

FISCAM OBJECTIVES

As noted on Page 6 of the Federal Information System Controls Audit Manual (FISCAM), the purpose of the manual is to provide guidance for performing effective and efficient Information System (IS) controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified IS control weaknesses; and inform financial, performance, and attestation auditors about IS controls and related audit issues, so that they can (1) plan their work in accordance with Generally Accepted Government Auditing Standards (GAGAS) and (2) integrate the work of IS controls specialists with other aspects of the financial or performance audit or attestation engagement.

When determining if a FISCAM review is necessary, reporting entities and service providers must assess the significance and materiality of each system. The reporting entity must identify all key systems and feeder systems that affect the assessable unit being asserted as audit ready. These key systems need to be evaluated and IT controls need to be identified and tested if the reporting entity is relying on:

- Controls within the system are identified as key controls in the controls assessment,
- Systems are used to generate or store original key supporting documentation, or
- Reports from a system are utilized in the execution of key controls.

Consistent with the approach followed when identifying Key Control Objectives (KCOs) to be included in the FIAR Guidance, OUSD(C) has identified the FISCAM Control Activities and Techniques needed to address the key internal controls over financial reporting (ICOFR) risk areas most likely to be present based on the Department's experience.

Reporting Entities must apply judgment in determining if additional IT Control Activities and Techniques should be included given their specific business processes and financial statements. Reporting Entities should also recognize that other FISCAM Control Activities and Techniques may address important compliance requirements and should be addressed as part of those programs.

Below is a summary analysis of those FISCAM Control Activities and Techniques that have the highest relevance to addressing key risk areas for financial reporting and other FISCAM Control Activities and Techniques that should be considered by the Reporting Entity in their audit readiness efforts.

FISCAM Control Techniques		Control Techniques with the <u>Highest</u> Relevance in a Financial Statement Audit	Other Control Techniques for Consideration in a Financial Statement Audit
IT General Controls	261	122	139
	100%	46.7%	53.3%
Process/Application Controls	163	144	19
	100%	88.3%	11.7%

TOTAL	424	266	158
	100%	62.7%	37.3%

Detailed information is contained in subsequent sections of this file as follows:

- IT Control Objectives - Section A
- FISCAM Control Activities and Techniques that have the highest relevance to addressing key risk areas for financial reporting - Sections B.1 and C.1
- Other FISCAM Control Activities and Techniques that should be considered by the Reporting Entity in their audit readiness efforts - Sections B.2 and C.2

A. IT CONTROL OBJECTIVES

IT General Control Objectives	
Security Management	<p>Controls provide reasonable assurance that security management is effective, including effective:</p> <ul style="list-style-type: none"> • security management program, • periodic assessments and validation of risk, • security control policies and procedures, • security awareness training and other security-related personnel issues, • periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, • remediation of information security weaknesses, and • security over activities performed by external third parties.
Access Controls	<p>Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective:</p> <ul style="list-style-type: none"> • protection of information system boundaries, • identification and authentication mechanisms, • authorization controls, • protection of sensitive system resources, • audit and monitoring capability, including incident handling, and • physical security controls.
Configuration Management	<p>Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective:</p> <ul style="list-style-type: none"> • configuration management policies, plans, and procedures, • current configuration identification information, • proper authorization, testing, approval, and tracking of all configuration changes, • routine monitoring of the configuration, • updating software on a timely basis to protect against known vulnerabilities, and • documentation and approval of emergency changes to the configuration.
Segregation of Duties	<p>Controls provide reasonable assurance that incompatible duties are effectively segregated, including effective:</p> <ul style="list-style-type: none"> • segregation of incompatible duties and responsibilities and related policies, and • control of personnel activities through formal operating procedures, supervision, and review.
Contingency Planning	<p>Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective:</p> <ul style="list-style-type: none"> • assessment of the criticality and sensitivity of computerized operations and identification of supporting resources, • steps taken to prevent and minimize potential damage and interruption, • comprehensive contingency plan, and • periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

IT Application Control Objectives	
Completeness	
	Controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.
Accuracy	
	Controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.
Validity	
	Controls provide reasonable assurance that (1) all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management's authorization; and (2) output contains only valid data.
Confidentiality	
	Controls provide reasonable assurance that application data and reports and other output are protected against unauthorized access.
Availability	
	Controls provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed.

B.1 GENERAL CONTROLS – RELEVANT TO AUDIT READINESS

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-1: Establish a Security Management Program	SM-1.1.1	The security management program is adequately documented, approved, and up-to-date.	<p>An agency/entity wide security management program has been developed, documented, and implemented that:</p> <ul style="list-style-type: none"> • covers all major facilities and operations, • has been approved by senior management and key affected parties, and • covers the key elements of a security management program: <ul style="list-style-type: none"> ○ periodic risk assessments, ○ adequate policies and procedures, ○ appropriate subordinate information security plans, ○ security awareness training, ○ management testing and evaluation, ○ a remedial action process, ○ security-incident procedures, and ○ continuity of operations. 	<p>Review documentation supporting the agency/entitywide security management program and discuss with key information security management and staff.</p> <p>Determine whether the program:</p> <ul style="list-style-type: none"> • adequately covers the key elements of a security management program, • is adequately documented, and • is properly approved. <p>Determine whether all key elements of the program are implemented. Consider audit evidence obtained during the course of the audit.</p>
Critical Element SM-1: Establish a Security Management Program	SM-1.1.2	The security management program is adequately documented, approved, and up-to-date.	The agency/entity-wide security management program is updated to reflect current conditions.	Based on a review of security management program documentation and interviews with key information security management and staff, determine whether the entity has adequate policies and procedures to identify significant changes in its IT environment that would necessitate an update to the program, and whether the program is periodically updated to reflect any changes.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-1: Establish a Security Management Program	SM-1.4.1	Subordinate security plans are documented, approved, and kept up-to-date.	<p>System and application security plans have been documented and implemented that:</p> <ul style="list-style-type: none"> • cover all major facilities and operations, • have been approved by key affected parties, • cover appropriate topics (for federal agencies, those prescribed by OMB Circular A-130; see table 4). 	<p>Review agency/entity policies and procedures for preparing security plans.</p> <p>Review the system and application security plans encompassing key areas of audit interest and critical control points.</p> <p>Determine whether the plans adequately cover appropriate topics (for federal agencies, refer to NIST SP 800-18 for guidance on security plans) and are properly approved.</p> <p>When conducting the audit, determine whether the plans have been implemented and accurately reflect the conditions noted.</p> <p>Determine whether security plans collectively cover all major facilities and operations.</p>
Critical Element SM-1: Establish a Security Management Program	SM-1.4.2	Subordinate security plans are documented, approved, and kept up-to-date.	The subordinate security plans are updated annually or whenever there are significant changes the agency/entity policies, organization, IT systems, facilities, applications, weaknesses identified, or other conditions that may affect security.	Review relevant security plans and any related documentation indicating whether they have been reviewed and updated and are current.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-1: Establish a Security Management Program	SM-1.5	An inventory of systems is developed, documented, and kept up-to-date.	A complete, accurate, and up-to-date inventory exists for all major systems that includes the identification of all system interfaces.	<p>Obtain the agency's/entity's systems inventory.</p> <p>Discuss with agency/entity management (1) the methodology and criteria for including or excluding systems from the inventory and (2) procedures and controls for ensuring the completeness, accuracy, and currency of the inventory.</p> <p>Determine whether systems tested during the audit are included in the inventory.</p> <p>Test the inventory for completeness, accuracy, and currency. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's process and controls for ensuring the accuracy of the inventory. Also, in the absence of effective controls over the inventory, the auditor would need to perform additional procedures to reasonably assure that all systems relevant to the audit have been identified.</p>
Critical Element SM-2: Periodically assess and validate risks	SM-2.1.1	Risk assessments and supporting activities are systematically conducted.	Appropriate risk assessment policies and procedures are documented and based on security categorizations.	Review risk assessment policies, procedures, and guidance.
Critical Element SM-2: Periodically assess and validate risks	SM-2.1.2	Risk assessments and supporting activities are systematically conducted.	Information systems are categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals.	Determine if security risk categorizations are documented, reasonable, and, for federal entities, if they comply with NIST FIPS Pub 199 and SP 800-60 .

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-2: Periodically assess and validate risks	SM-2.1.3	Risk assessments and supporting activities are systematically conducted.	Risks are reassessed for the entity-wide, system, and application levels on a periodic basis or whenever systems, applications, facilities, or other conditions change.	Obtain the most recent risk assessments encompassing key areas of audit interest and critical control points. Determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by sufficient testing (e.g., determine whether system vulnerabilities were identified using such techniques as automated scanning tools, security test evaluations or penetration tests). See NIST SP 800-30 for details. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management’s risk assessment process (including related controls), reading the risk assessments for the key systems relevant to the audit objectives, and determining whether risks identified by the IS controls audit are properly considered in the risk assessments.
Critical Element SM-2: Periodically assess and validate risks	SM-2.1.4	Risk assessments and supporting activities are systematically conducted.	Risk assessments and validations, and related management approvals are documented and maintained on file. Such documentation includes security plans, risk assessments, security test and evaluation results, and appropriate management approvals.	For a selection of risk assessments assess the completeness and adequacy of the required documentation.
Critical Element SM-2: Periodically assess and validate risks	SM-2.1.5	Risk assessments and supporting activities are systematically conducted.	Changes to systems, facilities, or other conditions and identified security vulnerabilities are analyzed to determine their impact on risk and the risk assessment is performed or revised as necessary based on OMB criteria.	Review criteria used for revising risk assessments. For recent changes that meet the criteria, determine if the risk assessment was redone or updated.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-3: Document and implement security control policies and procedures	SM-3.1	Security control policies and procedures are documented, approved by management and implemented.	Security control policies and procedures at all levels: <ul style="list-style-type: none"> • are documented, • appropriately consider risk, • address purpose, scope, roles, responsibilities, and compliance, • ensure that users can be held accountable for their actions, • appropriately consider general and application controls, • are approved by management, and • are periodically reviewed and updated. 	Review security policies and procedures and compare their content to NIST guidance (e.g., SP 800-30, SP 800-37, SP 800-100) and other applicable criteria (e.g., configuration standards).
Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.1.1	Owners, system administrators, and users are aware of security policies.	An ongoing security awareness program has been implemented that includes security briefings and training that is monitored for all employees with system access and security responsibilities. Coordinate with the assessment of the training program in SM-4.3.	Review documentation supporting evaluating the awareness program. Observe a security briefing. Interview data owners, system administrators, and system users. Determine what training they have and if they are aware of their security related responsibilities. Determine whether adequate procedures are implemented to monitor that all employees and contractors are receiving security awareness training.
Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.2.5	Hiring, transfer, termination, and performance policies address security.	A formal sanctions process is employed for personnel failing to comply with security policy and procedures.	Review the sanctions process. Determine how compliance with security policies is monitored and how sanctions were administered.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.2.6	Hiring, transfer, termination, and performance policies address security.	Where appropriate, termination and transfer procedures include: <ul style="list-style-type: none"> • exit interview procedures, • return of property, keys, identification cards, passes, etc., • notification to security management of terminations and prompt revocation of IDs and passwords, • immediate escort of terminated employees out of the entity’s facilities; and • identification of the period during which nondisclosure requirements remain in effect. 	Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine whether IDs and passwords for terminated employees still exist.
Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.3.2	Employees have adequate training and expertise.	Employee training and professional development are documented and monitored.	Review training records and related development are documented and monitored. documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.1	The effectiveness of security controls are periodically assessed.	Appropriate monitoring and testing policies and procedures are documented.	Review testing policies and procedures. Determine if there is an overall testing strategy or plan.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.2	The effectiveness of security controls are periodically assessed.	Management routinely conducts vulnerability assessments and promptly corrects identified control weaknesses.	<p>Interview officials who conducted the most recent agency/entity vulnerability assessment. Review the methodology and tools used, test plans and results obtained, and corrective action taken.</p> <p>Determine if testing is performed that complies with OMB and NIST certification and accreditation and other testing requirements.</p> <p>If appropriate, perform independent testing with the approval of management.</p> <p>Determine if identified control weaknesses are promptly corrected.</p>
Critical Element SM-6: Effectively Remediate Information Security Weaknesses	SM-6.1.1	Information security weaknesses are effectively remediated.	Management initiates prompt action to correct deficiencies. Action plans and milestones are documented.	<p>Review recent POA&Ms, FMFIA reports and prior year audit reports and determine the status of corrective actions. The objective of this procedure in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management’s POAM process and related controls to ensure the accuracy of the information in the POA&Ms, determining whether IS control weaknesses identified by the IS controls audit are included in the POA&Ms, and, if not, determining the cause. See OMB A-11 which recommends that audit remediation items be addressed within 6 months.</p>
Critical Element SM-6: Effectively Remediate Information Security Weaknesses	SM-6.1.3	Information security weaknesses are effectively remediated.	Corrective actions are tested and are monitored after they have been implemented and monitored on a continuing basis.	<p>Review a selection of corrective action plans to determine whether testing was performed and monitoring was conducted after implementation of corrective actions.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SM-7: Ensure that Activities Performed by External Third Parties are Adequately Secure	SM-7.1.1	External third party activities are secure, documented, and monitored.	<p>Appropriate policies and procedures concerning activities of external third parties (for example, service bureaus, contractors, other service providers such as system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include provisions for:</p> <ul style="list-style-type: none"> • clearances, • background checks, • required expertise, • confidentiality agreements, • security roles and responsibilities, • connectivity agreements, • expectations, • remedies, • audit access/audit reporting, • monitoring, • termination procedures, • security awareness training, • requirements definition, • security responsibilities, and • performance metrics. 	<p>Review policies and procedures pertaining to external third parties for the entity-wide, system, and application levels.</p> <p>Identify use of external third parties and review activities including compliance with applicable policies and procedures. See NIST SP 800-35 for guidance on IT security services.</p> <p>Determine how security risks are assessed and managed for systems operated by a third party.</p> <p>Assess the adequacy of controls over monitoring external third party services.</p> <p>Coordinate assessment of security awareness training with SM-4.</p> <p>Review any available SAS 70 and/or SSAE 16 reports to determine the nature, timing, and extent of tests of operating effectiveness and assess whether results provide sufficient information to obtain an understanding of the service organization's controls that would affect the entity's controls being assessed.</p>
Critical Element AC-1: Adequately protect information system boundaries	AC-1.1.1	Appropriately control connectivity to system resources.	Connectivity, including access paths and control technologies between systems and to internal system resources, is documented, approved by appropriate entity management, and consistent with risk.	Review access paths in network schematics, interface agreements, systems documentation, and in consultation with IT management and security personnel identify control points; determine whether the access paths and related system documentation is up-to-date, properly approved by management, and consistent with risk assessments.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
<p>Critical Element AC-1: Adequately protect information system boundaries</p>	<p>AC-1.1.2</p>	<p>Appropriately control connectivity to system resources.</p>	<p>Networks are appropriately configured to adequately protect access paths within and between systems, using appropriate technological controls (e.g., routers, firewalls, etc.)</p>	<p>Interview the network administrator; determine how the flow of information is controlled and how access paths are protected. Identify key devices, configuration settings, and how they work together. (This step is performed as a basis for the steps below).</p> <p>Perform security testing by attempting to access and browse computer resources including critical files, security software, and the operating system. These tests may be performed as (1) an “outsider” with no information about the entity’s computer systems, (2) an “outsider” with prior knowledge about the systems—for example, an ex-insider, and (3) an “insider” with and without specific information about the entity’s computer systems and with access to the entity’s facilities. Note: Due to the highly technical nature of such testing, it should be performed by persons possessing the necessary technical skills (e.g., an IT specialist). See Appendix V for additional information on the Knowledge, Skills, and Abilities needed to perform IS control audits. Also, see SM-5 for additional information on performing vulnerability assessments.</p> <p>When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity’s computer resources using default/generic IDs with easily guessed passwords. See NIST SP 800-42 for more details.</p> <p>When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, wireless, local area network, wide area network, and the Internet. See NIST SP 800-42 for more details.</p>

