04.03); * logical access to authenticators and authentication services and directories (see AC.02.04.05); and * physical access to facilities where systems reside, as well as sensitive areas within such facilities (see AC.04.01.08).   Consider whether the event types selected for logging that are applicable to the relevant information systems, including related operating systems and data management systems, are adequate to support appropriate incident response.  Determine whether the process established to periodically identify and select event types for logging is designed, implemented, and operating effectively and appropriate based on risk.  Note: An event is an observable occurrence. The types of events that require logging are those events that are significant and relevant to the 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. | NIST SP 800-53, AU-02  NIST SP 800-53, SA-20 |
| AC.05.01.03 All event types selected for logging are logged.  *Related controls: BP.01.02.03, BP.02.01.02, BP.02.01.05, BP.04.06.05, BP.05.04.05, 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   * inquiry of appropriate personnel, including information resource owners, authorizing officials, and IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as reports that log management software produces and management reviews.   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.  Determine whether all event types selected for logging that are applicable to relevant information systems are appropriately logged.  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. | NIST SP 800-53, AU-12 |
| AC.05.01.04 Audit records contain appropriate information for effective review, including sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and any identities associated with the event.  *Related control: AC.05.01.02, 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.  Determine whether the audit records contain appropriate information for effective review, including sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and any identities associated with the event.  Note: Audit record content that may be necessary to support the auditing function includes event descriptions, time stamps, source and destination addresses, user or process identifiers, success or fail indications, and file names involved. 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  NIST SP 800-53, AU-08  NIST SP 800-53, SC-45 |
| AC.05.01.05 Audit log storage capacity is allocated to meet audit log retention requirements. In the event of an audit logging process failure, including deficient audit log storage capacity, the system alerts appropriate personnel and personnel take timely, appropriate action.  *Related controls: AC.05.01.02 and AC.05.01.03* | Obtain an understanding of the entity’s processes and methods to reasonably assure that audit log storage capacity is allocated to meet log retention requirements through   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as implemented configuration settings, found in applicable system configuration files.   Inspect implemented storage parameters evidenced by applicable system configuration files and reports produced by log management software to determine whether the allocation of audit log storage capacity is adequate to meet audit log retention requirements.  Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. Consider whether all required audit records associated with such events are available for inspection.  If applicable, inspect available documentation for any instances in which an audit logging process failure occurred during the audit period and determine whether such instances were identified and appropriately resolved on a timely basis.  Determine whether audit log storage capacity is allocated to meet audit log retention requirements and whether appropriate action is taken on a timely basis in the event of an audit logging process failure. | NIST SP 800-53, AU-04  NIST SP 800-53, AU-05 |
| AC.05.01.06 Audit records and audit logging tools are protected from unauthorized access, modification, and deletion. In the event of unauthorized access, modification, or deletion of audit information, the system alerts appropriate personnel and personnel take timely, appropriate action.  *Related controls: SD.01.01.01, AC.05.01.02, and AC.05.01.03* | Obtain an understanding of the entity’s processes and methods to reasonably assure that audit records and audit logging tools are protected from unauthorized access, modification, and deletion through   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as implemented access control parameters.   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.  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.  If applicable, inspect available documentation for any instances in which unauthorized access, modification, or deletion of audit information occurred and determine whether such instances were identified and appropriately resolved on a timely basis.  Determine whether audit records and audit logging tools are protected from unauthorized access, modification, and deletion and whether appropriate action is taken on a timely basis in the event of unauthorized access, modification, or deletion of audit information.  Note: Audit information includes all information needed to successfully audit information system activity, such as audit records, audit log settings, reports that log management software produce, and personally identifiable information included in such reports. Log management tools and software are those programs and devices used to conduct information system audit and logging activities. | NIST SP 800-53, AU-09 |
| AC.05.01.07 Audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet legal and entity information retention requirements.  *Related controls: 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 are retained long enough to provide support for after-the-fact investigations of security incidents and to meet legal and regulatory requirements and entity policies on information retention through   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s log management tools and software, and * inspection of relevant documentation, such as policies and procedures for logging, monitoring, and managing log management tools and software, as well as implemented configuration settings, found in applicable system configuration files.   Inspect available audit records for a selection of events that occurred during the audit period applicable to the relevant information systems. Consider whether all required audit records associated with such events are available for inspection.  Determine whether audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet legal and regulatory requirements and entity policies on information retention. | NIST SP 800-53, AU-11 |
| AC.05.01.08 A process is established for session auditing based on risk. | Obtain an understanding of the entity’s process and methods for session auditing through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether such processes and methods   * adequately define the situations for which session auditing may be employed, * adequately address the use of personally identifiable information, and * are suitably designed and properly implemented based on risk.   Determine whether the process established for session auditing is designed, implemented, and operating effectively and appropriately based on risk.  Note: Session audits can include monitoring keystrokes, tracking websites visited, and recording information and file transfers. | NIST SP 800-53, AU-14 |
| AC.05.02 Incidents are properly analyzed, and appropriate actions are taken. | | |
| AC.05.02.01 Audit records are regularly reviewed and analyzed for indications of inappropriate or unusual activity, and audit records that indicate suspicious activity or suspected violations are reported and investigated.  *Related controls: AC.05.01.02, 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   * inquiry of appropriate personnel, including users, network and system administrators, information resource owners, and authorizing officials; * inspection of relevant policies and procedures for logging, monitoring, and managing log management tools and software; * observation of the processes for regularly reviewing and analyzing audit records; and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available audit records for a selection of events that occurred during the audit period applicable to the 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 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.  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. | NIST SP 800-53, AC-02  NIST SP 800-53, AU-06 |
| AC.05.02.02 Investigation results are reported to appropriate personnel, and disciplinary actions are taken when necessary.  *Related control: AC.05.02.01* | Inspect available audit records for a selection of events that occurred during the audit period applicable to the 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.  Determine whether investigation results are reported to appropriate personnel and disciplinary actions are taken when necessary. | NIST SP 800-53, AU-06  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.  *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.  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 |
| AC.05.02.04 External and internal security alerts, advisories, and directives are identified and promptly issued to appropriate personnel, who take appropriate action.  *Related control: SM.01.05.02* | Obtain an understanding of any entity-level policies or procedures governing the identification and issuance of external and internal security alerts, advisories, and directives through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of any entity-level policies or procedures governing the identification and issuance of external and internal security alerts, advisories, and directives. Consider whether appropriate action is taken in response to the issuance of external and internal security alerts, advisories, and directives.  Determine whether external and internal security alerts, advisories, and directives are identified and promptly issued to appropriate personnel, who take appropriate action. | NIST SP 800-53, SI-05 |
| AC.05.02.05 A coordinated, cross-entity approach to sharing incident information is implemented.  *Related control: SM.03.02.01* | Obtain an understanding of the entity’s approach for sharing incident information through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect available documentation demonstrating the implementation of the entity’s approach for sharing incident information. Consider whether the entity’s approach is appropriately coordinated within and across applicable entity units, including external parties when appropriate.  Determine whether a coordinated, cross-entity approach to sharing incident information is implemented.  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. | NIST SP 800-53, AU-16 |
| AC.05.02.06 Information spills and data losses are identified, isolated, and resolved by appropriate personnel. | Obtain an understanding of the entity’s processes and methods to identify, isolate, and resolve information spills and data losses through   * inquiry of appropriate personnel, including incident response team members, and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to identify, isolate, and resolve information spills and data losses. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably ensure that incidents involving information spills and data losses are properly analyzed and appropriate actions are taken.   Determine whether information spills and data losses are properly identified, isolated, and resolved by appropriate personnel.  Note: Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. Data loss is the unauthorized disclosure of proprietary, sensitive, or classified information through data theft (or exfiltration) and data leakage. | NIST SP 800-53, AU-13  NIST SP 800-53, IR-09  NIST SP 800-53, SI-20 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-24-107026

550 FISCAM Framework for Segregation of Duties

1. 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 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.
