Appendix 600C FISCAM Security Management Questionnaire

Purpose

The *Federal Information System Controls Audit Manual* (FISCAM) security management questionnaire includes the questions relevant to the information system (IS) controls included in the FISCAM Framework for Security Management. The FISCAM security management questionnaire is intended to assist auditors with obtaining and documenting an understanding of the entity’s information security management program. It does not include all procedures necessary to achieve the engagement objectives overall.

Instructions

The FISCAM security management questionnaire contains detailed questions that are organized by critical elements. A response to each question is noted by either “Yes,” “No,” or “N/A” (not applicable) in the “Response” column.” For each “No” response, a response to whether any compensating controls have been identified is noted in the “If no, have compensating controls been identified?” column. If compensating controls have been identified, a description of such controls is provided in the "Comment” column. If compensating controls are not identified, an explanation as to the potential effect on areas of audit interest is provided in the "Comment” column.

Questionnaire

| Question | Response  (yes, no, or N/A) | If no, have compensating controls been identified?  (yes, no, or N/A) | Reference to supporting documentation | Comment |
| --- | --- | --- | --- | --- |
| Information security management program structure (SM.01.01) | | | | |
| 1. Does the organizational structure supporting the entity’s information security management program have adequate independence, authority, expertise, and resources to achieve the entity’s information security objectives? |  |  |  |  |
| 1. Does the organizational structure supporting the entity’s privacy management program have adequate independence, authority, expertise, and resources to achieve the entity’s privacy objectives? |  |  |  |  |
| 1. Does the organizational structure supporting the entity’s supply chain risk management activities have adequate independence, authority, expertise, and resources? |  |  |  |  |
| Assignment of responsibilities for senior management (SM.01.02) | | | | |
| 1. Has an information security officer been appointed and given the appropriate authority and resources to coordinate, develop, implement, and maintain the entity’s information security management program? |  |  |  |  |
| 1. Has a senior management official been assigned as the authorizing official for each relevant information system and for the common controls that such systems inherit? |  |  |  |  |
| 1. Have information security responsibilities been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators, who possess the appropriate skills and technical expertise to satisfy their assigned responsibilities? |  |  |  |  |
| 1. Has a privacy officer been appointed and given the authority and resources to coordinate, develop, implement, and maintain the entity’s privacy management program? |  |  |  |  |
| 1. Have privacy responsibilities been clearly defined and appropriately assigned to senior management, information resource owners and users, IT management personnel, and security administrators, who possess the appropriate skills and technical expertise to satisfy their assigned responsibilities? |  |  |  |  |
| 1. Has a chief risk officer been appointed and given the appropriate authority and resources to align information security and privacy management processes with strategic, operational, budgetary planning, and risk management processes? |  |  |  |  |
| Information security management planning documentation (SM.01.03) | | | | |
| 1. Has an entity-level information security management program plan been effectively designed and appropriately documented and periodically reviewed and updated? When determining if the plan has been effectively designed, consider if the plan includes  * 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. |  |  |  |  |
| 1. Has an entity-level information privacy management program plan been effectively designed and appropriately documented and periodically reviewed and updated? When determining if the plan has been effectively designed, consider if the plan includes  * 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. |  |  |  |  |
| System development life cycle (SM.01.04) | | | | |
| 1. Have system development life cycle processes been appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| 1. Has an enterprise architecture that addresses security and privacy considerations been appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| Incident response program (SM.01.05) | | | | |
| 1. Has an entity-level incident response plan been effectively designed, appropriately documented, periodically reviewed and updated, and properly approved? When determining if the plan has been effectively designed, consider if the plan  * 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. |  |  |  |  |
| 1. Has an incident response program been effectively designed and properly implemented in accordance with the entity-level incident response plan? When determining if the program has been effectively designed, consider if the program includes  * 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. |  |  |  |  |
| System-level and Entity-level processes (SM.01.06) | | | | |