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-1: Adequately protect information system boundaries	AC-1.1.3	Appropriately control connectivity to system resources.	The information system identifies and authenticates specific network devices before establishing a connection.	Determine whether authentication methods used are appropriate based on risk in accordance with FIPS Pub 200 and NIST SP 800-53 .
Critical Element AC-1: Adequately protect information system boundaries	AC-1.1.7	Appropriately control connectivity to system resources.	Connectivity is approved only when appropriate to perform assigned official duties. This includes portable and mobile devices, and personally-owned information systems. Appropriate safeguards are established to detect viruses, provide for timely patch management, and other security measures are in place to validate appropriate access for users working remotely (e.g., home).	Interview network administrator and users; review justifications for a selection of connections. Determine if these systems use appropriate safeguards such as automatic updates for virus protection and up-to-date patch protection, etc.
Critical Element AC-1: Adequately protect information system boundaries	AC-1.2.1	Appropriately control network sessions.	The information system prevents further access to the system by initiating a session lock, after a specified period of inactivity that remains in effect until the user reestablishes access using identification and authentication procedures.	Observe whether the system automatically initiates a session lock during a period of inactivity, and how the user can directly initiate a session lock, and then unlock the session (See OMB M-06-16).
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC-2.1.1	Users are appropriately identified and authenticated.	Identification and authentication is unique to each user (or processes acting on behalf of users), except in specially approved instances (for example, public Web sites or other publicly available information systems).	Review pertinent policies and procedures and NIST guidance pertaining to the authentication of user identities; interview users; review security software authentication parameters.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.3	Users are appropriately identified and authenticated.	Effective procedures are implemented to determine compliance with identification and authentication policies.	Review adequacy of procedures for monitoring compliance with specific identification and authentication policies; selectively test compliance with key identification and authentication policies.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.5	Users are appropriately identified and authenticated.	Authenticators: are adequately controlled by the assigned user and not subject to disclosure; and cannot be easily guessed or duplicated. Additional considerations for passwords are described below.	Review pertinent entity policies and procedures; assess procedures for generating and communicating authenticators to users; interview users; review related security software parameters. Observe users using authenticators; attempt to logon without a valid authenticator. Assess compliance with NIST guidance on authenticator selection, content, and usage.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.6	Users are appropriately identified and authenticated.	Password-based authenticators: <ul style="list-style-type: none"> • are not displayed when entered; • are changed periodically (e.g., every 30 to 90 days); • contain alphanumeric and special characters; • are sufficiently long (e.g., at least 8 characters in length); • have an appropriate life (automatically expire); • are prohibited from reuse for a specified period of time (e.g., at least 6 generations); and • are not the same as the user ID. 	Review pertinent entity policies and procedures; assess procedures for generating and communicating passwords to users; interview users; review security software password parameters. Observe users keying in passwords; attempt to logon without a valid password; make repeated attempts to guess passwords. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing). Assess entity compliance with NIST SP 800-63 , which provides guidance on password selection and content.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.7	Users are appropriately identified and authenticated.	Attempts to log on with invalid passwords are log limited (e.g., 3 – 7 attempts).	Examine security parameters for failed log-on attempts; review security logs to determine whether attempts to gain access are logged and reviewed by entity security personnel; if appropriate, repeatedly attempt to logon using invalid passwords.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.8	Users are appropriately identified and authenticated.	Use of easily guessed passwords (such as names or words) are prohibited.	As appropriate, review a system-generated list of current passwords; search password file using audit software to identify use of easily guessed passwords. Review management’s controls to prevent or detect easily guessed passwords.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.9	Users are appropriately identified and authenticated.	Generic user IDs and passwords are not used.	Interview users and security managers; review a list of IDs and passwords to identify generic IDs and passwords in use.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.10	Users are appropriately identified and authenticated.	Vendor-supplied default passwords are replaced during installation.	Attempt to log on using common vendor supplied passwords; search password file using audit software. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing).