2. 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.

1. 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 National Institute of Standards and Technology (NIST) Special Publication (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   * preparation of data for input into the system, * approval of data for input into the system, * data input, * research and resolution of data input errors that the system identified, * research and resolution of data processing errors that the system identified, * reconciliation of interfaced data, and * verification of output data.   *Related controls: BP.04.01.02, BP.04.03.07, BP.04.06.02, BP.05.01.02, BP.05.06.01, BP.06.01.02, BP.06.01.03, BP.06.01.04, BP.06.01.05, BP.06.03.05, SM.01.02.03, SM.02.01.03, and AC.05.01.06* | Obtain an understanding of the entity’s processes and methods for identifying, documenting, and periodically reviewing and updating incompatible duties within and across business process functions through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inquire of appropriate personnel and inspect documentation to determine whether incompatible duties within and across business process functions have been properly identified and adequately documented. In determining whether incompatible duties have been properly identified, consider whether the following are true:   * Any business process functions (e.g., billing, cash receipts, purchasing, cash disbursements, and payroll) significant to the engagement objectives are identified as incompatible with other business process functions. * Any specific duties performed by information system users within or across business process functions significant to the engagement objectives are identified as incompatible with other duties. Incompatible duties include initiating and approving transactions and maintaining records and custody of assets.   In determining whether incompatible duties have been adequately documented, consider whether incompatible duties have been clearly identified and the rationale for such identification sufficiently explained to promote a shared understanding of risks among affected organizational units and individuals.  Inspect documentation and inquire of appropriate personnel to determine whether documented incompatible duties are periodically reviewed by appropriate personnel and properly updated to reflect changes in the entity’s organizational structure, operations, or use of information technology. Consider whether incompatible duties documentation has been recently reviewed and updated.  Note: Business process functions comprise the tasks necessary to perform, record, and report on the results of the entity’s mission-related operations. Incompatible duties within and across business process functions are documented in position descriptions and policies and procedures. Incompatible duties are also documented within segregation of duties matrices, which may be developed at the entity, organizational unit, business process function, and system levels. Segregation of duties matrices facilitate the entity’s communication and further identification of incompatible duties. | NIST SP 800-53, AC-05 |
| SD.01.01.02 Identify, document, and periodically review and update incompatible duties within and across IT management (i.e., system support) functions that should not be performed by the same organizational unit or individual. Such duties may include   * information security management, * IT asset management, * system or application design, * system or application programming, * system or application maintenance, * quality assurance testing, * change authorization, * code migration, * configuration auditing, * media management, * production control and scheduling, * application administration, * database administration; * operating system administration, * system administration, * network administration, * security administration, * log management, and * log monitoring.   *Related controls: BP.04.03.07, BP.06.03.05, SM.01.02.03, and SM.02.01.03* | Obtain an understanding of the entity’s processes and methods for identifying, documenting, and periodically reviewing and updating incompatible duties within and across IT management functions through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inquire of appropriate personnel and inspect documentation to determine whether incompatible duties within and across IT management functions have been properly identified and adequately documented. In determining whether incompatible duties have been properly identified, consider whether the following are true:   * Any incompatible duties within and across IT management functions are identified. Incompatible duties within and across IT management functions include authorizing, programming, testing, and implementing changes to relevant information systems and their components, as well as maintaining records and custody of IT assets. For example:   + Programmers should not have the ability to migrate code into the production environment and should not have access to production software or data.   + Security administrators who administer access controls should not also administer changes to network components, applications, databases, operating systems, or other system resources or components.   + Database administrators should not be involved in any IT management functions beyond the duties of database administration.   + Security, network, application, database, operating system, and other system administrators should not be responsible for maintaining the entity’s log management tools and software or reviewing reports that log management software produces.   In determining whether incompatible duties have been adequately documented, consider whether incompatible duties have been clearly identified and the rationale for such identification sufficiently explained to promote a shared understanding of risks among affected organizational units and individuals.  Inspect documentation and inquire of appropriate personnel to determine whether documented incompatible duties are periodically reviewed by appropriate personnel and properly updated to reflect changes in the entity’s organizational structure, operations, or use of information technology. Consider whether incompatible duties documentation has been recently reviewed and updated.  Note: IT management functions comprise the tasks necessary to develop, maintain, and secure the information systems that support the entity’s business process functions. Incompatible duties within and across IT management functions are documented in position descriptions and policies and procedures. Incompatible duties are also documented within segregation of duties matrices, which may be developed at the entity, organizational unit, IT management function, and system levels. Segregation of duties matrices facilitate the entity’s communication and further identification of incompatible duties. | NIST SP 800-53, AC-05 |
| 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.  *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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of personnel performing business process and IT management functions.   Through inquiry, inspection, and observation, identify and assess the adequacy of logical and physical access controls employed to enforce the segregation of identified incompatible duties relevant to the significant business processes. See applicable illustrative controls and audit procedures within AC.02 and AC.04.  Determine whether the segregation of identified incompatible duties relevant to the significant business processes is appropriately enforced by logical and physical access controls.  Note: System user functions and system support functions should be segregated whenever possible. For example, information system users should not have the ability to change application code or information system functionality. Additionally, information system users should not have administrative access to the underlying components of such systems, including related operating systems and data management systems. However, only information system users—not IT management personnel—should have the ability to initiate transactions and authorize changes to transaction data. | NIST SP 800-53, AC-05 |
| SD.01.02.02 The information system prohibits authorized users from performing incompatible duties within and across the business process functions that the system supports.  *Related controls: 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   * inquiry of appropriate personnel; * inspection of relevant documentation, including policies and procedures for the significant business processes; and * observation of personnel performing significant business processes.   Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system’s processes and methods. Consider whether the access privileges or roles assigned to information system users are appropriate to prohibit authorized users from performing incompatible duties.  Through inquiry, inspection, and observation, identify and assess the adequacy of configuration management controls enforcing the system’s processes and methods. Consider whether workflows or processing routines are appropriately designed and under configuration control to prohibit authorized users from bypassing or overriding segregation of duties controls.  Determine whether the system’s processes and methods are designed, implemented, and operating effectively to prohibit authorized users from performing incompatible duties relevant to the significant business processes. | NIST SP 800-53, AC-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   * inquiry of appropriate personnel; * inspection of relevant documentation, including policies and procedures for the significant business processes; and * observation of personnel performing significant business processes.   Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system’s processes and methods. Consider whether user functions, including user interface services, are appropriately segregated from IT management functions.  Determine whether the system’s processes and methods are designed, implemented, and operating effectively to prohibit authorized users from performing IT management functions relevant to the significant business processes.  Note: Business process functions comprise the tasks necessary to perform, record, and report on the results of the entity’s mission-related operations. These functions include the procedures by which transactions are initiated, recorded, processed, and reported, as well as the procedures by which transaction processing errors are detected and corrected.  IT management functions comprise the tasks necessary to develop, maintain, and secure the information systems that support the entity’s business process functions. They typically require access to privileged accounts. Preventing the presentation of IT management functions to nonprivileged users at interfaces ensures that administration options, including administrator privileges, are not available to the general user population. | NIST SP 800-53, AC-05  NIST SP 800-53, SC-02 |
| SD.01.02.04 The information system prohibits IT management personnel from performing business process functions. | Obtain an understanding of the processes and methods that the information system employs to prohibit IT management personnel from performing business process functions relevant to the significant business processes through   * inquiry of appropriate personnel; * inspection of relevant documentation, including policies and procedures for the significant business processes; and * observation of personnel performing significant business processes.   Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system’s processes and methods. Consider whether security administrators who administer access controls are prohibited from performing business process functions.  Determine whether the system’s processes and methods are designed, implemented, and operating effectively to prohibit IT management personnel from performing business process functions relevant to the significant business processes. | NIST SP 800-53, AC-05  NIST SP 800-53, SC-02 |