| 1. Has the entity-level inventory of major information systems (i.e., all major applications and general support systems) been appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| 1. Is the entity-level process for selecting and implementing security controls effectively designed and implemented? When determining if the process has been effectively designed, consider if minimum security requirements for information and information systems are satisfied. |  |  |  |  |
| 1. Has the system-level concept of operations document for each relevant information system been appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| 1. Has the system-level security and privacy architecture for each relevant information system been appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| 1. Have the system security and privacy plans for each relevant information system included in the systems inventory been effectively designed, appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| 1. Has the system-level supply chain risk management plan for each relevant information system been effectively designed, appropriately documented, and periodically reviewed and updated? |  |  |  |  |
| Information security and privacy workforce and roles (SM.02.01) | | | | |
| 1. Has a security and privacy workforce development and improvement program been established and documented? |  |  |  |  |
| 1. Are information security and privacy roles, responsibilities, and position risk designation accurately identified and included in position descriptions? |  |  |  |  |
| 1. Are incompatible duties accurately identified and included in position descriptions? |  |  |  |  |
| Screening activities (SM.02.02) | | | | |
| 1. Are references for prospective employees properly contacted and background investigations and agency checks properly performed based on position risk designations? |  |  |  |  |
| 1. Are rescreening activities, including periodic reinvestigations, performed based on position risk designations as required by applicable statutes, regulations, executive orders, implementing entity guidance, directives, and other specific criteria? |  |  |  |  |
| 1. Does the entity obtain signed access agreements prior to granting access to information and information systems? |  |  |  |  |
| Information security and privacy training and awareness program (SM.02.03) | | | | |
| 1. Has an information security and privacy literacy training and awareness program been effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses? |  |  |  |  |
| 1. Has a role-based information security and privacy training program been effectively designed, appropriately documented, periodically reviewed and updated, and properly monitored for user completion of mandatory training courses? |  |  |  |  |
| 1. Have current rules that describe the responsibilities and expected behavior for information and information system usage, security, and privacy been acknowledged in writing by individuals prior to their being granted access to information and information systems? |  |  |  |  |
| Training activities (SM.02.04) | | | | |
| 1. Have employee training records been appropriately documented, monitored, and retained? |  |  |  |  |
| 1. Have the results of employee training been evaluated by appropriate personnel, and have appropriate actions been taken? |  |  |  |  |
| Transfer and termination activities (SM.02.05) | | | | |
| 1. Have transfer and termination activities been appropriately completed on a timely basis? Consider the following transfer and termination activities:  * 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. * Identify the period during which nondisclosure requirements remain in effect for terminated employees. |  |  |  |  |
| Noncompliance with security and privacy policies and procedures (SM.03.01) | | | | |
| 1. Have the entity’s formal sanctions process and methods for individuals failing to comply with information security and privacy policies and procedures been appropriately employed? |  |  |  |  |
| External-party accountability (SM.03.02) | | | | |
| 1. Have the terms and conditions for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems been appropriately documented, periodically reviewed and updated, and properly approved? |  |  |  |  |
| 1. Has the entity-level process for assessing the effectiveness of information security and privacy controls that external parties design, implement, or operate effectively been designed and implemented to achieve the entity’s information security and privacy objectives and hold external parties accountable for their assigned internal control responsibilities? |  |  |  |  |
| 1. Has the interorganizational joint authorization process for systems with multiple authorizing officials and at least one authorizing official from an external party been effectively designed and implemented to achieve the entity’s information security and privacy objectives and hold external parties accountable for their assigned internal control responsibilities? |  |  |  |  |
| Complementary user-entity controls (SM.03.03) | | | | |
| 1. Have complementary user-entity controls related to external parties been identified and implemented and are they operating effectively? |  |  |  |  |
| Risk management strategies (SM.04.01) | | | | |