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.11	Users are appropriately identified and authenticated.	Passwords embedded in programs are prohibited. (Note: An embedded password is a password that is included into the source code of an application or utility. Applications often need to communicate with other applications and systems and this requires an “authentication” process which is sometimes accomplished through the use of embedded passwords).	Discuss with entity security management how it obtains reasonable assurance that there are no embedded passwords used. If used, determine whether procedures have been established to monitor their use. Review selected programs for embedded passwords.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.12	Users are appropriately identified and authenticated.	Use of and access to authenticators is controlled (e.g., their use is not shared with other users).	Review procedures to ensure that accounts are not shared. Select accounts to determine compliance with procedures.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.13	Users are appropriately identified and authenticated.	Effective procedures are implemented to handle lost, compromised, or damaged authenticators (e.g., tokens, PKI certificates, biometrics, passwords, and key cards).	Identify procedures for handling lost or compromised authenticators; interview users and selectively test compliance with procedures.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.15	Users are appropriately identified and authenticated.	Where appropriate, digital signatures, PKI, and electronic signatures are effectively implemented.	Determine how non-repudiation is assured and if PKI and electronic/digital signatures are effectively implemented.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.16	Users are appropriately identified and authenticated.	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.	Review pertinent entity policies and procedures; assess procedures for generating and communicating certificates to users; interview users; review security software certificate parameters; obtain the help of experts if needed.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.17	Users are appropriately identified and authenticated.	Authentication information is obscured (e.g., password is not displayed).	Review procedures for controlling the display of authentication information.
Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.18	Users are appropriately identified and authenticated.	Appropriate session-level controls are implemented (e.g., name/address resolution service, session authenticity).	Assess the adequacy of session-level controls to include name/address resolution service, session authenticity, protection of session level information held in temporary storage, and controls to ensure that one session ends before the next session begins (prevent overlapping sessions).
Critical Element AC-3: Implement effective authorization controls	AC-3.1.1	User accounts are appropriately controlled.	Resource owners have identified authorized users and the access they are authorized to have.	These audit procedures should be coordinated with section 3.4 (segregation duties) to ensure that users do not have access to incompatible functions. Review written policies and procedures; a selection of users (both application and information security personnel), review access authorization documentation and applicable rights and privileges in the information system.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-3: Implement effective authorization controls	AC-3.1.2	User accounts are appropriately controlled.	Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs. (Standard naming conventions are essential to ensure effective configuration management identification and control of production files and programs vs. test files and programs).	Determine directory names for sensitive or critical files and obtain security reports of related access rules. Using these reports, determine who has access to sensitive files and whether the access matches the level and type of access authorized. Determine whether standard naming conventions are established and used effectively.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.3	User accounts are appropriately controlled.	Security managers review access authorizations and discuss any questionable authorizations with resource owners.	Interview security managers and review documentation provided to them to determine whether they review access authorizations to include follow-ups with resource owners on questionable authorizations.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.4	User accounts are appropriately controlled.	All changes to security access authorizations are automatically logged and periodically reviewed by management independent of the security function; unusual activity is investigated.	Review a selection of recent changes to security access authorizations and related logs for evidence of management review and unusual activity; determine if unusual activity is being/has been investigated.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.5	User accounts are appropriately controlled.	Resource owners periodically review access authorizations for continuing appropriateness.	Interview owners and review supporting documentation; determine whether they review access authorizations; determine whether inappropriate access rights are removed in a timely manner.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.6	User accounts are appropriately controlled.	Access is limited to individuals with a valid business purpose (least privilege).	Identify who has access to user accounts and sensitive system resources and the business purpose for this access.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-3: Implement effective authorization controls	AC-3.1.7	User accounts are appropriately controlled.	Unnecessary accounts (default, guest accounts) are removed, disabled, or otherwise secured.	Verify that unnecessary accounts are removed, disabled, or secured.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.8	User accounts are appropriately controlled.	Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters; review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.9	User accounts are appropriately controlled.	Access to shared file systems is restricted to the extent possible (for example, only to particular hosts, and only for the level of access required).	Determine how access to shared file systems is restricted and verify that it works effectively.
Critical Element AC-3: Implement effective authorization controls	AC-3.1.10	User accounts are appropriately controlled.	Emergency or temporary access (e.g., firecall IDs) is appropriately controlled, including: <ul style="list-style-type: none"> • documented and maintained, • approved by appropriate managers, • securely communicated to the security function, • automatically terminated after a predetermined period, and • all activity is logged. 	Review pertinent policies and procedures for emergency/temporary access IDs, including firecall IDs; compare a selection of both expired and active temporary and emergency authorizations (obtained from authorizing parties) with a system generated list of authorized users. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed. Review procedures for monitoring the use of emergency/temporary IDs (including firecall IDs) to ensure that access was used properly to correct a problem.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-3: Implement effective authorization controls	AC-3.2.1	Processes and services are adequately controlled.	<p>Available processes and services are minimized, such as through:</p> <ul style="list-style-type: none"> installing only required processes and services based on least functionality, restricting the number of individuals with access to such services based on least privilege, monitoring the use of such services, and maintaining current service versions. <p>Note; Installed processes and services should be consistent with approved system baseline.</p>	Review procedures for minimizing processes and services consistent with approved system baseline; interview system administrator; identify what services are installed and determine if they are required; determine who has access to these services and if they need them; determine how access to these services is monitored; and determine if the service versions are kept current. If appropriate, scan for poorly configured, unnecessary, and dangerous processes and services.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.1	Access to sensitive system resources is restricted and monitored.	Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose.	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions. Identify and test who has access to sensitive/privileged accounts and determine the reason for that access.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.2	Access to sensitive system resources is restricted and monitored.	Use of sensitive/privileged accounts is adequately monitored.	Determine if the use of sensitive and privileged accounts is monitored and evaluate the effectiveness of monitoring procedures.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.3	Access to sensitive system resources is restricted and monitored.	Logical access to utilities and tools is adequately controlled (for example, remote maintenance).	Determine the last time the access capabilities of staff with special system access privileges (e.g., system programmers) were reviewed. Review security software settings to identify types of activity logged. Observe personnel accessing system software, such as sensitive utilities and note the controls encountered to gain access. Attempt to access the operating system and other system software. Select some application programmers and determine whether they are authorized access.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.4	Access to sensitive system resources is restricted and monitored.	Files relied upon by operating systems are appropriately controlled.	Determine if access to files relied upon by operating systems are adequately controlled.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.5	Access to sensitive system resources is restricted and monitored.	Passwords/authentication services and directories are appropriately controlled and encrypted when appropriate.	Determine if password files and authentication services are adequately protected from unauthorized access. Determine if password files are encrypted.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.8	Access to sensitive system resources is restricted and monitored.	The information system partitions or separates user functionality (including user interface services) from information system management functionality.	Interview officials and review related system documentation. Coordinate with vulnerability analysis.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.9	Access to sensitive system resources is restricted and monitored.	The information system isolates security functions from nonsecurity functions.	Interview officials and review related system documentation. Coordinate with vulnerability analysis.
Critical Element AC-4: Adequately protect sensitive system resources	AC-4.2.5	Adequate media controls have been implemented.	Security parameters are clearly associated with information exchanged between information systems.	Determine if security parameters are clearly associated with information exchanged.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.1.1	An effective incident response program is documented and approved.	<p>An effective incident-response program has been implemented and include:</p> <ul style="list-style-type: none"> • documented policies, procedures, and plans; • documented testing of the incident response plan and follow-up on findings; • a means of prompt centralized reporting; • active monitoring of alerts/advisories; • response team members with the necessary knowledge, skills, and abilities; • training on roles and responsibilities and periodic refresher training; • links to other relevant groups; • protection against denial-of-service attacks (see http://icat.nist.gov); • appropriate incident-response assistance; and • consideration of computer forensics. 	<p>Interview security manager, response team members, and system users; review documentation supporting incident handling activities; compare practices to policies, procedures, and related guidance such as NIST SP 800-61 that provides guidance on incident-handling and reporting. Determine qualifications of response team members; review training records; identify training in incident response roles and responsibilities.</p> <p>Identify the extent to which computer forensics is used and compare to applicable guidelines and industry best practices.</p>
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.2.1	Incidents are effectively identified and logged.	An effective intrusion detection system has been implemented, including appropriate placement of intrusion-detection sensors and incident thresholds.	Obtain the design and justification for the intrusion detection system; determine if the placement of sensors and incident thresholds is appropriate based on cost and risk.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.2.3	Incidents are effectively identified and logged.	All auditable events, including access to and modifications of sensitive or critical system resources, are logged.	Review security software settings to identify types of activity logged; compare to NIST SP 800-92 guidance on auditable events.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.2.4	Incidents are effectively identified and logged.	Audit records contain appropriate information for effective review including sufficient information to establish what events occurred, when the events occurred (for example, time stamps), the source of the events, and the outcome of the events.	Determine if audit records/logs are reviewed and whether they contain appropriate information; see NIST SP 800- 92 for guidance.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.2.5	Incidents are effectively identified and logged.	Audit record storage capacity is adequate and configured to prevent such capacity from being exceeded. In the event of an audit failure or audit storage capacity being reached, the information system alerts officials and appropriate action is taken.	Determine the retention period for audit records and logs and whether it complies with applicable guidance. Determine if audit capacity is sufficient and what happens should it be exceeded.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.2.6	Incidents are effectively identified and logged.	Audit records and tools are protected from unauthorized access, modification, and deletion. Audit records are effectively reviewed for unusual or suspicious activity or violations.	Determine how access to audit records/logs is controlled; review logs for suspicious activity and evidence of entity follow-up and appropriate corrective action.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.2.7	Incidents are effectively identified and logged.	Audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Determine if audit record retention (for example, logs etc.) meet legal requirements and entity policy for computer forensics. See General Records Schedule 20 and 24 for guidance on requirements for record retention. (http://archives.gov/recordsmgmt/ardor/grs20.html and http://archives.gov/recordsmgmt/ardor/grs24.html)
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.3.1	Incidents are properly analyzed and appropriate actions taken.	Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported and investigated.	Review pertinent policies and procedures; review security violation reports; examine documentation showing reviews of questionable activities.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.3.2	Incidents are properly analyzed and appropriate actions taken.	Security managers investigate security violations and suspicious activities and report results to appropriate supervisory and management personnel.	Test a selection of security violations to verify that follow-up investigations were performed and reported to appropriate supervisory and management personnel.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.3.3	Incidents are properly analyzed and appropriate actions taken.	Appropriate disciplinary actions are taken.	For the selection reviewed in AC-5.3.2, determine what action was taken against the perpetrator.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.3.4	Incidents are properly analyzed and appropriate actions taken.	Violations and incidents are analyzed, summarized, and reported to senior management and appropriate government authorities.	Interview senior management and personnel responsible for summarizing violations; review any supporting documentation. Determine if automated tools are used to analyze network activity and whether it complies with security policy.
Critical Element AC-5: Implement an effective audit and monitoring capability	AC-5.3.8	Incidents are properly analyzed and appropriate actions taken.	Critical system resources are periodically reviewed for integrity.	Determine how frequently alterations to critical system files are monitored (for example, integrity checkers, etc.).
Critical Element AC-6. Establish adequate physical security controls	AC-6.1.2	Establish an effective physical security management program based on risk.	Facilities and areas housing sensitive and critical resources have been identified. The following generally constitute sensitive areas: computer rooms, tape libraries, telecommunication closets, mechanical/ electrical rooms, cooling facilities and data transmission and power lines.	Review diagram of physical layout of the computer network, telecommunications, and cooling system facilities (for example, HVAC); Inspect these areas for physical access control weaknesses.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-6: Establish adequate physical security controls	AC-6.1.5	Establish an effective physical security management program based on risk.	Conduct annual employee physical security awareness training. Coordinate this step with SM-4.	Review information (for example, individual training records, training program content) on security awareness training and its frequency.
Critical Element AC-6: Establish adequate physical security controls	AC-6.3.1	Establish adequate security at entrances and exits based on risk.	All employee access is authorized and credentials (for example, badges, identification cards, smart cards) are issued to allow access.	Observe and document all access control devices used to secure the facility.
Critical Element AC-6: Establish adequate physical security controls	AC-6.3.2	Establish adequate security at entrances and exits based on risk.	Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	Observe entries to and exits from facilities during and after normal business hours. Obtain a list of employees and contractors with badged access and check the justification for such access. Check whether terminated employees/contractors have turned in their badge.
Critical Element AC-6: Establish adequate physical security controls	AC-6.3.3	Establish adequate security at entrances and exits based on risk.	Management conducts regular reviews of individuals with physical access to sensitive facilities to ensure such access is appropriate.	Review procedures used by management to ensure that individuals accessing sensitive facilities are adequately restricted. Evaluate support for physical access authorizations and determine appropriateness.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element AC-6: Establish adequate physical security controls	AC-6.4.3	Establish adequate interior security based on risk.	Sensitive information technology and infrastructure resources are adequately secured (for example, using keys, alarm systems, security software and other access control devices), including: <ul style="list-style-type: none"> • the badging system, • computer room, master consoles, and tape libraries, • display and output devices, • data transmission lines, • power equipment and power cabling, • mobile or portable systems, and • utility and mechanical areas (HVAC, elevator, water). 	Interview officials. Walk through facilities and observe potential vulnerabilities and security controls [measures] used to protect sensitive information technology resources. Observe entries to and exits from sensitive areas during and after normal business hours. Review security software features and settings. Evaluate the badging system: who has access to the badging system and how it is protected; how is physical control maintained over unissued and visitor badges. Test the controls.
Critical Element AC-6: Establish adequate physical security controls	AC-6.4.4	Establish adequate interior security based on risk.	Management conducts regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate.	Review procedures used by management to ensure that individuals accessing sensitive areas are adequately restricted. Determine if there is a periodic (e.g., annual) auditing and reconciliation of ID cards. Evaluate support for physical access authorizations and determine appropriateness.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-1: Develop and document CM policies, plans, and procedures	CM-1.1	CM policies, plans, and procedures have been developed, documented, and implemented.	<p>An effective configuration management process is documented and implemented, including:</p> <ul style="list-style-type: none"> • a CM plan that identifies roles, responsibilities, procedures, and documentation requirements; • guidance that is appropriate for personnel with varying levels of skill and experience; • trained personnel who are familiar with the organization’s configuration management process;3 • permitting only essential capabilities and restricting the use of dangerous functions, ports, protocols, and services; • regular review and approval of configuration changes by management (for example, Configuration Control Board (CCB)); • appropriate representation on CCB from across the entity; • a formal SDLC methodology that includes system-level security engineering principles to be considered in the design, development, and operation of an information system, • appropriate systems documentation. 	<p>Review CM policies, plans, and procedures to identify roles, responsibilities, procedures, and documentation requirements.</p> <p>Determine if a CCB exists and is operating effectively.</p> <p>Review organizational chart to ensure that the CCB has appropriate representation from across the entity.</p> <p>Interview hardware and software managers to identify the currency and completeness of CM policies, plans, procedures, and documentation.</p> <p>Review CM documentation and test whether recent changes are incorporated.</p> <p>Review the SDLC methodology and ensure that security is adequately considered throughout the life cycle.</p> <p>Review a selection of system documentation to verify that the SDLC methodology was followed and complies with appropriate guidance, such as NIST SP 800-64 and SP 800-27.</p>

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-2: Maintain current configuration identification information	CM-2.1.1	Current configuration identification information is maintained.	A current and comprehensive baseline inventory of hardware, software, and firmware is documented, backed up, and protected. Information system documentation describes security controls in sufficient detail to permit analysis and testing of controls. For Federal entities, baseline meets minimum configuration management standards as required by NIST standards and OMB.	Request an inventory of all computer assets and determine if the inventory is accurate, complete, and whether duplicate copies are adequately protected. Select items in the inventory and trace to the asset and verify that the configuration (model, settings, etc.) is accurate. Select assets at the entity and verify that they are accurately recorded in the inventory. (Note: Selections should be focused on areas that are most relevant to the audit.)
Critical Element CM-2: Maintain current configuration identification information	CM-2.1.3	Current configuration identification information is maintained.	Configuration settings optimize the system's security features.	Determine if key component security settings conform with NIST SP 800-70 and vendor recommendations.
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.1	All configuration changes are properly managed (authorized, tested, approved, and tracked).	An appropriate formal change management process is documented.	Review the change management methodology for appropriateness. Review system documentation to verify that the change management methodology was followed.
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.2	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Configuration changes are authorized by management. Configuration management actions are recorded in sufficient detail so that the content and status of each configuration item is known and previous versions can be recovered.	Review system logs for configuration changes. Determine whether these changes have been properly authorized. Examine a selection of CM and software change request forms for approvals and sufficiency of detail. Interview CM management and software development staff. Review a selection of configuration exceptions identified by the entity in its configuration audit (Refer to CM 4.1) or through other audit procedures to identify any weaknesses in the entity's configuration change process.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM 3.1.4	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Detailed specifications are prepared by the programmer and reviewed by a programming supervisor for system and application software changes.	For the software change requests selected for control activity CM-3.1.2: <ul style="list-style-type: none"> • review specifications and related documentation for evidence of supervisory review.
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM 3.1.5	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Test plan standards have been developed for all levels of testing that define responsibilities for each party (for example, users, system analysts, programmers, auditors, quality assurance, library control).	Review test plan standards.
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM 3.1.6	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Test plans are documented and approved that define responsibilities for each party involved (for example, users, systems analysts, programmers, auditors, quality assurance, library control).	For the software change requests selected for control activity CM-3.1.2: <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, abends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.7	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Test plans include appropriate consideration of security.	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, abends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.8	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Unit, integration, and system testing are performed and approved in accordance with the test plan and apply a sufficient range of valid and invalid conditions.	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, abends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.9	All configuration changes are properly managed (authorized, tested, approved, and tracked).	A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, abends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.11	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Test results are documented and appropriate responsive actions are taken based on the results.	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, abends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.12	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Program changes are moved into production only when approved by management and by persons independent of the programmer.	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, abends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.13	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.14	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Appropriate tools (for example, library mgt. software and manual techniques) are used to: <ul style="list-style-type: none"> • produce audit trails of program changes, • maintain program version numbers, • record and report program changes, • maintain creation/date information for production modules, • maintain copies of previous versions, and • control concurrent updates. 	Review pertinent policies and procedures. Interview personnel responsible for appropriate tools and library control. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. Determine whether documentation is maintained on program changes, program version numbers, creation/date information, and copies of prior versions. Review procedures for controlling concurrent updates. Assess the adequacy of access controls over CM tools (e.g., library management software) to ensure segregation of duties is adequately enforced. (Coordinate with audit procedures in AC 4.1).
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.15	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Configuration/software changes are documented so that they can be traced from authorization to the final approved code and they facilitate “trace-back” of code to design specifications and functional requirements by system testers.	For the software change requests selected for control activity CM-3.1.2: <ul style="list-style-type: none"> • trace changes from authorization to the final approved code; and, • trace changes back from code to design specifications and functional requirements.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.16	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Program development and maintenance, testing, and production programs are maintained separately (for example, libraries) and movement between these areas is appropriately controlled, including appropriate consideration of segregation of duties (see the Segregation of Duties control category).	<p>Review pertinent policies and procedures and interview library control personnel.</p> <p>Examine libraries in use. Test access to each program library (e.g., development, test, production) by examining security system parameters.</p> <p>Review program changes procedures for adherence to appropriate segregation of duties between application programming and movement of programs into production. For a selection of program changes, examine related documentation to verify that (1) procedures for authorizing movement among libraries were followed and (2) before and after images were compared to ensure that unauthorized changes were not made to the programs.</p>
Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.17	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Access to all programs, including production code, source code, and extra program copies, are adequately protected.	<p>For critical software production programs, determine whether access control software rules are clearly defined.</p> <p>Test access to program libraries by examining security system parameters.</p>
Critical Element CM-4: Routinely monitor the configuration	CM-4.1.1	The configuration is routinely audited and verified.	Routinely validate that the current configuration information is accurate, up-to-date, and working as intended for networks, operating systems, and infrastructure applications.	<p>Identify the standards and procedures used to audit and verify the system configuration.</p> <p>Determine when and how often the configuration is verified and audited.</p> <p>Review a selection of the configuration verifications and audits for compliance with applicable standards. Verify that vendor supplied system software is still supported by the vendor.</p> <p>Evaluate adequacy of the configuration audits based on the results of the IS control audit tests performed.</p>