| SD.01.02.05 The information system isolates security functions from nonsecurity functions.  *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   * inquiry of appropriate personnel; * inspection of relevant documentation, including policies and procedures for security functions; and * observation of IT management personnel performing security functions.   Through inquiry, inspection, and observation, identify and assess the adequacy of logical access controls enforcing the system’s processes and methods. Consider whether the information system adequately restricts access to security functions using appropriate access control mechanisms and by implementing least privilege capabilities.  Determine whether the system’s processes and methods are designed, implemented, and operating effectively to isolate security functions from nonsecurity functions relevant to the significant business processes.  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. | NIST SP 800-53, AC-05  NIST SP 800-53, AC-06  NIST SP 800-53, SC-03  NIST SP 800-53, SC-39 |
| 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.  *Related controls: BP.04.03.07 and BP.06.03.05*  *Related critical element: AC.05* | Obtain an understanding of the entity’s processes and methods for (1) approving exceptions to segregation of duties requirements and (2) designing and implementing alternative general controls to mitigate risks resulting from incompatible duties that cannot be segregated through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inquire of appropriate personnel to obtain an understanding of any approved exceptions to segregation of duties requirements.  Inspect documentation for any approved exceptions to segregation of duties requirements relevant to the significant business processes and areas of audit interest. Consider whether the documentation for any such exceptions   * has been recently reviewed and updated; * describes the status of any mitigating factors or compensating controls cited as part of the entity’s approval of the exception; * accurately describes the impact of the exception on business process and IT management functions, as well as information systems and common controls available for inheritance, to enable senior management and authorizing officials to assess risk and determine whether the mitigating factors or compensating controls sufficiently reduce risk to an acceptable level; and * demonstrates that the exception was properly approved in accordance with the entity’s procedures.   Obtain an understanding of any compensating controls or alternative general controls cited as part of the entity’s approval of relevant exceptions through   * inquiry of appropriate personnel; * inspection of relevant documentation, including policies and procedures; and * observation of the entity’s application of compensating controls.   Determine whether the compensating controls or alternative general controls are designed, implemented, and operating effectively to mitigate the risks associated with incompatible duties that cannot be separated.  Determine whether management appropriately considered and accepted any residual risks associated with exceptions to segregation of duties requirements. | NIST SP 800-53, AC-05 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-24-107026

560 FISCAM Framework for Configuration Management

1. The configuration management (CM) category relates to identifying and managing 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.
2. 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.

1. 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (rev. 5) controls** |
| --- | --- | --- |
| 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.01.01.01 System-level configuration management plans are developed, documented, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system-level configuration management plans through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect the system-level configuration management plans for each relevant information system. Consider whether the plans   * identify roles and responsibilities; * incorporate or reference current entity-level configuration management policies and procedures; * define configuration items for the information system and place such items under configuration management; * establish a process for identifying configuration items throughout the system development life cycle; * establish processes for managing the configuration of these items for the information system and monitoring implemented configuration settings against baseline configurations; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); * include required information in accordance with authoritative criteria; and * are adequate to address configuration management activities applicable to the information system, including any changes to the baseline configuration of the system.   Determine whether the system-level configuration management plans for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, consider whether the system-level configuration management plans for relevant information systems have been implemented.  Note: Configuration management plans satisfy the requirements in entity-level configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities. The plans are generated during the development and acquisition stages of the system development life cycle. The plans describe how to advance changes through change management processes; update implemented configuration settings and baseline configuration settings; maintain information system component inventories; control development, test, and operational environments; and maintain system documentation. | NIST SP 800-53, CM-02  NIST SP 800-53, CM-09 |
| CM.01.01.02 Management selects, tests, and implements configuration settings that optimize the security features of the system and minimize available processes and services consistent with operational requirements and management’s baseline configuration.  *Related control: CM.01.01.03* | Obtain an understanding of the entity’s processes and methods for selecting, testing, and implementing configuration settings for the relevant information systems through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for selecting, testing, and implementing configuration settings for information systems and information system components.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the implemented configuration settings for a selection of configuration items for relevant information systems. Consider whether the implemented configuration settings   * optimize the system’s security features; * minimize available processes and services consistent with operational requirements; * align with entity-level requirements, including any entity-defined common secure configurations; and * are consistent with the corresponding baseline configuration settings.   Determine whether the implemented configuration settings for the configuration items selected have been properly selected, tested, and implemented.  Throughout the engagement, consider whether the implemented configuration settings for the relevant information systems are appropriate for optimizing the systems’ security features and minimizing available processes and services consistent with operational requirements.  Note: Deploying information system components with minimal functionality reduces the need to secure every end point and may reduce the exposure of information, systems, and services to attacks. It may be necessary to enhance or augment the security features of an information system or component that supports critical or essential mission and business functions to maximize the trustworthiness of the resource. Data execution prevention controls can be implemented to protect the information system from adversaries that launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. | NIST SP 800-53, CM-06  NIST SP 800-53, CM-07  NIST SP 800-53, SA-04  NIST SP 800-53, SA-08  NIST SP 800-53, SA-23  NIST SP 800-53, SC-25  NIST SP 800-53, SC-29  NIST SP 800-53, SC-34  NIST SP 800-53, SC-51  NIST SP 800-53, SI-14  NIST SP 800-53, SI-16  NIST SP 800-53, SI-21 |
| CM.01.01.03 Baseline configurations of systems are developed, documented, and periodically reviewed and updated.  *Related control: CM.01.01.02* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating baseline configurations of systems through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for maintaining baseline configurations of systems.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the baseline configurations for the relevant information systems. Consider whether the baseline configurations   * are under configuration control; * are adequate to serve as a basis for future builds, releases, or changes to the information systems; * are based on documented configuration change decisions and reflect the existing enterprise architecture; * include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture; * have been recently reviewed and updated, as appropriate; and * have been approved by the appropriate senior official(s).   Determine whether the baseline configurations for the relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, consider whether the baseline configurations for relevant information systems have been properly maintained.  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. | NIST SP 800-53, CM-02 |
| CM.01.01.04 System documentation for administrators and users is developed, documented, and periodically reviewed and updated.  *Related controls: SM.02.02.03, SM.02.03.03, and AC.02.03.03* | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating system documentation for administrators and users through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for maintaining system documentation.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the system documentation for administrators and users of the relevant information systems. Consider whether the documentation   * is appropriately protected commensurate with the security categorization of the information system; * accurately describes for administrators the secure configuration, installation, and operation of the information system and its components, as well as the effective use and maintenance of security and privacy mechanisms and any known vulnerabilities associated with administrative functions; * accurately describes for users any user-accessible security and privacy mechanisms and their use, as well as user responsibilities for maintaining the security of the system and the privacy of individuals; * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); * includes required information in accordance with authoritative criteria; and * has been distributed to appropriate personnel.   Determine whether system documentation for administrators and users of relevant information systems has been appropriately documented, periodically reviewed and updated, and properly approved.  Note: Entities may require different levels of detail in the documentation for the design and implementation of controls in information systems, information system components, or information system services. The levels of detail are based on mission and business function requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing.  System documentation helps personnel understand the implementation and operation of controls. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, program or software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system. When adequate documentation cannot be obtained from manufacturers or suppliers of information systems, information system components, or information system services, entities may need to recreate the documentation relevant to the implementation or operation of the controls. | NIST SP 800-53, SA-04  NIST SP 800-53, SA-05 |
| CM.01.02 An inventory of information system components is developed and maintained. | | |