| 1. Has the entity-level risk management strategy for information security and privacy risks been effectively designed, appropriately documented, and periodically reviewed and updated? When determining if the process has been effectively designed, consider if the strategy includes determination of assumptions and constraints affecting entity risk assessments, organizational risk tolerance, and entity-level priorities to guide and inform risk-based decisions. |  |  |  |  |
| 1. Has the entity-level continuous monitoring strategy been effectively designed, appropriately documented, and periodically reviewed and updated? When determining if the process has been effectively designed, consider if the strategy establishes the metrics, frequency, and type(s) of control assessments and monitoring, as well as the process for correlating, analyzing, and responding to control assessment and monitoring results. |  |  |  |  |
| 1. Has the entity-level supply chain risk management strategy been effectively designed, appropriately documented, and periodically reviewed and updated? When determining if the process has been effectively designed, consider if the strategy manages risks associated with developing, acquiring, maintaining, and disposing of systems, system components, and system services. |  |  |  |  |
| Risk identification, analysis, and response activities (SM.04.02) | | | | |
| 1. Does the security categorization for each relevant information system flow logically from the supporting rationale documented and approved within the respective system security and privacy plan? |  |  |  |  |
| 1. Have risk assessments for relevant information systems been conducted and documented in accordance with effectively designed and implemented processes and methods for conducting and documenting such assessments? |  |  |  |  |
| 1. Have vulnerability scan reports and results from vulnerability monitoring, including results of penetration testing, been appropriately considered as part of the risk assessments conducted and documented for relevant information systems? |  |  |  |  |
| 1. Have risk assessment results for relevant information systems been documented, analyzed, and approved by management in accordance with effectively designed and implemented processes and methods for analyzing and responding to risks? |  |  |  |  |
| 1. Are risks reassessed periodically, at an appropriate frequency, to address changes to relevant information systems, the systems’ environments of operation, or other conditions that may affect the security or privacy state of the systems? |  |  |  |  |
| 1. Have findings from risk assessments, security assessments, privacy assessments, monitoring activities, and audits been addressed within appropriate time frames in accordance with organizational risk tolerance? |  |  |  |  |
| Information security and privacy policies and procedures (SM.05.01) | | | | |
| 1. Does management appropriately develop, document, periodically review and update, and properly approve information security and privacy policies and procedures implemented at the entity and system levels? |  |  |  |  |
| System authorization (SM.05.02) | | | | |
| 1. Have common controls been authorized for inheritance before commencing operations and reauthorized on a periodic basis thereafter? |  |  |  |  |
| 1. Has the authorizing official(s) appropriately (1) authorized each relevant information system to operate before commencing operations, (2) authorized the use of inherited common controls, and (3) reauthorized relevant information systems to operate and use inherited common controls periodically? |  |  |  |  |
| 1. Does the authorization package for each relevant information system include the authorization to operate, executive summary, system security and privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones? |  |  |  |  |
| Monitoring activities (SM.06.01) | | | | |
| 1. Has the system-level continuous monitoring strategy for each relevant information system been effectively designed, appropriately documented, and periodically reviewed and updated? |  |  |  |  |
| 1. Have system-level control monitoring activities been implemented in accordance with the system-level continuous monitoring strategy to assess controls and identify risks at a frequency sufficient to support risk-based decisions? |  |  |  |  |
| 1. Have assessors, with appropriate skills and technical expertise, properly performed security and privacy control assessments for each relevant information system on a periodic basis? |  |  |  |  |
| 1. Are control assessment reports shared with appropriate personnel and documented in sufficient detail to enable such personnel to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements? |  |  |  |  |
| 1. Are performance measures and compliance metrics periodically evaluated and appropriately employed to measure the effectiveness or efficiency of information security and privacy functions? |  |  |  |  |
| Remediation of control deficiencies and vulnerabilities (SM.07.01) | | | | |
| 1. Are plans of action and milestones for relevant information systems appropriately documented and periodically reviewed and updated? |  |  |  |  |
| 1. Are control deficiencies and vulnerabilities adequately analyzed in relation to the entire entity and are appropriate corrective actions applied entity-wide? |  |  |  |  |
| 1. Are remediation tasks and milestones accomplished by scheduled completion dates? |  |  |  |  |