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-4: Routinely monitor the configuration	CM-4.1.2	The configuration is routinely audited and verified.	The verification and validation criteria for the configuration audit is appropriate and specifies how the configuration item will be evaluated in terms of correctness, consistency, necessity, completeness, and performance.	Review evaluation criteria for selected releases to determine whether verification and validation criteria for the configuration audit addresses the correctness, consistency, necessity, completeness, and performance of the configuration items. Identify all configuration items, deviations and waivers, and the status of tests. Determine if configuration items have gaps in the documentation or if there are defects in the change management process.
Critical Element CM-4: Routinely monitor the configuration	CM-4.1.3	The configuration is routinely audited and verified.	Confirm compliance with applicable configuration management policy, plans, standards, and procedures.	Compare configuration policy, plans, standards, and procedures with observations.
Critical Element CM-4: Routinely monitor the configuration	CM-4.1.4	The configuration is routinely audited and verified.	The information system periodically verifies the correct operation of security functions – on system start up and restart, on command by user with appropriate privilege – (providing system audit trail documentation) and takes appropriate action (for example, notifies system administrator, shuts the system down, restarts the system) when anomalies are discovered.	Interview officials and review related system documentation. Observe or test this system capability to determine that procedures are followed and related system documentation is generated and reviewed by entity security staff.
Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.1	Software is promptly updated to protect against known vulnerabilities.	Information systems are scanned periodically to detect known vulnerabilities.	Interview entity officials. Identify the criteria and methodology used for scanning, tools used, frequency, recent scanning results, and related corrective actions. Coordinate this work with the AC section.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.2	Software is promptly updated to protect against known vulnerabilities.	An effective patch management process is documented and implemented, including: <ul style="list-style-type: none"> • identification of systems affected by recently announced software vulnerabilities; • prioritization of patches based on system configuration and risk; • appropriate installation of patches on a timely basis, including testing for effectiveness and potential side effects on the entity’s systems; and • verification that patches, service packs, and hotfixes were appropriately installed on affected systems. 	Review pertinent policies and procedures. Interview users and data processing staff.
Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.3	Software is promptly updated to protect against known vulnerabilities.	Software is up-to-date; the latest versions of software patches are installed.	Compare vendor recommended patches to those installed on the system. If patches are not up-to-date, determine why they have not been installed.
Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.4	Software is promptly updated to protect against known vulnerabilities.	An effective virus, spam, and spyware protection process is documented and implemented, including: appropriate policies and procedures; effective protection software is installed that identifies and isolates suspected viruses, spam, and spyware; and virus, spam, and spyware definitions are up-to-date.	Review pertinent policies and procedures. Interview users and data processing staff. Verify that actual software is installed and up-to-date.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CM-6: Appropriately document and approve emergency changes to the configuration	CM-6.1.1	Adequate procedures for emergency changes are documented and implemented.	Appropriately document and implement procedures for emergency changes.	Review procedures to determine whether they adequately address emergency change requirements.
Critical Element CM-6: Appropriately document and approve emergency changes to the configuration	CM-6.2.1	Emergency changes to the configuration are documented and approved.	Appropriately document and approve emergency changes to the configuration and notify appropriate personnel for analysis and follow-up.	For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.
Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.1	Incompatible duties have been identified and policies implemented to segregate these duties.	Policies and procedures for segregating duties exist and are up-to-date.	Review pertinent policies and procedures. Interview selected management and information security personnel regarding segregation of duties.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.2	Incompatible duties have been identified and policies implemented to segregate these duties.	Distinct system support functions where possible are performed by different individuals, including the following: <ul style="list-style-type: none"> • information security management, • systems design, • applications programming, • systems programming, • quality assurance/testing, • library management/change management, • computer operations, • production control and scheduling, • data control, • data security, • data administration, • network administration, • configuration management. 	Review an entity organization chart showing information security functions and assigned personnel. Interview selected personnel and determine whether functions are appropriately segregated. Determine whether the chart is current and each function is staffed by different individuals. Review relevant alternate or back up assignments and determine whether the proper segregation of duties is maintained. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.3	Incompatible duties have been identified and policies implemented to segregate these duties.	No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual: <ul style="list-style-type: none"> • data entry and verification of data, • data entry and its reconciliation to output, • input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information), • data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor’s review and approval). 	Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.4	Incompatible duties have been identified and policies implemented to segregate these duties.	Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Interview management, observe activities, and test transactions. Note: Perform this in conjunction with SD-2.2.
Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.5	Incompatible duties have been identified and policies implemented to segregate these duties.	Data processing personnel are not users of information systems. They and security managers do not initiate, input, or correct transactions.	Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.
Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.7	Incompatible duties have been identified and policies implemented to segregate these duties.	Access controls enforce segregation of duties.	Audit procedures are found in section AC-3.1, but this item is listed here as a reminder. Logical and physical access controls should enforce segregation of duties.
Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.2.2	Active supervision and review are provided for all personnel.	Access authorizations are periodically reviewed for incompatible functions.	Review a selection of access authorizations for incompatible functions and evidence of supervisory review.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.2.3	Active supervision and review are provided for all personnel.	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (for example, periodic risk assessments).	Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. Note: This audit step should be performed in conjunction with audit steps in critical elements SM-2 (Periodically assess and validate risks) and SM-5 (Monitor the effectiveness of the security program).
Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.2.5	Active supervision and review are provided for all personnel.	Supervisors routinely review user activity logs for incompatible actions and investigate any abnormalities.	Interview supervisors and review user activity logs for incompatible actions. Check for evidence of supervisory review.

Title / Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
<p>Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources</p>	<p>CP-1.1.1</p>	<p>Critical data and operations are identified and prioritized.</p>	<p>The entity categorizes information systems in accordance with appropriate guidance, such as FIPS 199, and documents the results in the system security plan.</p>	<p>Perform the following procedures for CP-1.1.1 to CP-1.1.2.</p> <p>Review the policies and methodology used to categorize systems and create the critical operations list. This list should identify each system and its criticality in supporting the entity’s primary mission or business functions.</p> <p>Review how systems are categorized and the critical operations list. Determine if the justifications have been documented and that they (1) prioritize data and operations by primary mission or business functions; (2) are approved by senior management; and (3) reflect current operating conditions, including key system interdependencies.</p> <p>Determine if technology supporting critical operations is identified and appropriately considered in processing priorities.</p> <p>Interview program, information technology, and security administration officials.</p> <p>Determine their input and assessment of the reasonableness of priorities established.</p>

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
<p>Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources</p>	<p>CP-1.1.2</p>	<p>Critical data and operations are identified and prioritized.</p>	<p>A list of critical operations and data has been documented that:</p> <ul style="list-style-type: none"> • identifies primary mission or business functions, • prioritizes data and operations, • is approved by senior program managers, and • reflects current conditions including system interdependencies and technologies. 	<p>Perform the following procedures for CP-1.1.1 to CP-1.1.2.</p> <p>Review the policies and methodology used to categorize systems and create the critical operations list. This list should identify each system and its criticality in supporting the entity’s primary mission or business functions.</p> <p>Review how systems are categorized and the critical operations list. Determine if the justifications have been documented and that they (1) prioritize data and operations by primary mission or business functions; (2) are approved by senior management; and (3) reflect current operating conditions, including key system interdependencies.</p> <p>Determine if technology supporting critical operations is identified and appropriately considered in processing priorities.</p> <p>Interview program, information technology, and security administration officials.</p> <p>Determine their input and assessment of the reasonableness of priorities established.</p>

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources	CP-1.2.1	Resources supporting critical operations are identified and analyzed.	Resources supporting critical operations and functions have been identified and documented. Types of resources identified should include: <ul style="list-style-type: none"> • computer hardware, • computer software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources. 	Interview program and security administration officials responsible for developing the critical operations listing. Review documentation supporting the critical operations listing to verify that the following resources have been identified for each critical operation: <ul style="list-style-type: none"> • computer hardware and software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources. Appropriate documentation may include contingency-related plans in NIST SP 800-34 .
Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources	CP-1.2.2	Resources supporting critical operations are identified and analyzed.	Critical information technology resources have been analyzed to determine their impact on operations if a given resource were disrupted or damaged. This analysis should evaluate the impact of the outages over time and across related resources and dependent systems.	Determine if a current business impact analysis has been conducted that identifies critical information technology resources, disruption impacts, allowed outage times, and recovery priorities.
Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources	CP-1.3.1	Emergency processing priorities are established.	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	Review related policies, plans, and procedures for emergency processing and ensure: <ul style="list-style-type: none"> • recovery priorities have been developed, • management has approved priorities, and • priorities are documented. Request a copy of the continuity of operations plan. Interview program and security administration officials to determine whether they are aware of all policies and procedures for emergency processing priorities and maintain copies of the continuity of operations plan.

Title / Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.1.1	Information system back up and recovery procedures have been implemented.	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	<p>Review written policies and procedures for backing up and transporting files. Determine how often files are backed up and rotated off site, retention periods, and security involved in transport.</p> <p>Compare inventory records with the files maintained off-site and determine the age of these files.</p> <p>For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports.</p> <p>Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.</p> <p>Determine if the technology is implemented in such a manner as to provide appropriate availability, including consideration of backup procedures, system configuration, redundancy, environmental controls, staff training, and routine maintenance.</p>
Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.1.4	Information system back up and recovery procedures have been implemented.	<p>The information system back up and recovery procedures adequately provide for recovery and reconstitution to the system’s original state after a disruption or failure including:</p> <ul style="list-style-type: none"> • system parameters are reset; • patches are reinstalled; • configuration settings are reestablished; • system documentation and operating procedures are available; • application and system software is reinstalled; • information from the most recent backup is available; and • the system is fully tested. 	<p>Interview entity officials and determine whether comprehensive procedures and mechanisms exist to fully restore the information security to its original state.</p> <p>Determine if this recovery capability has been tested and, if so, review the test plan and test results.</p>

B.2 GENERAL CONTROLS – OTHER

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.1 Security Management (SM)	Critical Element SM-1: Establish a Security Management Program	SM-1.2.1	A security management structure has been established.	Senior management establishes a security management structure for entity-wide, system, and application levels that have adequate independence, authority, expertise, and resources.	Review security policies and plans, the entity’s organization chart, and budget documentation. Interview security management staff. Evaluate the security structure: independence, authority, expertise, and allocation of resources required to adequately protect the information systems.
3.1 Security Management (SM)	Critical Element SM-1: Establish a Security Management Program	SM-1.2.2	A security management structure has been established.	An information systems security manager has been appointed at an agency/entity level and at appropriate subordinate (i.e., system and application) levels and given appropriate authority.	Review pertinent organization charts and job descriptions. Interview the overall security manager and subordinate security managers responsible for specific systems and applications.
3.1 Security Management (SM)	Critical Element SM-1: Establish a Security Management Program	SM-1.3	Information security responsibilities are clearly assigned.	The security program documentation clearly identifies owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined at the entity-wide, system, and application levels for (1) information resource owners and users, (2) information technology management and staff, (3) senior management, and (4) security administrators.	Review security program documentation detailing security responsibilities and rules of behavior for security officials, resource owners, and users at the entity-wide, system, and application levels.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.1 Security Management (SM)	Critical Element SM-2: Periodically access and validate risks	SM-2.1.6	Risk assessments and supporting activities are systematically conducted.	Federal systems are certified and accredited before being placed in operation and at least every 3 years, or more frequently if major system changes occur.	For federal systems that are significant to the audit objectives, review certification and accreditation documentation and determine compliance with NIST SP 800-37 . The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding the certification and accreditation process (including related controls), reading the certifications and accreditations for the key systems relevant to the audit objectives, and determining whether the certification and accreditation documentation for the systems tested is consistent with the testing results.
3.1 Security Management (SM)	Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.1.2	Owners, system administrators, and users are aware of security policies.	Security policies are distributed to all affected personnel, including system and application rules and expected user behaviors.	Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. If appropriate, call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password. (See Section 2.2.2 "Appropriateness of Control Testing" for discussion of performance issues relating to this type of testing).