| CM.01.02.01 An inventory of system components is developed, documented, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, and periodically reviewing and updating inventories of information system components through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for maintaining information system component inventories.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the inventories of components for relevant information systems. Consider whether each inventory   * accurately reflects the information system; * includes records for all components for the information system; * does not include duplicate records for any components; * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); and * includes required information in accordance with authoritative criteria and in sufficient detail to promote accountability for information system components.   Reconcile inventory records to any listings of information system components included in other information system documentation, such as information security and privacy plans, baseline configurations, or other system documentation. For a selection of inventory records, perform audit procedures to verify the accuracy and validity of the records. When verifying the accuracy and validity of inventory records related to hardware, consider whether the associated hardware components are appropriately marked to identify the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.  Determine whether the inventories of components for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.  Note: An information system component is a discrete identifiable IT asset that represents a building block of a system and may include hardware, software, and firmware. Entities may choose to implement centralized information system component inventories that include components for all entity information systems. In such situations, entities ensure that the inventories include system-specific information required for component accountability.  Information system component inventories are subject to configuration management policies and procedures, and changes to inventory records generally require an appropriate senior official’s approval. Identifying individuals who are responsible and accountable for administering information system components ensures that the assigned components are properly administered and that entity personnel can contact those individuals if some action is required. System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability. | NIST SP 800-53, CM-02  NIST SP 800-53, CM-08  NIST SP 800-53, PE-22 |
| CM.01.02.02 Unauthorized system components are detected and appropriately addressed on a timely basis. | Obtain an understanding of the entity’s processes and methods for detecting and addressing unauthorized information system components through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for monitoring the baseline configurations for information systems.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Observe appropriate personnel as they perform procedures for detecting and addressing unauthorized information system components.  Obtain an understanding of any automated tools the entity uses to facilitate the detection of unauthorized information system components. If automated tools are used, perform appropriate audit procedures to assess whether such tools are properly configured and appropriately employed to detect unauthorized system components and alert appropriate personnel.  Inspect available documentation for a selection of instances in which the entity detected unauthorized information system components. Consider whether appropriate actions were taken to address these components on a timely basis.  Determine whether unauthorized system components are detected and appropriately addressed on a timely basis.  Note: Entities can improve the accuracy, completeness, and consistency of information system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented.  Monitoring for unauthorized information system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to entity systems contributes to providing adequate security. Entities may combine information system component inventory and baseline configuration monitoring activities.  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. | NIST SP 800-53, CM-02  NIST SP 800-53, CM-08 |
| CM.01.02.03 Counterfeit system components are detected and appropriately addressed on a timely basis.  *Related control: CM.03.03.02* | Obtain an understanding of the entity’s processes and methods for detecting and addressing counterfeit information system components through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for determining the authenticity of information system components prior to installation.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Observe appropriate personnel as they perform procedures for detecting and addressing counterfeit information system components.  Inspect available documentation for a selection of instances in which the entity detected counterfeit information system components. Consider whether appropriate actions were taken to address these components on a timely basis.  Determine whether counterfeit information system components are detected and appropriately addressed on a timely basis.  Note: Sources of counterfeit information system components include manufacturers, developers, vendors, and contractors. Entities develop policies and procedures to detect, address, and report counterfeit information system components. | NIST SP 800-53, SR-09  NIST SP 800-53, SR-10  NIST SP 800-53, SR-11 |
| CM.01.03 Configuration items for information systems are identified and placed under configuration management. | | |
| CM.01.03.01 The types of configuration items for information systems are clearly defined. | Inspect the system-level configuration management plans for each relevant information system, as applicable.  Determine whether the types of configuration items for relevant information systems are clearly defined.  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 configuration management process. Configuration items are the information system components, such as the hardware, software, firmware, and documentation that are placed under configuration management. | NIST SP 800-53, CM-02  NIST SP 800-53, CM-09 |
| CM.01.03.02 Configuration items for information systems are identified and placed under configuration management. | Obtain an understanding of the entity’s processes and methods to identify configuration items for information systems and place these items identified under configuration management through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for identifying configuration items and managing the configuration of such items.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to identify configuration items for information systems and place the items identified under configuration management. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that configuration items for information systems are properly identified and placed under configuration management.   Inspect listings of configuration items for the relevant information systems.  Determine whether configuration items for relevant information systems are properly identified and placed under configuration management.  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. | NIST SP 800-53, CM-02  NIST SP 800-53, CM-09 |
| 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.  *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   * inquiry of appropriate personnel and * 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.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the established configuration settings for a selection of configuration items for the relevant information systems. Consider whether these settings   * reflect the most restrictive mode consistent with operational requirements; * align with entity-level requirements, including any entity-defined common secure configurations; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are consistent with implemented configuration settings.   Determine whether the established configuration settings for the configuration items selected have been appropriately documented, periodically reviewed and updated, and properly approved.  Throughout the engagement, consider whether the established configuration settings for the configuration items for relevant information systems have been properly maintained.  Note: Entities establish entity-level configuration settings and subsequently determine specific configuration settings for the items that make up information systems and information system components. The established settings become part of the configuration baseline for the system.  Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for IT products and platforms. They also provide instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including IT product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors. | NIST SP 800-53, CM-06 |
| 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.  *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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity-level and system-level processes. Consider whether the processes   * identify roles and responsibilities; * are integrated with the entity’s system development life cycle processes; * address each type of change to information systems and information system components that is configuration controlled and subject to the entity-level and system-level processes, as applicable; * specify the processes and methods employed for authorizing, testing, and approving planned changes to information systems and information system components, as well as retaining records of such actions for subsequent review and monitoring; * specify the processes and methods for updating baseline configuration documentation as part of the change management process; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are adequate to facilitate and document controlled modifications to hardware, firmware, and software components of entity information systems.   Inspect a selection of changes to configuration items for each relevant information system.  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.  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. | NIST SP 800-53, CM-03  NIST SP 800-53, SA-10  NIST SP 800-53, SA-11  NIST SP 800-53, SA-15  NIST SP 800-53, SA-17 |
| CM.02.01.02 Management authorizes proposed changes to software for development.  *Related control: BP.04.07.01* | Obtain an understanding of the entity’s processes and methods for considering proposed changes to software for the relevant information systems through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   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   * demonstrates that proposed changes are considered and authorized prior to development and * facilitates tracing of source code to the design specifications and functional requirements associated with authorized changes.   Determine whether management has authorized proposed changes to software for relevant information systems for development. | NIST SP 800-53, SA-10 |
| CM.02.01.03 Security and privacy impact analyses are conducted, and the results are documented, approved, and disseminated prior to the implementation of planned changes. | Obtain an understanding of the entity’s processes and methods for conducting security and privacy impact analyses and documenting, approving, and disseminated results through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect any security or privacy impact analyses conducted in connection with planned changes to the relevant information systems. Consider whether such analyses   * have been appropriately documented, approved, and disseminated and * are appropriately considered as part of the processes for formally authorizing, testing, and approving planned changes to information systems and information system components.   Determine whether security and privacy impact analyses are properly conducted, and the results are appropriately documented, approved, and disseminated prior to the implementation of planned changes.  Note: Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks.  Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required. A privacy impact assessment analyzes how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. | NIST SP 800-53, CM-04  NIST SP 800-53, RA-08 |
| 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   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   * provides sufficient evidence of the approval, execution, and review of test plans and results, as appropriate; * demonstrates that a comprehensive set of test transactions and data was developed and used in testing to represent the various activities and conditions that are likely to be encountered in the production environment; * clearly presents the results of testing, including any flaws identified; * identifies the necessary resources, planned actions, and time frames for flaw remediation; and * demonstrates that planned changes to information systems and information system components, including authorized changes to software, are only implemented into the production environment by authorized personnel after management approval.   Inspect available documentation for flaw remediation. Consider whether all flaws identified through testing are remediated or tracked for remediation.  Determine whether planned changes to information systems and information system components, including authorized changes to software, are properly tested. Determine whether flaws identified through testing are appropriately remediated.  Note: Unit testing, integration testing, and regression testing, as well as security and privacy control assessments, are generally performed. Manual code reviews, as well as static code analysis and dynamic code analysis, may also be performed to assess changes to custom software for business process applications. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risks to entities. Entities can minimize such risks by developing and using a comprehensive set of test transactions and data during the development and testing of changes to information systems, information system components, and information system services. | NIST SP 800-53, SA-11 |
| 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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s system development and configuration management tools and software, and * inspection of relevant documentation, such as policies and procedures for using and managing the entity’s system development and configuration management tools and software, as well as implemented configuration settings, found in system configuration files for the tools and software employed.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the implemented configuration settings for the system development and configuration management tools and software employed in connection with relevant information systems and their components. Consider whether the implemented configuration settings are appropriate.  Determine whether management properly employs appropriate tools and software to support the entity’s system development and configuration management processes applicable to relevant information systems.  Note: System development and configuration management tools and software are often employed to produce audit trails of program or software changes; maintain version control of hardware descriptions, source code, and object code; track version numbers on operating systems, applications, programs, and software implemented; log and monitor changes to information system components; remove previous versions of software or firmware components of information systems from the production environment; maintain the composition of open source and proprietary source code, including the current version; securely archive copies of previous versions; and control concurrent updates to information system components. | NIST SP 800-53, SA-15 |
| 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.  *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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity-level and system-level processes. Consider whether the processes   * identify roles and responsibilities; * are integrated with the entity’s system development life cycle processes; * define emergency changes and address each type of change to information systems and information system components that is subject to the entity-level and system-level processes for implementing emergency changes, as applicable; * specify the processes and methods employed for documenting and analyzing emergency changes to information systems and information system components and retaining records of such changes for subsequent review and monitoring; * specify the processes and methods for updating baseline configuration documentation as part of the change management process; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are adequate to facilitate and document controlled modifications to hardware, firmware, and software components of entity information systems in emergency situations where formal authorization, testing, and approval procedures are not feasible.   Inspect a selection of emergency changes to configuration items for each relevant information system.  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.  Note: Making emergency changes often involves using sensitive system utilities or methods that grant much broader access than would normally be needed. It is important that such access is strictly controlled and that its use is promptly reviewed.  Shortly after an emergency change is made, the usual configuration management controls are applied retroactively. The change is subjected to the same review, testing, and approval processes that apply to scheduled changes. In addition, data center management or security administrators periodically review logs of emergency changes and related documentation to determine whether all such changes have been tested and have received final approval. | NIST SP 800-53, CM-03  NIST SP 800-53, SA-10  NIST SP 800-53, SA-11  NIST SP 800-53, SA-15  NIST SP 800-53, SA-17 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as comparing policies and procedures for monitoring implemented configuration settings for information systems and information system components against established configuration settings, including any such settings derived from entity-defined common secure configurations.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Observe appropriate personnel as they perform procedures for identifying and addressing deviations from established configuration settings.  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.  Inspect available documentation for a selection of deviations that the entity identified. Consider whether appropriate actions were taken to address the deviations on a timely basis. Such actions may include   * changing implemented configuration settings for configuration items through a formal configuration management process, * addressing the deviation through the entity’s process for managing plans of action and milestones to document and communicate the actions necessary to fully address the deviation, or * approving the deviation and accepting the risk associated with it.   Inspect implemented configuration settings for a selection of configuration items for the relevant information systems. Consider whether the implemented settings align with the established configuration settings for the configuration items.  Determine whether deviations from established configuration settings are properly identified and appropriately addressed on a timely basis.  Note: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. IT products for which configuration settings can be defined include servers, workstations, operating systems, mobile devices, input and output devices, protocols, and applications.  Common secure configurations include the United States Government Configuration Baseline and security technical implementation guides. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method for uniquely identifying, tracking, and controlling configuration settings. | NIST SP 800-53, CM-06 |
| CM.02.03.02 The correct operation of security and privacy functions provided by systems or system components is periodically verified, and appropriate action is taken when anomalies are identified. | Obtain an understanding of the entity’s processes and methods for periodically verifying security and privacy functions, which relevant information systems provide, are operating correctly through   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for verifying security and privacy functions provided by information systems and information system components, as well as addressing any anomalies identified through security and privacy function verification.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  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.  Obtain an understanding of any automated tools the entity uses to facilitate security and privacy function verification. If automated tools are used, perform appropriate audit procedures to assess whether such tools are properly configured and appropriately employed to identify anomalies.  Determine whether the correct operation of security and privacy functions that systems or their components provide is periodically verified and appropriate action is taken when anomalies are identified. | NIST SP 800-53, SI-06 |
| CM.02.03.03 Management employs integrity verification tools to detect unauthorized changes to systems and system components.  *Related controls: BP.04.07.03 and BP.06.06.05* | Obtain an understanding of the entity’s processes and methods for detecting unauthorized changes to systems and system components through   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s integrity verification tools, and * inspection of relevant documentation, such as policies and procedures for using and managing the entity’s integrity verification tools, as well as implemented configuration settings, found in system configuration files for the tools employed.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for a selection of instances in which management reviewed the output of the entity’s integrity verification tools employed in connection with relevant information systems and their components. Consider whether appropriate personnel properly reviewed such output and took appropriate, timely action to address any unauthorized changes detected.  Inspect the implemented configuration settings for the integrity verification tools employed in connection with relevant information systems and their components. Consider whether the implemented configuration settings are appropriate for detecting unauthorized changes to systems and system components.  Determine whether management properly employs integrity verification tools to detect unauthorized changes to systems and their components.  Note: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications. | NIST SP 800-53, SI-07 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system design documentation, system security and privacy plans, and system-level configuration management plans.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to separate and control access to the development, test, integration, and production environments for relevant information systems. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk; * facilitate segregation of duties for program development and implementation, including the movement of programs between environments; and * reasonably assure that the development, test, integration, and production environments are sufficiently separated and appropriately controlled.   Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports that access control software produces to determine whether access to the development, test, integration, and production environments for relevant information systems is appropriately restricted to authorized personnel.  Determine whether the development, test, integration, and production environments for relevant information systems are sufficiently separated and appropriately controlled.  Note: Information system preproduction environments (i.e., development, test, and integration) are protected commensurate with risk throughout the system development life cycle for the information system, information system component, or system service. | NIST SP 800-53, SA-03  NIST SP 800-53, SC-32  NIST SP 800-53, SC-49  NIST SP 800-53, SC-50 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as system design documentation, system security and privacy plans, and system-level configuration management plans.   Inspect documentation demonstrating the design and implementation of the entity’s processes and methods to separate and control access to source code repositories and program libraries for relevant information systems. Consider whether such processes and methods   * are suitably designed and properly implemented based on risk and * reasonably assure that source code repositories and program libraries are sufficiently separated and appropriately controlled.   Inspect implemented access control parameters evidenced by applicable access control lists, system configuration files, and reports that access control software produces to determine whether access to source code repositories and program libraries for relevant information systems is appropriately restricted to authorized personnel.  Determine whether source code repositories and program libraries for relevant information systems are sufficiently separated and appropriately controlled.  Note: Source code is a set of computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator. Source code is written by a programmer in a programming language that humans can read and understand. Source code is ultimately translated into object code, which a computer can read. Programs, or computer programs, are complete sets of ordered instructions that a computer executes to perform a specific operation or task. | NIST SP 800-53, CM-05  NIST SP 800-53, SA-08  NIST SP 800-53, SA-10 |