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.1 Security Management (SM)	Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.2.1	Hiring, transfer, termination, and performance policies address security.	For prospective employees, references are contacted and background checks performed. Individuals are screened before they are given authorization to access organizational information and information systems.	Review hiring policies. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
3.1 Security Management (SM)	Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.2.2	Hiring, transfer, termination, and performance policies address security.	Periodic reinvestigations are performed as required by law, and implementing regulations [at least once every 5 years], consistent with the sensitivity of the position. For federal entities, criteria can be obtained from the Office of Personnel Management (OPM).	Review applicable laws, regulations and reinvestigation policies (e.g., 5 CFR 731.106(a); OPM/Agency policy, regulations and guidance; FIPS 201 & NIST SP 800-73, 800-76, 800-78 ; and, any criteria established for the risk designation of the assigned position.) For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed as required.
3.1 Security Management (SM)	Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.2.3	Hiring, transfer, termination, and performance policies address security.	Nondisclosure or security access agreements are required for employees and contractors assigned to work with sensitive information.	Review policies on confidentiality or security agreements. For a selection of such users, determine whether confidentiality or security agreements are on file.
3.1 Security Management (SM)	Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.2.4	Hiring, transfer, termination, and performance policies address security.	When appropriate, regularly scheduled vacations exceeding several days are required, and the individual's work is temporarily reassigned.	Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed employee's work during vacations.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.1 Security Management (SM)	Critical Element SM-4: Implement effective security awareness and other security-related personnel policies	SM-4.3.1	Employees have adequate training and expertise.	Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	Review job descriptions for security management personnel and for a selection of other system users. For a selection of employees, compare personnel records on education and experience with job descriptions.
3.1 Security Management (SM)	Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.3	The effectiveness of security controls are periodically assessed.	Management routinely conducts privacy impact assessments and promptly corrects identified control weaknesses.	Review privacy impact assessments, including the methodology, a selection of test plans, and related testing results.
3.1 Security Management (SM)	Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.4	The effectiveness of security controls are periodically assessed.	The frequency and scope of security control testing is commensurate with risk.	Determine if the frequency and scope of security control testing is based on risk.
3.1 Security Management (SM)	Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.5	The effectiveness of security controls are periodically assessed.	Performance measures and compliance metrics monitor the security processes and report on the state of compliance in a timely manner.	Review agency/entity performance measures and compare to NIST guidance (e.g., NIST SP 800-55).
3.1 Security Management (SM)	Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.6	The effectiveness of security controls are periodically assessed.	An independent evaluation (periodic, e.g., annual) of the entity's information security program tests the effectiveness of the security policies, procedures, and practices.	Review the results of these evaluations and assess their adequacy and effectiveness.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.1 Security Management (SM)	Critical Element SM-5: Monitor the effectiveness of the security program	SM-5.1.7	The effectiveness of security controls are periodically assessed.	Federal agencies report on the results of the annual independent evaluations to appropriate oversight bodies. Under OMB guidance, the head of each agency must submit security and privacy reports to OMB, which consolidates the information for a report to Congress. The Comptroller General must also periodically evaluate and report to Congress on the adequacy and effectiveness agency information security policies and practices.	Evaluate the reporting/summarization process and identify any significant discrepancies between reports at each level and whether the reports agree with independent audit evaluations. Note that OMB has annual requirements for FISMA and privacy reporting.
3.1 Security Management (SM)	Critical Element SM-6: Effectively Remediate Information Security Weaknesses	SM-6.1.2	Information security weaknesses are effectively remediated.	Deficiencies are analyzed in relation to the entire agency/entity, and appropriate corrective actions are applied entity-wide.	Review corrective action plans to determine whether entity-wide solutions were appropriately considered.
3.1 Security Management (SM)	Critical Element SM-7: Ensure that Activities Performed by External Third Parties are Adequately Secure	SM-7.1.2	External third party activities are secure, documented, and monitored.	Security requirements are included in the information system acquisition contracts based on an assessment of risk.	Review security provisions of selected contracts and determine that requirements are implemented. See FAR requirements for acquisition plans (48 CFR 7.1, 7.103 (u)).