| 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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s system development and configuration management tools and software, and * inspection of relevant documentation, such as policies and procedures for the entity’s system development and configuration management processes.   Inspect implemented access control parameters evidenced by applicable access control lists or system configuration files for the entity’s system development and configuration management tools.  Determine whether logical access to the tools and software that support the entity’s system development and configuration management processes is appropriately controlled. | NIST SP 800-53, CM-05  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.  *Related controls: SM.04.01.01, SM.04.01.02, SM.06.01.01, and AC.02.03.10* | Obtain an understanding of the entity-level and system-level processes and methods that the entity employs for conducting vulnerability monitoring and scanning for relevant information systems and their components through   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity and system-level processes. Consider whether the processes   * identify roles and responsibilities; * are integrated with the entity-level risk management strategy, as well as the entity-level and system-level continuous monitoring strategies, as applicable; * specify the processes and methods employed for vulnerability monitoring and scanning and for analyzing their results; * specify the processes and methods for sharing information obtained from the vulnerability monitoring and scanning processes with appropriate personnel to help eliminate similar control deficiencies and vulnerabilities in other information systems; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are adequate to facilitate the proper identification and timely remediation of control deficiencies and vulnerabilities.   Determine whether the entity-level and system-level processes for vulnerability monitoring and scanning for relevant information systems and their components are designed, implemented, and operating effectively.  Note: Entities establish required vulnerability monitoring and scanning processes for information system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, and sensors), networked printers, scanners, and copiers—are not overlooked.  Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include using continuous 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. | NIST SP 800-53, RA-05 |
| CM.03.01.02 Management employs appropriate tools and software to support the entity’s vulnerability monitoring and scanning processes.  *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   * inquiry of appropriate personnel, including IT management personnel responsible for the entity’s vulnerability monitoring and scanning tools and software, and * inspection of relevant documentation, such as policies and procedures for using and managing the entity’s vulnerability monitoring and scanning tools and software, as well as implemented configuration settings, found in system configuration files for the tools and software employed.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the implemented configuration settings for the vulnerability monitoring and scanning tools and software employed in connection with relevant information systems and their components. Consider whether the implemented configuration settings are appropriate.  Determine whether management properly employs appropriate tools and software to support the entity’s vulnerability monitoring and scanning processes applicable to relevant information systems.  Note: The capability to readily update vulnerability monitoring tools and software as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not overlooked. Properly maintaining and updating vulnerability monitoring tools and software also helps to ensure that potential vulnerabilities in information systems and information system components are identified and addressed as quickly as possible.  Vulnerability monitoring tools and software that facilitate interoperability include tools that are SCAP validated. Entities may employ scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures naming convention and that use the Open Vulnerability Assessment Language to determine the presence of vulnerabilities. Entities may also employ scanning tools that express vulnerability impact using the Common Vulnerability Scoring System. Sources for vulnerability information include the Common Weakness Enumeration listing and the National Vulnerability Database. | NIST SP 800-53, RA-05 |
| CM.03.02 Critical updates and patches for information systems are implemented, and unsupported information system components are replaced on a timely basis. | | |
| CM.03.02.01 Entity-level and system-level processes for flaw remediation, including patch management, are established and implemented.  *Related controls: 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   * inquiry of appropriate personnel, * inspection of relevant policies and procedures, and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity-level and system-level processes. Consider whether the processes   * identify roles and responsibilities; * are integrated with the entity-level risk management strategy, as well as the entity-level and system-level continuous monitoring strategies, as applicable; * 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; * specify the processes and methods employed for timely flaw remediation, including patch management; * have been recently reviewed and updated, as appropriate; * have been approved by the appropriate senior official(s); and * are adequate to facilitate the proper identification and timely remediation of control deficiencies and vulnerabilities.   Inspect a selection of vendor-recommended patches and compare 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.  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.  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.  By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. The time periods for flaw remediation may vary based on a variety of risk factors, including the security categorization of the information system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission or business functions that the information system supports, or the threat environment.  Some types of flaw remediation may require more testing than others. Entities determine the nature and extent of testing needed for the specific type of flaw remediation activity under consideration. In making this determination, entities consider the types of changes that are configuration controlled and subject to the entity-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. | NIST SP 800-53, SI-02 |
| 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   Inspect the inventory of information system components for relevant information systems, as well as listings of configuration items for such systems. Identify any information system components that have reached, or are approaching, end of life and are not, or will no longer be, supported by the developer, vendor, or manufacturer. Consider whether such components are scheduled for replacement or supported by other means through alternative sources.  Determine whether unsupported system components are replaced or alternative sources for continued support are identified and employed on a timely basis.  Note: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. | NIST SP 800-53, SA-22 |
| CM.03.03 Information systems and information system components are protected from spam and malicious code. | | |
| CM.03.03.01 Spam and malicious code protection mechanisms are selected and employed based on risk. | Obtain an understanding of any entity-level policies or procedures governing the selection of spam and malicious code protection mechanisms through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of spam and malicious code protection mechanisms selected for use in connection with relevant information systems and their components.  Determine whether the spam and malicious code protection mechanisms selected for use in connection with relevant information systems and their components are appropriate based on risk.  Note: Spam is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as image steganography. Spam and malicious code protection mechanisms are implemented at system entry and exit points, which include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. | NIST SP 800-53, SC-35  NIST SP 800-53, SI-03  NIST SP 800-53, SI-08 |
| CM.03.03.02 Management prevents the installation of software and firmware components lacking recognized and approved digital signature certificates.  *Related control: CM.01.02.03* | Obtain an understanding of any entity-level policies or procedures governing the use of signed information system components through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Consider whether the policies and procedures   * identify roles and responsibilities; * are incorporated into or referenced by the entity’s configuration management processes, including the entity-level and system-level processes for managing planned and emergency changes to information systems and information system components; * specify the processes and methods employed to validate that software and firmware components have been digitally signed using a certificate that the entity recognized and approved prior to installation; * have been recently reviewed and updated; * have been approved by the appropriate senior officials; and * are adequate to prevent unsigned software and firmware components from being installed.   Inspect a selection of software and firmware components for the relevant information systems. Consider whether such components are signed with an entity-approved certificate.  Determine whether management adequately prevents the installation of software and firmware components lacking recognized and approved digital signature certificates for relevant information systems.  Note: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input and output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures are methods of code authentication. | NIST SP 800-53, CM-14 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-24-107026

570 FISCAM Framework for Contingency Planning

1. 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.
2. 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.

1. 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 National Institute of Standards and Technology (NIST) Special Publication (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. | | |
| CP.01.01.01 Management performs criticality analyses for systems, system components, and system services. | Obtain an understanding of management’s process for conducting and documenting criticality analyses through   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the results of criticality analyses performed for the information systems, information system components, and information system services relevant to the significant business processes. Consider whether management’s assumptions based on its analyses are reasonable and whether such assumptions are appropriately documented. Additionally, consider whether criticality analyses are updated when significant changes are made to the corresponding systems, system components, or system services.  Determine whether the criticality analyses for the information systems, information system components, and information system services relevant to the significant business processes were properly performed and appropriately documented.  Note: Criticality analyses may also be performed for business process applications. Large or complex information systems supporting multiple mission and business functions may include multiple business process applications. System engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes identification of organizational missions a system supports; decomposition into the specific functions to perform those missions; and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.  For critical system components that cannot be trusted due to specific threats to and vulnerabilities in those components for which there are no viable security controls to adequately mitigate risk, reimplementation or custom development of such components may reduce potential attacks by adversaries. | NIST SP 800-53, RA-09  NIST SP 800-53, SA-20 |
| 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.  *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   * inquiry of appropriate personnel and * inspection of relevant documentation, such as policies and procedures for developing contingency plans.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect the contingency plans for each relevant information system, as applicable. Consider whether the plans   * identify critical or essential mission and business functions, as applicable, and associated contingency requirements, including how critical or essential mission and business functions will be maintained in the event of a system disruption, compromise, or failure; * are based on current information and reflect current conditions, including contingency roles, responsibilities, and assigned individuals with contact information; * have been recently reviewed and updated; * have been approved by the appropriate senior officials; * are integrated with the risk management and system development life cycle processes; * are appropriately aligned with other organizational plans, including the critical infrastructure and key resources protection plan, as well as business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, insider threat implementation plans, data breach response plans, cyber-incident response plans, breach response plans, and occupant emergency plans, as applicable; * address information system interdependencies; * include required information in accordance with authoritative criteria; * identify and allocate appropriate resources to support achieving continuity of operations and prioritize recovery and reconstitution procedures; * address the failure and timely recovery and reconstitution of the information system and system components to a known state; * adequately consider whether alternate processing and storage sites (both internal and external to the entity) can be relied on for continuity or operations without compromising security concerns; and * are adequate to address eventual, full-system restoration and implementation of alternative mission or business processes without deterioration of the controls originally planned and implemented.   Determine whether the contingency plans for relevant information systems have been appropriately documented, periodically reviewed and updated, and properly approved.  Note: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached.  Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design, as systems can be designed for redundancy, to provide backup capabilities, and for resilience. Additionally, for systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. | NIST SP 800-53, CP-02  NIST SP 800-53, CP-10  NIST SP 800-53, CP-12  NIST SP 800-53, SC-24 |
| CP.01.02.02 A critical infrastructure and key resources protection plan is developed, documented, disseminated, and periodically reviewed and updated. | Obtain an understanding of the entity’s processes and methods for developing, documenting, disseminating, and periodically reviewing and updating the critical infrastructure and key resources protection plan through   * inquiry of appropriate personnel and * inspection of relevant entity documentation.   Inspect the critical infrastructure and key resources protection plan. Consider whether the plan   * has been recently reviewed and updated, as appropriate; * has been approved by the appropriate senior official(s); * includes required information in accordance with authoritative criteria; * is consistent with applicable statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, and guidelines; * provides an overview of the entity’s protection strategies based on management’s prioritization of critical or essential mission and business functions and management’s determination of the criticality of information systems, information system components, and information system services; * considers the risks and potential impacts of a system disruption, compromise, or failure on the performance of critical or essential mission and business functions; and * addresses the relevant information systems.   Determine whether the crucial infrastructure and key resources protection plan has been appropriately developed, documented, disseminated, and periodically reviewed and updated.  Note: The development of contingency plans is coordinated with the critical infrastructure and key resources protection plan, as well as with other organizational plans, such as business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, insider threat implementation plans, data breach response plans, cyber-incident response plans, breach response plans, and occupant emergency plans. | NIST SP 800-53, PM-08 |
| CP.01.03 Information system users and other personnel are trained to fulfill their roles and responsibilities associated with the information system contingency plan in the event of a system disruption. | | |
| CP.01.03.01 Management establishes, documents, and periodically reviews and updates contingency training that incorporates lessons learned from contingency plan testing or actual system disruptions into contingency training techniques. Management monitors the completion status of applicable mandatory training courses for information system users. | Obtain an understanding of the entity’s processes and methods for establishing, documenting, and periodically reviewing and updating contingency training through   * inquiry of appropriate personnel, including any senior officials responsible for contingency training, and * inspection of relevant documentation.   Inspect documentation for contingency training for each relevant information system, as applicable. Consider whether   * training course materials are consistent with information system user roles and responsibilities and the content has been reviewed and updated when required because of system changes and at an appropriate frequency; * lessons learned from contingency plan testing or actual system disruptions are incorporated into course materials and training techniques; * mandatory training courses are identified and communicated to information system users as a condition for system access, as applicable; and * management monitors and maintains records of the completion status of applicable mandatory training courses for information system users.   Determine whether contingency training for relevant information systems is effectively designed, appropriately documented, and periodically reviewed and updated, and whether user attendance and completion are monitored.  Note: Actions addressed in contingency plans, and for which training may be required, include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack.  Additionally, fail-safe procedures may be required when certain failure conditions occur, and training on such procedures may be beneficial. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel. | NIST SP 800-53, CP-02  NIST SP 800-53, CP-03  NIST SP 800-53, SI-17 |
| 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   * inquiry of appropriate personnel, including users and authorizing officials; * inspection of relevant policies and procedures for contingency plan testing; and * inspection of other relevant documentation demonstrating the design and implementation of the processes.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect available documentation for any instances in which the contingency plans for relevant information systems were tested during the audit period. Consider whether such actions were appropriate and performed in accordance with the entity’s policies and procedures for contingency plan testing.  Determine whether the processes for periodically testing the contingency plans for relevant information systems are designed, implemented, and operating effectively to reasonably assure that contingency plans are effective, and the entity is ready to execute such plans.  Note: Methods for testing contingency plans to determine their effectiveness and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans. | NIST SP 800-53, CP-04 |
| CP.01.04.02 Contingency plan test results are documented, reviewed by management, and used to inform updates to the system-level contingency plans.  *Related control: CP.01.02.01* | Inspect contingency plan test results documented for the relevant information systems.  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  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   * inquiry of appropriate personnel; * inspection of relevant documentation; and * observation of the entity’s use of climate controls to maintain and monitor temperature, humidity, and other environmental factors.   Perform walk-throughs of the facilities where 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.  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.  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. | NIST SP 800-53, PE-14 |
| 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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the location of any master shutoff or isolation valves within the facilities.   Perform walk-throughs of the facilities where 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.  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.  Note: Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations. | NIST SP 800-53, PE-15 |
| CP.02.01.03 Emergency shutoff switches are accessible, functional, and known to appropriate personnel to provide the 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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the location of any emergency shutoff switches within the facilities.   Perform walk-throughs of the facilities where 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.  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   * inquiry of appropriate personnel, * inspection of relevant documentation, and * observation of the entity’s use of fire detection and suppression systems.   Perform walk-throughs of the facilities where relevant information systems reside. Identify the fire detection and suppression systems that the entity employs. Consider whether an independent power source supports the fire detection and suppression systems.  Determine whether management adequately maintains and monitors fire detection and suppression systems for the facilities where relevant information systems reside.  Note: Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility. | NIST SP 800-53, PE-13 |