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-1: Adequately protect information system boundaries	AC-1.1.4	Appropriately control connectivity to system resources.	Remote dial-up access is appropriately controlled and protected.	Interview network administrator and users; determine how remote dial-up access is controlled and protected (for example, monitor the source of calls and dial back mechanism); identify all dial-up lines through automatic dialer software routines and compare with known dial-up access; discuss discrepancies with management.
3.2 Access Controls (AC)	Critical Element AC-1: Adequately protect information system boundaries	AC-1.1.5	Appropriately control connectivity to system resources.	Remote Internet access is appropriately controlled and protected.	Interview network administrator and users; determine how connectivity is controlled and protected. Determine if federal agency policies, procedures, and practices comply with NIST SP 800-63 guidance on remote electronic authentication. Also, refer to OMB Memorandum 04-04 E-Authentication Guidance for Federal Agencies.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-1: Adequately protect information system boundaries	AC-1.1.6	Appropriately control connectivity to system resources.	Remote wireless access is appropriately controlled and protected.	<p>Interview network administrator and users; determine how connectivity is controlled and protected. Refer to NIST SP 800-97 Establishing Wireless Robust Security Networks: A guide to IEEE.802.11i for additional security assessment guidance.</p> <p>Test and validate entity controls: (1) use a wireless sniffer to capture data (for example, service set IDs (SSID)), (2) if an SSID is obtained, associate the SSID to the access point, (3) identify what network resources are available, (4) determine if a security protocol⁷⁶ is implemented, and (5) if a security protocol is used, employ a program to test the strength of the encryption algorithm.</p> <p>Test and validate entity controls to identify rogue wireless access points. Test for rogue wireless access points. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing).</p>
3.2 Access Controls (AC)	Critical Element AC-1: Adequately protect information system boundaries	AC-1.2.2	Appropriately control network sessions.	Where connectivity is not continual, network connection automatically disconnects at the end of a session.	Interview network administrator and users; observe whether the control is implemented.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-1: Adequately protect information system boundaries	AC-1.2.3	Appropriately control network sessions.	Appropriate warning banners are displayed before logging onto a system: <ul style="list-style-type: none"> • system use notification (for example, U. S. Government system, consent to monitoring, penalties for unauthorized use, privacy notices), • previous logon notification (for example, date and time of last logon and unsuccessful logons). 	Interview network administrator and users; observe whether the control is fully implemented and complies with NIST guidance.
3.2 Access Controls (AC)	Critical Element AC-2: Implement effective identification and authentication mechanisms	AC-2.1.2	Users are appropriately identified and authenticated.	Account policies (including authentication policies and lockout policies) are appropriate given the risk, and enforced.	Review account policies and determine if they are based on risk and seem reasonable, based on interviews with system administrator and users. Determine how they are enforced, and test selected policies.
3.2 Access Controls (AC)	Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.4	Users are appropriately identified and authenticated.	Selection of authentication methods (for example, passwords, tokens, biometrics, key cards, PKI certificates, or a combination therein) are appropriate, based on risk.	Determine whether authentication methods used are appropriate, based on system risk levels determined by the entity using NIST FIPS 199 . See NIST SP 800-53 authentication controls as specified for entity designated system risk levels.
3.2 Access Controls (AC)	Critical Element AC-2: Implement effective identification and authentication mechanisms	AC 2.1.14	Users are appropriately identified and authenticated.	Concurrent sessions are appropriately controlled.	Review procedures for controlling and auditing concurrent logons from different workstations. See NIST SP 800-53 .
3.2 Access Controls (AC)	Critical Element AC-3: Implement effective authorization controls	AC-3.2.2	Processes and services are adequately controlled.	The function and purpose of processes and services are documented and approved by management.	Obtain documentation describing the function and purpose of processes and services, and evidence of management approval.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-3: Implement effective authorization controls	AC-3.2.3	Processes and services are adequately controlled.	Information available to potential unauthorized users is appropriately restricted.	Determine if information about available processes and services is appropriately restricted.
3.2 Access Controls (AC)	Critical Element AC-3: Implement effective authorization controls	AC-3.2.4	Processes and services are adequately controlled.	The information system prohibits remote activation of collaborative computing mechanisms (for example, video and audio conferencing) and provides an explicit indication of use to the local users (for example, use of camera or microphone).	Determine if remote activation of collaborative computing services have been physically disconnected.
3.2 Access Controls (AC)	Critical Element AC-3: Implement effective authorization controls	AC-3.2.5	Processes and services are adequately controlled.	For publicly available systems, the information system controls protect the integrity and availability of the information and applications.	Identify controls used to protect the integrity and availability of the information and applications on such systems and test controls to ensure their effectiveness.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.6	Access to sensitive system resources is restricted and monitored.	Mobile code is appropriately controlled.	Interview system administrator and perform appropriate procedures to determine if mobile code is adequately controlled.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.7	Access to sensitive system resources is restricted and monitored.	Where appropriate, access is restricted based on time and/or location.	Determine if access is appropriately restricted based on time and/or location.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.1.10	Access to sensitive system resources is restricted and monitored.	The information system establishes a trusted communications path between the user and the security functionality of the system.	Interview officials with system and communication responsibilities and examine appropriate records such as developer design documents.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.2.1	Adequate media controls have been implemented.	Only authorized users have access to printed and digital media removed from the information system.	Interview personnel and review procedures. Observe entity practices and review selected access logs.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.2.2	Adequate media controls have been implemented.	The information system automatically identifies how information is to be used: <ul style="list-style-type: none"> • output is marked using standard naming conventions, and • internal data in storage, process and transmission is labeled. 	Interview appropriate personnel. For output, identify standard naming conventions and examine the system configuration. For internal data, examine the labeling mechanism and internal data for accurate labels. Test output and internal data for appropriate results.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.2.3	Adequate media controls have been implemented.	The organization controls the pickup, transport, and delivery of information system media (paper and electronic) to authorized personnel.	Interview officials and review appropriate policy and procedures. Observe selected media transport practices and receipts.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.2.4	Adequate media controls have been implemented.	Systems media is securely stored according to its sensitivity.	Determine if media storage practices are adequate and comply with applicable requirements (for federal agencies, FIPS 199 security categories).
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.2.6	Adequate media controls have been implemented.	Approved equipment, techniques, and procedures are implemented to clear sensitive data from digital media before its disposal or release for reuse outside of the organization.	Review written procedures; interview personnel responsible for clearing data from digital media. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and disposal of software. For selected items still in the entity's possession, test to determine whether they have been appropriately sanitized.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.3.1	Adequate media controls have been implemented.	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs where appropriate.	Determine if cryptographic tools are properly implemented. (See NIST standards for federal agencies) To evaluate the use of cryptographic tools, the auditor should obtain the assistance of a specialist.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.3.2	Adequate media controls have been implemented.	Encryption procedures are implemented in data communications where appropriate based on risk.	Capture passwords transmitted over the network and determine if they are encrypted; for federal system, determine if cryptographic authentication complies with FIPS 140-2 . To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.3.3	Adequate media controls have been implemented.	For authentication to a cryptographic module, the information system employs appropriate authentication methods.	Interview appropriate officials and review supporting documentation. For federal agencies, compare the authentication process to FIPS 140-2 requirements.
3.2 Access Controls (AC)	Critical Element AC-4: Adequately protect sensitive system resources	AC-4.3.4	Adequate media controls have been implemented.	The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.	Compare policy and practices to appropriate guidance, such as NIST guidance in SP 800-56 and SP 800-57 for cryptographic key establishment and management, respectively.
3.2 Access Controls (AC)	Critical Element AC-5: Implement an effective audit an monitoring capability	AC-5.2.2	Incidents are effectively identified and logged.	An effective process has been established based on a risk assessment, to identify auditable events that will be logged.	Interview the security manager to determine the process for determining what actions are logged. Determine if security event correlation tools are used to identify anomalous network activity.
3.2 Access Controls (AC)	Critical Element AC-5: Implement an effective audit an monitoring capability	AC-5.3.5	Incidents are properly analyzed and appropriate actions taken.	Alerts and advisories are issued to personnel when appropriate.	Identify recent alerts and advisories and determine if they are up-to-date; interview entity personnel to determine what actions were taken.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-5: Implement an effective audit an monitoring capability	AC-5.3.6	Incidents are properly analyzed and appropriate actions taken.	Incident and threat information is shared with owners of connected systems.	Determine if incident and threat data are shared with owners of connected systems; follow up with owners of connected systems to see if they received this information in a timely manner.
3.2 Access Controls (AC)	Critical Element AC-5: Implement an effective audit an monitoring capability	AC-5.3.7	Incidents are properly analyzed and appropriate actions taken.	Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate.	Review policies and procedures and interview appropriate personnel; review any supporting documentation.
3.2 Access Controls (AC)	Critical Element AC-5: Implement an effective audit an monitoring capability	AC-5.3.9	Incidents are properly analyzed and appropriate actions taken.	Appropriate processes are applied to gather forensic evidence in support of investigations.	Review entity processes to gather forensic information and determine whether they are adequate. Discuss with appropriate entity management.
3.2 Access Controls (AC)	Critical Element AC-6. Establish adequate physical security controls	AC-6.1	Establish an effective physical security management program based on risk.	N/A	Coordinate AC-6 procedures with sections SM-2 (assess and validate risks), SM-3 policies and procedures), SD-1 segregation of duties), and CP-2 environmental controls).
3.2 Access Controls (AC)	Critical Element AC-6. Establish adequate physical security controls	AC-6.1.1	Establish an effective physical security management program based on risk.	Use a risk management approach to identify level of physical security needed for the facility and implement measures commensurate with the risks of physical damage or access.	Interview entity officials to discuss how their physical security program is organized and whether they use a risk management approach. Obtain and review any facility risk assessments performed by the entity or by independent entities.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6. Establish adequate physical security controls	AC-6.1.3	Establish an effective physical security management program based on risk.	All significant threats to the physical well-being of these resources have been identified and related risks determined.	Interview entity officials. Review risk analysis to ensure that it includes physical threats to employees and assets. Review any recent audit reports or other evaluations of the facility's physical security.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.1.4	Establish an effective physical security management program based on risk.	Establish law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies, provide procedures for the timely receipt and dissemination of threat information, and implement a standardized security/threat classifications and descriptions (for example, alert levels).	Check if the organization has established law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies. Review how the organization receives and disseminates security alerts. Identify governmental agencies involved in the flow of security information and interview appropriate officials. Review procedures and nomenclature for threat information.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.1.6	Establish an effective physical security management program based on risk.	Security control procedures (for example, trusted vendors/suppliers, background checks, etc.) are established for non-employees (contractors, custodial personnel).	Review security control procedures scope and adequacy.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.1.7	Establish an effective physical security management program based on risk.	Periodic monitoring and independent evaluations of the physical security program are conducted. Physical security incidents are effectively monitored and appropriate countermeasures are implemented.	<p>Check if the entity evaluates its physical security program and controls.</p> <p>Obtain and review the entity’s most recent self assessments and compliance review report. Determine if security incidents are recorded, effectively analyzed, and result in appropriate countermeasures.</p> <p>Coordinate with SM-5: Monitor the effectiveness of the security program, and AC-5: Implement an effective audit and monitoring capability.</p>
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.1.8	Establish an effective physical security management program based on risk.	When possible, do not co-locate high risk operations with non-essential support organizations (for example, cafeteria, day care, banks, news media). If not possible, place appropriate security between such support organizations and critical facilities.	Identify co-located operations and their respective risk levels. Determine if the entity co-locates high risk operations with support operations and assess the security impact.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.1.9	Establish an effective physical security management program based on risk.	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	Review appointment and verification procedures for visitors, contractors, and maintenance personnel. Compare actual practices to procedures.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.2.1	Establish adequate perimeter security based on risk.	Control/restrict vehicle and pedestrian traffic around the facility based on the facility’s risk level. Specific measures include fences, gates, locks, guard posts, perimeter patrols and inspections.	Determine if vehicle and pedestrian traffic around the facility is adequately controlled for the risk level. Inspect the perimeter for physical security and access control weaknesses. Assess the effectiveness of perimeter guard procedures and practices for controlling access to facility grounds.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.2.2	Establish adequate perimeter security based on risk.	Control employee and visitor parking. For example, restrict access to facility parking and parking adjacent to the facility (including leases), use ID systems and procedures for authorized parking (for example, placard, decal, card key), have signs and arrangements for towing of unauthorized vehicles and adequate lighting for parking areas.	Observe parking area and related controls. Check if identification systems and procedures for authorized parking are in place. Determine what is done about unauthorized vehicles (e.g. towing).
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.2.3	Establish adequate perimeter security based on risk.	Monitor the perimeter with closed circuit television (CCTV) including cameras with time lapse video recording and warning signs advising of 24 hour video surveillance.	Inspect the facility surveillance camera system to assess its capacity and ability to assist in protecting the facility's perimeter.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.2.4	Establish adequate perimeter security based on risk.	Lighting is adequate for effective surveillance and evacuation operations. Emergency power backup exists for lighting (as well as for alarm and monitoring systems).	Observe perimeter and exterior building lighting to determine its adequacy. Also, determine if emergency power is available for security systems. Request test results.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.2.5	Establish adequate perimeter security based on risk.	Extend perimeter barriers (for example, concrete, steel) and parking barriers, as needed, to prevent unauthorized access and reduce exposure to explosions.	Determine if perimeter barriers are used and extended if appropriate.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.3.4	Establish adequate security at entrances and exits based on risk.	Intrusion detection systems with central monitoring capability are used to control access outside of normal working hours (for example, nights and weekends).	Determine if an intrusion detection system is used and test its use for appropriate exterior and interior apertures.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.3.5	Establish adequate security at entrances and exits based on risk.	Visitor access logs are maintained and reviewed.	Compare entries in the log to a list of personnel authorized access.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.3.6	Establish adequate security at entrances and exits based on risk.	X-ray and magnetometer equipment is used to screen people, possessions, and packages.	Observe how this equipment is used and test its effectiveness.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.3.7	Establish adequate security at entrances and exits based on risk.	The entity controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.	Review procedures and interview officials. Attempt to enter and exit the facility with information systems items at various entry points and times.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.3.8	Establish adequate security at entrances and exits based on risk.	Entry and exit points are monitored by using CCTV capability. Also, high security locks and alarm systems are required for all doors that are not guarded.	Observe use of these devices and test as appropriate. Inspect the building's) for physical access control weaknesses.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.3.9	Establish adequate security at entrances and exits based on risk.	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter the facility after fire drills, etc.	Review written emergency procedures. Examine documentation supporting prior fire drills. Observe a fire drill.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.1	Establish adequate interior security based on risk.	An ID badge should generally be displayed at all times. [All individuals must display an ID at all times.]	Observe use of employee and visitor IDs. See what happens if you do not display your own ID.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.2	Establish adequate interior security based on risk.	Visitors such as vendors, contractors, and service personnel who need access to sensitive areas are prescreened, formally signed in, badged and escorted.	Review visitor entry logs. Observe entries to and exits from sensitive areas during and after normal business hours. Interview guards at facility entry.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.5	Establish adequate interior security based on risk.	As appropriate, physical access logs to sensitive areas are maintained and routinely reviewed.	Compare entries in the logs to a list of personnel authorized access.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.6	Establish adequate interior security based on risk.	Unissued keys, badges, or other entry devices are secured. Issued keys or other entry devices are regularly inventoried.	Observe practices for safeguarding keys, badges, and other devices.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.7	Establish adequate interior security based on risk.	Entry codes are changed periodically.	Review documentation of entry code changes.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.8	Establish adequate interior security based on risk.	All deposits and withdrawals of storage media from the library are authorized and logged.	Review procedures for the removal and return of storage media to and from the library. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.9	Establish adequate interior security based on risk.	Documents/equipment are appropriately stored and are subject to maintenance and accountability procedures.	Examine and verify maintenance and accountability procedures for storage of documents and equipment.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.4.10	Establish adequate interior security based on risk.	Critical systems have emergency power supplies (for example, all alarm systems, monitoring devices, entry control systems, exit lighting, communication systems).	Verify that critical systems, (e.g., alarm systems, monitoring devices, entry control systems, exit lighting, and communication systems) have emergency power supplies. Identify back up systems and procedures and determine the frequency of testing. Review testing results.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.5.1	Adequately protect against emerging threats, based on risk.	Appropriate plans have been developed and controls implemented based on a risk assessment such as a shelter in place plan and/or evacuation plan for a potential CBR attack. A plan is in place and tested to respond to emerging threats such as a CBR attack (e.g. an appropriate shelter in place and/or evacuation plan).	Interview officials, review planning documents, and related test results. Observe and document the controls in place to mitigate emerging threats.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.5.2	Adequately protect against emerging threats, based on risk.	Outdoor areas such as air intakes, HVAC return air grilles, and roofs have been secured by restricting public access and relocating or protecting critical entry points (for example, air intake vents, protective grills, etc.).	Observe location of these devices and identify security measures that have been implemented.
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.5.3	Adequately protect against emerging threats, based on risk.	All outdoor air intakes are monitored by CCTV, security lighting, and/or intrusion detection sensors.	Verify that all outdoor air intakes are monitored by CCTV or other similar security.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.2 Access Controls (AC)	Critical Element AC-6: Establish adequate physical security controls	AC-6.5.4	Adequately protect against emerging threats, based on risk.	The ventilation and air filtration system has been evaluated for vulnerabilities to CBR agents and remedial action taken based on cost and risks.	Interview officials and review the results any evaluations.
3.3 Configuration Management (CM)	Critical Element CM-2: Maintain current configuration identification information	CM-2.1.2	Current configuration identification information is maintained.	Hardware, software, and firmware are mapped to application it supports.	Determine whether management has mapped the hardware, software and firmware to the application it supports.
3.3 Configuration Management (CM)	Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1	All configuration changes are properly managed (authorized, tested, approved, and tracked).	N/A	Where appropriate, these audit procedures should be applied to both internal and external developers and coordinated with section SM-7. (Ensure that activities performed by external third parties are adequately secure.)
3.3 Configuration Management (CM)	Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.3	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Relevant stakeholders have access to and knowledge of the configuration status of the configuration items.	Interview users and ensure that they have ready access to software change requests, test reports, and configuration items associated with the various baselines being managed.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.3 Configuration Management (CM)	Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.10	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Live data are not used in testing of program changes, except to build test data files.	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none"> • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of system failures (for example, bends) and, if so, whether they indicate inadequate testing before implementation.</p> <p>Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.</p>
3.3 Configuration Management (CM)	Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.18	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Configuration changes to network devices (for example, routers and firewalls) are properly controlled and documented.	Review a selection of configuration settings to key devices and determine if configuration changes are adequately controlled and documented.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.3 Configuration Management (CM)	Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	CM-3.1.19	All configuration changes are properly managed (authorized, tested, approved, and tracked).	Clear policies restricting the use of personal and public domain software and prohibiting violations of software licensing agreements have been developed and are enforced.	Review pertinent policies and procedures. Interview users and data processing staff. Review and test management enforcement process.
3.3 Configuration Management (CM)	Critical Element M-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.5	Software is promptly updated to protect against known vulnerabilities.	The entity: (1) establishes usage restrictions and implementation guidance for IPv6 technology based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of IPv6 within the information system. Appropriate organizational officials authorize the use of IPv6.	Review policies and procedures for IPv6 . Determine if known security vulnerabilities are mitigated by appropriate protective measures.
3.3 Configuration Management (CM)	Critical Element M-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.6	Software is promptly updated to protect against known vulnerabilities.	The entity: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.	Review policies and procedures for VoIP. Determine if security considerations in NIST SP 800-58 are used in the information system.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.3 Configuration Management (CM)	Critical Element M-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.7	Software is promptly updated to protect against known vulnerabilities.	Noncurrent software releases are adequately secure, given the risk.	Review pertinent policies and procedures. Interview users and data processing staff.
3.3 Configuration Management (CM)	Critical Element M-5: Update software on a timely basis to protect against known vulnerabilities	CM-5.1.8	Software is promptly updated to protect against known vulnerabilities.	Appropriate software usage controls (software restrictions, user-installed software) are implemented and exceptions are identified.	Assess the adequacy of software usage controls.
3.4 Segregation of Duties (SD)	Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.1.6	Incompatible duties have been identified and policies implemented to segregate these duties.	Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Review the adequacy of documented operating procedures for the data center.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.4 Segregation of Duties (SD)	Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.2.1	Job descriptions have been documented.	Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	<p>Review job descriptions for several positions in organizational units and for user security administrators.</p> <p>Determine whether duties are clearly described and prohibited activities are addressed.</p> <p>Review the effective dates of the position descriptions and determine whether they are current.</p> <p>Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.</p>
3.4 Segregation of Duties (SD)	Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.2.2	Job descriptions have been documented.	Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	Review job descriptions and interview management personnel to determine if all job positions have documented technical knowledge, skills, and ability requirements that can be used for hiring, promoting, and performance evaluations.
3.4 Segregation of Duties (SD)	Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.3.1	Employees understand their duties and responsibilities.	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	<p>Interview personnel filling positions for the selected job descriptions (see SD-1.2).</p> <p>Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.4 Segregation of Duties (SD)	Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.3.2	Employees understand their duties and responsibilities.	Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	Determine from interviewing personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
3.4 Segregation of Duties (SD)	Critical Element SD-1: Segregate incompatible duties and establish related policies	SD-1.3.3	Employees understand their duties and responsibilities.	Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	Interview management personnel in these activities.
3.4 Segregation of Duties (SD)	Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.1.1	Formal procedures guide personnel in performing their duties.	Detailed, written instructions exist and are followed for the performance of work.	Perform the following procedures for SD-2.1.1 to SD-2.1.3. Review manuals to determine whether formal procedures exist to guide personnel in performing their work. Interview supervisors and personnel. Observe processing activities.
3.4 Segregation of Duties (SD)	Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.1.2	Formal procedures guide personnel in performing their duties.	Instruction manuals provide guidance on system operation.	Perform the following procedures for SD-2.1.1 to SD-2.1.3. Review manuals to determine whether formal procedures exist to guide personnel in performing their work. Interview supervisors and personnel. Observe processing activities.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.4 Segregation of Duties (SD)	Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.1.3	Formal procedures guide personnel in performing their duties.	Application run manuals provide instruction operating specific applications.	Perform the following procedures for SD-2.1.1 to SD-2.1.3. Review manuals to determine whether formal procedures exist to guide personnel in performing their work. Interview supervisors and personnel. Observe processing activities.
3.4 Segregation of Duties (SD)	Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.2.1	Active supervision and review are provided for all personnel.	Personnel are provided adequate supervision and review, including each shift for computer operations.	Interview supervisors and personnel. Observe processing activities.
3.4 Segregation of Duties (SD)	Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	SD-2.2.4	Active supervision and review are provided for all personnel.	Staff performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	Interview management and subordinate personnel. Select documents or actions requiring supervisory review and approval for evidence of such performance (for example, approval of input of transactions, software changes).
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.1.2	Information system back up and recovery procedures have been implemented.	System and application documentation is maintained at the off-site storage location.	Locate and examine documentation.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.1.3	Information system back up and recovery procedures have been implemented.	The backup storage site is <ul style="list-style-type: none"> • geographically removed from the primary site (for example, not subject to the same hazards), and • protected by environmental controls and physical access controls. 	Examine the backup storage site. Determine if there are accessibility problems between the storage and processing sites in the event of an area wide disaster.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2	Adequate environmental controls have been implemented.	N/A	Audit procedures for CP-2.2 should be performed in conjunction with Section AC-6 regarding physical access controls. Perform the following procedures to determine whether control techniques CP-2.2.1 through 2.2.10 are achieved. <ul style="list-style-type: none"> • Examine the entity’s facilities. • Interview site managers.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.1	Adequate environmental controls have been implemented.	Fire detection and suppression devices have been installed and are working, for example, smoke detectors, fire extinguishers, and sprinkler systems.	Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency. Observe fire detection and suppression devices. Determine whether the activation of heat and smoke detectors will notify the fire department.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.2	Adequate environmental controls have been implemented.	Controls have been implemented to mitigate other disasters, such as floods, earthquakes, terrorism, etc.	Review the entity’s assessment of environmental risks and related controls.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.3	Adequate environmental controls have been implemented.	Redundancy exists in critical systems (for example, power and air cooling systems).	Observe the operation, location, maintenance, and access to critical systems.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.4	Adequate environmental controls have been implemented.	Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known.	Observe whether water can enter through the computer room ceiling or whether pipes are running through the facility and that there are water detectors on the floor.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.5	Adequate environmental controls have been implemented.	An uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shut down.	Observe power backup arrangements and results of testing.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.6	Adequate environmental controls have been implemented.	Humidity, temperature, and voltage are controlled within acceptable levels.	Determine whether humidity, temperature, and voltage are appropriately controlled.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.7	Adequate environmental controls have been implemented.	Emergency lighting activates in the event of a power outage and covers emergency exits and evacuation routes.	Observe that emergency lighting works and that power and other cabling is protected.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.8	Adequate environmental controls have been implemented.	A master power switch or emergency shut-off switch is present and appropriately located.	Observe power shut-off arrangements.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.9	Adequate environmental controls have been implemented.	Environmental controls are periodically tested at least annually for federal agencies.	Review test policies. Review documentation supporting recent tests of environmental controls and follow-up actions.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.2.10	Adequate environmental controls have been implemented.	Eating, drinking, and other behavior that may damage computer equipment is prohibited.	Review policies and procedures regarding employee behavior. Observe employee behavior.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.3.1	Staff have been trained to respond to emergencies.	Operational and support personnel have received training and understand their emergency roles and responsibilities.	Interview security personnel and appropriate operational and support staff and ensure that they understand their roles and responsibilities.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.3.2	Staff have been trained to respond to emergencies.	Personnel receive periodic environmental controls training including emergency fire, water, and alarm incident procedures.	Review training records and training course documentation. Determine whether all personnel have received up-to-date training and that the scope of the training is adequate.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.3.3	Staff have been trained to respond to emergencies.	Emergency response procedures are documented.	Review emergency response procedures for completeness and determine whether roles and responsibilities are clearly defined.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.3.4	Staff have been trained to respond to emergencies.	Emergency procedures are periodically tested.	Review test policies. Review test documentation. Interview operational and data center staff.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.1	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Policies and procedures exist and are up-to-date.	Review policies and procedures.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.2	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	Perform the following procedures to determine whether control techniques CP-2.4.2 through 2.4.4 are achieved. Interview information security, data processing, and user management. Review maintenance documentation. Determine when maintenance is performed, if it is in accordance with vendor specifications, and if there is minimal impact on system availability.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.3	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Regular and unscheduled maintenance performed is documented.	Perform the following procedures to determine whether control techniques CP-2.4.2 through 2.4.4 are achieved. Interview information security, data processing, and user management. Review maintenance documentation. Determine when maintenance is performed, if it is in accordance with vendor specifications, and if there is minimal impact on system availability.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.4	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	Perform the following procedures to determine whether control techniques CP-2.4.2 through 2.4.4 are achieved. Interview information security, data processing, and user management. Review maintenance documentation. Determine when maintenance is performed, if it is in accordance with vendor specifications, and if there is minimal impact on system availability.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.5	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interview information security and data center management.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.6	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Goals are established by senior management on the availability of data processing and on-line services.	<p>Perform the following procedures to determine whether control techniques CP-2.4.6 through 2.4.8 are achieved.</p> <p>Interview senior management, information security management, data processing management, and user management.</p> <p>Review supporting documentation, including system performance metrics.</p>
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.7	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Records are maintained on the actual performance in meeting service schedules.	<p>Perform the following procedures to determine whether control techniques CP-2.4.6 through 2.4.8 are achieved.</p> <p>Interview senior management, information security management, data processing management, and user management.</p> <p>Review supporting documentation, including system performance metrics.</p>
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.8	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	<p>Perform the following procedures to determine whether control techniques CP-2.4.6 through 2.4.8 are achieved.</p> <p>Interview senior management, information security management, data processing management, and user management.</p> <p>Review supporting documentation, including system performance metrics.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.9	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Senior management periodically reviews and compares the service performance achieved with the goals and surveys of user departments to see if their needs are being met.	Interview senior management, information security management, data processing management, and user management. Review supporting documentation such as user surveys, service goals, metric measuring system availability, service schedules, and test plans.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.10	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	For control techniques CP-2.4.10 and CP-2.4.11, review supporting documentation for scheduling of hardware changes, including staff notifications.
3.5 Contingency Planning (CP)	Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	CP-2.4.11	Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Advance notification of hardware changes and related software changes is given to users so that service is not unexpectedly interrupted.	For control techniques CP-2.4.10 and CP-2.4.11, review supporting documentation for scheduling of hardware changes, including staff notifications.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive	CP-3.1.1	An up-to-date contingency plan is documented.	A contingency plan has been documented that: <ul style="list-style-type: none"> • is based on clearly defined contingency planning policy; 	Review contingency planning policy and determine if it documents the entity's overall contingency objectives and establishes the organizational framework

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
	contingency plan			<ul style="list-style-type: none"> • reflects current conditions, including system interdependencies; • has been approved by key affected groups, including senior management, information security and data center management, and program managers; • clearly assigns responsibilities for recovery; • includes detailed instructions for restoring operations (both operating system and critical applications); • identifies the alternate processing facility and the back up storage facility; • includes procedures to follow when the data/service center is unable to receive or transmit data; • identifies critical data files; • is detailed enough to be understood by all entity managers; • includes computer and telecommunications hardware compatible with the entity’s needs; • includes necessary contact numbers; • includes appropriate system-recovery instructions; • has been distributed to all appropriate personnel; and • has been coordinated with related plans and activities. 	<p>and responsibilities for contingency planning.</p> <p>Obtain contingency plans (see NIST SP 800-34) and compare their provisions with the most recent risk assessment and with a current description of automated operations.</p> <p>Compare the contingency plans to security related plans, facility-level plans, and agency/entity level plans such as those in NIST contingency planning guidance.</p> <p>Determine if the contingency plans include:</p> <ul style="list-style-type: none"> • appropriate consideration of the technology, including alternative processing requirements, • recovery of the security infrastructure, and • interdependencies with other systems (i.e., other component, federal, state, or local agencies) that could affect the contingency operations.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.1.2	An up-to-date contingency plan is documented.	Contingency plans are reevaluated before proposed changes to the information system are approved to determine if major modifications have security ramifications that require operational changes in order to maintain adequate risk mitigation.	Interview senior management, information security management, and program managers.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.1.3	An up-to-date contingency plan is documented.	Procedures allow facility access in support of restoration of lost information under the contingency plans in the event of an emergency.	Determine whether emergency and temporary access authorizations are properly approved, documented, controlled, communicated, and automatically terminated after a predetermined period. These procedures should be performed in conjunction with Section AC-3.1.8 and AC- 6.1.8 regarding access controls.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.1.4	An up-to-date contingency plan is documented.	The plan provides for backup personnel so that it can be implemented independent of specific individuals.	Review the contingency plan.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.1.5	An up-to-date contingency plan is documented.	User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.	Interview senior management, information security management, and program managers.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.1.6	An up-to-date contingency plan is documented.	Several copies of the current contingency plan are securely stored off-site at different locations.	Observe copies of the contingency and related plans held off-site.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.1.7	An up-to-date contingency plan is documented.	The contingency plan is periodically reassessed and revised as appropriate. At a minimum, the plan is reassessed when there are significant changes in the entity mission, organization, business processes, and IT infrastructures (e.g., hardware, software, personnel).	Review the plan and any documentation supporting recent plan reassessments.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.2.1	Arrangements have been made for alternate data processing, storage, and telecommunications facilities.	Contracts or interentity agreements have been established for backup processing facilities that: <ul style="list-style-type: none"> • are in a state of readiness commensurate with the risks of interrupted operations, • have sufficient processing and storage capacity, and • are likely to be available for use. 	Interview officials and review contracts and agreements including processing priorities for the backup site. Determine if the back up site is properly configured and ready to be used as an operational site.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.2.2	Arrangements have been made for alternate data processing, storage, and telecommunications facilities.	Alternate network and telecommunication services have been arranged.	Interview officials and review contracts and agreements including the priority of service provisions for the backup service provider. Determine if the backup service provides separate failure points and is geographically removed from the primary provider.
3.5 Contingency Planning (CP)	Critical Element CP-3: Develop and document a comprehensive contingency plan	CP-3.2.3	Arrangements have been made for alternate data processing, storage, and telecommunications facilities.	Arrangements are planned for travel, lodging, and protection of necessary personnel, if needed.	Interview officials and review the plan.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
3.5 Contingency Planning (CP)	Critical Element CP-4: Periodically test the contingency plan and adjust it as appropriate	CP-4.1.1	The plan is periodically tested.	The contingency plan is periodically tested under conditions that simulate a disaster. Disaster scenarios tested may be rotated periodically. Typically, contingency plans are tested annually or as soon as possible after a significant change to the environment that would alter the assessed risk.	Review testing policies and methodology used to select disaster scenarios. Determine when and how often contingency plans are tested. Determine if technology is appropriately considered in periodic tests of the contingency plan and resulting adjustments to the plan. Review test results. Observe a disaster recovery test.
3.5 Contingency Planning (CP)	Critical Element CP-4: Periodically test the contingency plan and adjust it as appropriate	CP-4.2.1	Test results are analyzed and the contingency plan is adjusted accordingly.	Test results are documented and a report, such as a lessons learned report, is developed and provided to senior management.	Review final test report. Interview senior managers to determine if they are aware of the test results.
3.5 Contingency Planning (CP)	Critical Element CP-4: Periodically test the contingency plan and adjust it as appropriate	CP-4.2.2	Test results are analyzed and the contingency plan is adjusted accordingly.	The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.