| 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   * inquiry of appropriate personnel; * inspection of relevant documentation, including any necessary agreements permitting the timely transfer and resumption of processing for critical or essential mission and business functions, as well as the storage and retrieval of system backup information, if the primary processing or storage sites are unavailable; and * observations of alternate processing and storage sites.   Perform walk-throughs of the alternate processing and storage sites where 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 equivalent or commensurate to those at the primary processing and storage sites.  Determine whether sufficiently separated alternate processing and storage sites are maintained for the relevant information systems to provide and support processing capabilities when the primary processing or storage sites are unavailable.  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. | NIST SP 800-53, CP-06  NIST SP 800-53, CP-07  NIST SP 800-53, PE-17 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect relevant telecommunications services contracts and agreements. Consider whether such contracts and agreements include provisions addressing availability requirements, including priority of service. Consider whether any physical infrastructure is shared between the primary and alternate telecommunications service providers and, if so, how risks relevant to a single point of failure resulting from a natural disaster, structural failure, hostile attack, or errors would be mitigated.  Determine whether alternate telecommunication services are available for relevant information systems. | NIST SP 800-53, CP-08 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of any alternate security mechanisms that the entity employs for relevant information systems.  Determine whether alternate security mechanisms for critical security functions are available and appropriate for the relevant information systems.  Note: Given the cost and level of effort required to establish and maintain alternate security mechanisms, such mechanisms are generally only applied to critical security functions of information systems, information system components, or information system services. | NIST SP 800-53, CP-13  NIST SP 800-53, SI-13 |
| CP.02.02.04 In the event of a loss of the primary power source, emergency lighting is activated, and an uninterruptible power supply is available to provide temporary power while the alternate power source is started. | Obtain an understanding of the entity’s use of emergency lighting and an uninterruptible power supply in the event of a loss of the primary power source at the facilities where relevant information systems reside through   * inquiry of appropriate personnel and * inspection of relevant documentation.   Perform walk-throughs of the facilities where relevant information systems reside.  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.  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. | NIST SP 800-53, PE-11  NIST SP 800-53, PE-12 |
| 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Perform walk-throughs of the facilities where relevant information resources reside.  Inspect the results of any recent tests of the entity’s alternate power supply. Consider whether the alternate power supply provided sufficient power to support operations while the primary power source was unavailable.  Determine whether, in the event of a loss of the primary power source at the facilities where relevant information 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   * inquiry of appropriate personnel and * inspection of relevant documentation.   Inspect documentation demonstrating the design and implementation of any alternate communications protocols or alternate communications paths that the entity employs for the relevant information systems.  Determine whether alternate communications mechanisms are available and appropriate for relevant information systems.  Note: Switching communications protocols may affect application software and operational aspects of systems. It is important for entities to assess the potential side effects of introducing alternate communications protocols prior to implementation. An incident, whether adversarial or nonadversarial, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. | NIST SP 800-53, CP-11  NIST SP 800-53, SC-47 |
| CP.02.03 System backups are regularly conducted, and system media containing backup data and software are properly maintained to facilitate the recovery and reconstitution of information systems following a system disruption. | | |
| CP.02.03.01 System backups of data and software are conducted regularly consistent with risk. | Obtain an understanding of the entity’s processes for conducting system backups through   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of system-level contingency plans for each relevant information system, as applicable.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes for conducting system backups for relevant information systems. Consider whether   * the frequency at which system backups are conducted is adequate, * access to system backups is appropriately controlled, and * the retention periods for system backups are aligned with entity-level policies.   See also AC.03.02.01 and AC.03.02.02.  Inspect the results of any recent tests of the entity’s system backups. Consider whether the confidentiality, integrity, and availability of system backups are adequately protected through reperformance of the entity’s test procedures or independent analysis.  Determine whether system backups of data and software for relevant information systems are properly conducted regularly consistent with risk. | NIST SP 800-53, CP-09 |
| 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   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of system-level contingency plans for each relevant information system, as applicable.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes for transferring and maintaining system media containing backup data and software for relevant information systems. Consider whether   * the locations of the alternate processing or storage sites are appropriate to minimize disruption and * the methods used to transport, receive, and replace system backups permit them to be tracked throughout the process.   See also AC.03.01.03, AC.03.01.04, and AC.03.01.05.  Inspect the results of any recent tests of the entity’s system backups. Consider whether the confidentiality, integrity, and availability of system backups are adequately protected through reperformance of the entity’s test procedures or independent analysis. Consider whether such backups of software reflect the most recent version in use and are protected from modification.  Determine whether system media containing backup data and software are properly maintained at alternate processing or storage sites. | NIST SP 800-53, CP-06 |
| 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   * inquiry of appropriate personnel; * inspection of relevant policies and procedures; and * inspection of maintenance contracts or service agreements with external parties, as applicable.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes for approving, controlling, and monitoring the use of system maintenance tools.  Inspect documentation demonstrating the design and implementation of the entity’s processes for obtaining maintenance support, as well as any spare parts or replacement hardware needed to perform system component maintenance on a timely basis. Consider whether   * the entity has established a process for authorizing access for external personnel engaged to perform system component maintenance, * maintenance contracts or service agreements include provisions to define timeliness and specify requirements for completing timely maintenance, * requirements for the performance of system component maintenance in accordance with vendor specifications are included in the entity’s policies and procedures, and * the entity maintains an inventory of spare parts or replacement hardware for system components that support critical or essential mission and business functions.   Inspect available documentation for a selection of system components to assess whether maintenance has been performed for such components in accordance with vendor specifications.  Determine whether management maintains appropriate tools and resources for performing system component maintenance for relevant information systems on a timely basis. | NIST SP 800-53, MA-03  NIST SP 800-53, MA-05  NIST SP 800-53, MA-06 |
| 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes for scheduling and performing system component maintenance for relevant information systems. Consider whether   * flexibility exists in operations, including processing for critical or essential mission and business functions, to accommodate regularly scheduled maintenance and a reasonable amount of unscheduled maintenance; * management has established goals for the availability of services and processing capabilities; * advance notice of regularly scheduled maintenance and timely communication of unscheduled maintenance is provided to system users, as well as others affected by or involved in such maintenance, to minimize the impact on operations; and * performance measures and compliance metrics are periodically evaluated and appropriately employed to measure the effectiveness or efficiency of system component maintenance.   Determine whether management schedules and performs system component maintenance in a manner that minimizes service outages and disruption of operations. | NIST SP 800-53, MA-06 |
| 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   * inquiry of appropriate personnel and * inspection of relevant policies and procedures.   See SM.05.01.01 for factors to consider in assessing the adequacy of policies and procedures.  Inspect documentation demonstrating the design and implementation of the entity’s processes for controlling system component maintenance for relevant information systems. Consider whether   * management reviews and approves maintenance activities, regardless of whether such activities are performed locally or remotely; * the removal of a system component from an entity facility for maintenance, repair, or replacement requires explicit approval from management; * affected, or potentially affected controls, are tested to determine whether such controls operate as intended following system component maintenance; * records, which provide evidence for all maintenance actions and approvals, are properly prepared and maintained; * the entity has implemented processes for approving, controlling, and monitoring the use of system maintenance tools and for periodically reviewing previously approved system maintenance tools for continuing appropriateness; * strong authentication methods and appropriate session-level controls are employed in connection with remote maintenance and diagnostic activities; * field maintenance is appropriately controlled; * entity personnel with adequate technical competence supervise or oversee the performance of maintenance activities; and * maintenance activities are appropriately logged and adequately monitored.   Determine whether management performs system component maintenance for relevant information systems in a controlled manner. | NIST SP 800-53, MA-02  NIST SP 800-53, MA-04  NIST SP 800-53, MA-05  NIST SP 800-53, MA-07 |

Source: GAO (analysis) and National Institute of Standards and Technology Special Publication 800-53 (security and privacy controls). | GAO-24-107026

1. GAO, *Government Auditing Standards: 2018 Revision Technical Update April 2021*, [GAO-21-368G](https://www.gao.gov/products/gao-21-368g) (Washington, D.C.: April 2021). [↑](#footnote-ref-1)
2. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](https://www.gao.gov/products/GAO-14-704G) (Washington, D.C.: September 2014). [↑](#footnote-ref-2)
3. 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-3)
4. 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. [↑](#footnote-ref-4)