C.1 APPLICATION CONTROLS – RELEVANT TO AUDIT READINESS

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.1.1	A comprehensive application security plan is in place.	<p>A comprehensive application security plan has been developed and documented. Topics covered include:</p> <ul style="list-style-type: none"> • Application identification and description; • Application risk level; • Application owner; • Person responsible for the security of the application; • Application interconnections/ information sharing; • A description of all of the controls in place or planned, including how the controls are implemented or planned to be implemented and special considerations; • Approach and procedures regarding security design and upgrade process; • Process for developing security roles; • General security administration policies, including ongoing security role maintenance and development; • Identification of sensitive transactions in each functional module; • Identification of high risk segregation of duty cases; • Roles and responsibilities of the security organization supporting the system with consideration to segregation of duties; • Security testing procedures; 	Inspect the application security plan to determine whether it adequately addresses all of the relevant topics.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
				<ul style="list-style-type: none"> • Coordination with entity-wide security policies; • Procedures for emergency access to the production system, including access to update programs in production, direct updates to the database, and modification of the system change option; • System parameter settings, compliant with entity-wide agency policies; • Access control procedures regarding the use of system delivered critical user IDs. 	
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.1.2	A comprehensive application security plan is in place.	Sensitive accounts are identified for each business process or sub-process, and appropriate security access privileges are defined and assigned.	Review the entity’s identification of sensitive transactions for the business process being audited for appropriateness and completeness. Observe and inspect procedures for identifying and assigning sensitive activities. Inspect authorizations for sensitive activities.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.1.3	A comprehensive application security plan is in place.	Access privileges are developed to prevent users from executing incompatible transactions within the application via menus or screens.	Through inquiry and inspection, determine whether the application security plan includes plans to identify segregation of duty conflicts in each of the business processes under assessment (master data and transaction data; data entry and reconciliation), and addresses controls to mitigate risks of allowing segregation of duty conflicts in a user’s role.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.2.1	Application security risk assessments and supporting activities are periodically performed.	<p>Security risks are assessed for the applications and supporting systems on a periodic basis or whenever applications or supporting systems significantly change.</p> <p>The risk assessments and validation, and related management approvals, are documented and maintained.</p> <p>The risk assessments are appropriately incorporated into the application security plan.</p>	<p>Obtain the most recent security risk assessment for each application under assessment. Inspect the risk assessments to determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by testing. Consider compliance with OMB, NIST, and other requirements/ guidance and whether technology and business processes are appropriately considered in the risk assessment.</p> <p>Obtain and inspect the relevant application security plan(s) to determine whether the risk assessments are appropriately incorporated into the application security plan.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.3.1	Policies and procedures are established to control and periodically assess the application.	Business process owners accept risks and approve the policies and procedures.	Determine through interview with entity management whether policies and procedures have been established to review access to the application.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.3.2	Policies and procedures are established to control and periodically assess the application.	<p>Policies and Procedures:</p> <ul style="list-style-type: none"> • are documented, • appropriately consider business process security needs, and • appropriately consider segregation of application user activity from the system administrator activity. 	Review policies and procedures to determine whether they have appropriately considered (1) business security needs and (2) segregation of application user activity from system administrator activity.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.5.2	Management monitors and periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	Security controls related to each major application are tested at least annually.	Inspect the overall testing strategy, a selection of test plans and related testing results. Determine if the scope of testing complies with OMB Circular A-123 Revised (federal entities) and other appropriate guidance. Determine if C&A testing is performed that complies with OMB and NIST requirements.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.6.1	Management effectively remediates information security weaknesses.	Management has a process in place to correct deficiencies.	Inquire of management and inspect security policies and procedures, including assessment and resolution plan.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.6.2	Management effectively remediates information security weaknesses.	Management initiates prompt action to correct deficiencies. Action plans and milestones are documented and complete.	Inspect recent FMFIA/A-123 and POA&M (or equivalent) reports for reasonableness of corrective actions (nature and timing). Determine whether application security control deficiencies (identified by the audit, by management testing, and by others) are included in the plans of action and milestones (or equivalent). and determine the status of corrective actions.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.6.3	Management effectively remediates information security weaknesses.	Deficiencies are analyzed by application (analysis may be extended to downstream, upstream, and other related applications), and appropriate corrective actions are applied.	Evaluate the scope and appropriateness of planned corrective actions through inquiry of management and inspection of evidence.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.6.4	Management effectively remediates information security weaknesses.	Corrective actions are tested after they have been implemented and monitored on a continuing basis.	Inspect documentation to determine if implemented corrective actions have been tested and monitored periodically.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.7.1	External third party provider activities are secure, documented, and monitored.	<p>Policies and procedures concerning activities of third party providers are developed and include provisions for:</p> <ul style="list-style-type: none"> • Application compliance with entity’s security requirements, and • Monitoring of compliance with regulatory requirements 	<p>Inspect policies and procedures pertaining to external parties for the application under assessment.</p> <p>Inspect documentation to determine whether the external third party provider’s need to access the application is appropriately defined and documented.</p> <p>Review contracts with third-party providers to determine compliance with the Privacy Act, where applicable.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.1.1	Application boundaries are adequately protected.	<p>Application boundaries are identified in security plans.</p> <p>Application boundaries are adequately secure.</p>	<p>Review security plans for proper identification of application boundaries.</p> <p>Evaluate the effectiveness of controls over application boundaries.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.2	Application users are appropriately identified and authenticated.	<p>Identification and authentication is unique to each user.</p> <p>All approved users should enter their user ID (unique) and password (or other authentication) to gain access to the application.</p>	<p>Inspect pertinent policies and procedures, and NIST guidance for authenticating user IDs.</p> <p>Through inquiry, observation or inspection, determine the method of user authentication used (password, token, biometrics, etc.).</p> <p>If a password system is used, gain understanding of the specific information and evaluate its appropriateness, including application security authentication parameters, inspection of system reports or observation of the system, including appropriate testing. See AC-2 for more information on criteria for evaluating password policies.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.3.1	Security policies and procedures appropriately address ID and password management.	<p>The entity has formal procedures and processes for granting users access to the application. The entity's IT security policies and procedures contain guidance for:</p> <ul style="list-style-type: none"> • Assigning passwords; • Changing and resetting passwords; and • Handling lost or compromised passwords 	<p>Through inquiry, observation, and inspection, understand and assess procedures used by the entity for application password management:</p> <ul style="list-style-type: none"> • Procedures for initial password assignment, including the password parameters; • Procedures for password changes, including initial password change; • Procedures for handling lost passwords (password resetting); and • Procedures for handling password compromise.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.3.2	Security policies and procedures appropriately address ID and password management.	<p>The application locks the user’s account after a pre-determined number of attempts to log-on with an invalid password. The application may automatically reset the user account after a specific time period (an hour or a day), or may require an administrator to reset the account.</p> <p>If the user is away from his/her workspace for a preset amount of time, or the user's session is inactive, the application automatically logs off the user’s account.</p>	<p>After obtaining an understanding of the user authentication process, inspect and/or observe the following:</p> <ul style="list-style-type: none"> • Whether access to the application is permitted only after the user enters their user ID and password. • Observe a user executing invalid logins and describe the actions taken. <p>Either 1) inspect system security settings, or 2) observe an idle user workspace to determine whether the application logs the user off after an elapsed period of idle time.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.4.1	Access to the application is restricted to authorized users.	Before a user obtains a user account and password for the application, the user’s level of access has been authorized by a manager and the application administrator.	Review policies and procedures. From a selection of user accounts determine whether the user level of access was authorized by appropriate entity management.
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.4.2	Access to the application is restricted to authorized users.	Owners periodically review access to ensure continued appropriateness.	Interview security administrators and inspect evidence of the effectiveness of periodic review of access by owners.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.4.3	Access to the application is restricted to authorized users.	Access is limited to individuals with a valid business purpose (least privilege).	<p>Interview owners and inspect documentation, to determine whether appropriate procedures are in place remove or modify application access, as needed.</p> <p>Through inquiry, observation, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how.</p> <p>Based on the selection of users in AS-2.4.1 above, determine whether the user access is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.5.1	Public access is controlled. (Based on an entity’s business mission, the entity may allow the public to have access to the application).	The entity implements a security plan and process for 1) identification and authorization of users; 2) access controls for limited user privileges; 3) use of digital signatures; 4) prohibition of direct access by the public to production data; and 5) compliance with NIST guidance.	<p>Obtain an understanding of the following controls through inquiry of the application owner, inspection of source documents, and/or observation of the following:</p> <ul style="list-style-type: none"> • Identification and authentication; • Access controls for limiting user privileges(read, write, modify, delete); • Use of digital signatures; • Prohibition of direct access by the public to live databases and restricted/sensitive records; and Legal considerations (i.e., privacy laws, OMB, NIST, etc.).

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.6.1	User access to sensitive transactions or activities is appropriately controlled.	Owners have identified sensitive transactions or activities for the business process.	Inquire of responsible personnel and inspect pertinent policies and procedures covering segregation of application duties.
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.6.2	User access to sensitive transactions or activities is appropriately controlled.	Owners authorize users to have access to sensitive transactions or activities.	<p>Determine whether the process owners have identified a list of sensitive transactions or activities for their area.</p> <p>Inspect the user administration procedures to determine whether they include a requirement for the process owner to approve access to transactions or activities in their area of responsibility.</p> <p>Through inquiry and inspection, determine whether user access is authorized by process owners.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.6.3	User access to sensitive transactions or activities is appropriately controlled.	Security Administrators review application user access authorizations for access to sensitive transactions and discuss any questionable authorizations with owners.	<p>Select user access request forms or other authorization documents [can use selection from AS-2.4.1 and AS-2.4.3] and inspect them to determine whether the process owners have approved user access to appropriate transactions or activities.</p> <p>Interview security administrators and inspect user access authorization procedures to determine whether access to sensitive transactions require approval by the process owner.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.6.4	User access to sensitive transactions or activities is appropriately controlled.	Owners periodically review access to sensitive transactions and activities to ensure continued appropriateness.	Inspect evidence of periodic review by owners of access to sensitive transactions.
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.6.5	User access to sensitive transactions or activities is appropriately controlled.	Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters and review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees and, for a selection, determine whether system access was promptly terminated.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.6.6	User access to sensitive transactions or activities is appropriately controlled.	Access to sensitive transactions is limited to individuals with a valid business purpose (least privilege).	<p>Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed.</p> <p>Through inquiry, observations, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how.</p> <p>Obtain a list of users with access to identified sensitive transactions for the business process under assessment. Inspect the list to determine whether the number of users having access to sensitive transactions/ activities is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.7.1	Sensitive application resources are adequately protected.	<p>The entity identifies sensitive application resources.</p> <p>Access to sensitive application resources restricted to appropriate users.</p> <p>Sensitive application data is encrypted, where appropriate.</p>	<p>Evaluate the completeness of sensitive application resources identified.</p> <p>Assess the adequacy of IS controls over sensitive application resources.</p> <p>Review implementation of encryption of sensitive application data, where appropriate.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.8.1	An effective access audit and monitoring program is in place, documented, and approved.	Policies and procedures are established to reasonably assure that application security audit and monitoring is effective.	<p>Inspect documented policies and procedures for application security administration for each application in scope</p> <p>Determine whether the monitoring program has built-in procedures to identify inappropriate user assignments.</p> <p>Through inquiry and inspection, determine whether monitoring procedures are performed on a regular basis.</p> <p>Determine whether the exceptions are handled appropriately and in a timely manner.</p>
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.9.1	Application security violations are identified in a timely manner.	Logging and other parameters are appropriately set up to notify of security violations as they occur.	Observe and inspect application logging and other parameters that identify security violations and exceptions. (For example, parameter set up indicates whether or not users can logon to an application more than once).
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.10.1	Exceptions and violations are properly analyzed and appropriate actions taken.	<p>Reportable exceptions and violations are identified and logged.</p> <p>Exception reports are generated and reviewed by security administration.</p> <p>If an exception occurs, specific action is taken based upon the nature of exception.</p>	<p>Observe and inspect management’s monitoring of security violations, such as unauthorized user access.</p> <p>Inspect reports that identify security violations. Through inquiry and inspection, note management’s action taken.</p> <p>Inspect reports of authorized segregation of duty conflicts sensitive process access; Assess business level authorization and monitoring, if applicable.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.1.1	Policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly.	Appropriate policies and procedures are established for application configuration management.	<p>Inspect documented policies and procedures related to application change control procedures.</p> <p>Through inquiry and inspection, identify key transactions that provide user access to change application functionality.</p> <p>Inspect transaction reports of changes made to the application. From a selection of changes, inspect documentation of the changes made, including the validity, reasons, authorization, and the user authority. Note the handling of exceptions.</p>
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.3.1	A system development life cycle methodology has been implemented.	<p>A SDLC methodology has been developed that:</p> <ul style="list-style-type: none"> • provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, • is sufficiently documented to provide guidance to staff with varying levels of skill and experience, • provides a means of controlling changes in requirements that occur over the system life, and • includes documentation requirements. 	<p>Review SDLC methodology.</p> <p>Review system documentation to verify that SDLC methodology was followed.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.4.1	Authorizations for changes are documented and maintained.	Change request forms are used to document requests and related projects.	Identify recent software modification and determine whether change request forms were used.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.4.2	Authorizations for changes are documented and maintained.	Change requests must be approved by both system users and IT staff.	Examine a selection of software change request forms for approval.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.1	Changes are controlled as programs progress through testing to final approval.	Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysis, programmers, auditors, quality assurance, library control).	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X- Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.2	Changes are controlled as programs progress through testing to final approval.	Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS- 3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.3	Changes are controlled as programs progress through testing to final approval.	Software changes are documented so that they can be traced from authorization to the final approved code.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.4	Changes are controlled as programs progress through testing to final approval.	Test plans are documented and approved that define responsibilities for each party involved.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.5	Changes are controlled as programs progress through testing to final approval.	Unit, integration, and system testing are performed and approved: <ul style="list-style-type: none"> • in accordance with the test plan and • applying a sufficient range of valid and invalid conditions. 	Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved. Review test plan standards. Examine a selection of recent software changes and: <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.6	Changes are controlled as programs progress through testing to final approval.	A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS 3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.7	Changes are controlled as programs progress through testing to final approval.	Test results are reviewed and documented.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS 3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.5.8	Changes are controlled as programs progress through testing to final approval.	Program changes are moved into production only upon documented approval from users and system development management.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS 3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and:</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.6.1	Access to program libraries is restricted.	Separate libraries are maintained for program development and maintenance, testing, and production programs.	Examine libraries to determine whether separate libraries are used for development and maintenance, testing, and production.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.6.2	Access to program libraries is restricted.	Source code is maintained in a separate library.	Verify source code exists for a selection of production code modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load module size.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.6.3	Access to program libraries is restricted.	Access to all programs, including production code, source code, and extra program copies are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.7.1	Movement of programs and data among libraries is controlled.	A group independent of the user and programmers control movement of programs and data among libraries. Before and after images of program code are maintained and compared to ensure that only approved changes are made.	Review pertinent policies and procedures. For a selection of program changes, examine related documentation to verify that: <ul style="list-style-type: none"> procedures for authorizing movement among libraries were followed, and before and after images were compared.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.8.1	Access to application activities/ transactions is controlled via user roles (access privileges).	User accounts are assigned to a role in the application. Roles are designed and approved by management to provide appropriate access and prevent an unauthorized user from executing critical transactions in production that change application functionality.	Inspect system reports and identify users who have access to configuration transactions. For a selection of users identified above, inspect user authorization forms to determine whether the user's access was authorized.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.9.1	Access to all application programs/codes and tables are controlled.	AS-3.9.1 Changes to application programs, codes and tables are either restricted or denied in the production environment. All changes are made using the approved change control process. User access to the application programs, codes, and tables is provided only for emergency user IDs.	<p>Through inquiry and inspection, identify key programs and tables for the application.</p> <p>Inspect system reports of users with access to the key programs, codes and tables. Select users that have access to the identified programs and tables.</p> <p>Inspect documentation supporting how the access was provided. Note exceptions.</p>
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.10 .1	Access to administration (system) transactions that provide access to table maintenance and program execution is limited to key users.	Security design includes consideration for sensitive administration (system) transactions and restricted user access to these transactions.	<p>Inspect policies and procedures regarding restricted access to system administration transactions.</p> <p>Through inquiry and inspection, identify the system administration transactions.</p> <p>Inspect system reports of user access to these transactions.</p> <p>Select users with administration access and inspect documentation to determine whether access was authorized.</p> <p>Select system administration transactions executed by the system users and inspect resulting changes to the system elements, such as the program code or table.</p> <p>Inspect critical or privileged IDs (e.g., fire call ID) to determine if activity is logged.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.11.1	Access and changes to programs and data are monitored.	Procedures are established to reasonably assure that key program and table changes are monitored by a responsible individual who does not have the change authority. The procedures provide the details of reports/logs to run, specific valuation criteria and frequency of the assessment.	Inspect documented procedures related to monitoring change control. Select reports or logs that are reviewed, and inspect to note evidence of monitoring compliance.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.12.1	Changes are assessed periodically.	Periodic assessment of compliance with change management process, and changes to configurable objects and programs.	Inspect evidence of documented assessments performed. Determine who performed the assessment and note the exception handling procedures.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.13.1	Applications are updated on a timely manner to protect against known vulnerabilities.	The entity follows an effective process to identify vulnerabilities in applications and update them.	Determine whether vendor supplied updates have been implemented. Assess management's process for identifying vulnerabilities and updating applications.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-3.14.1	Emergency application changes are properly documented, tested, and approved.	The entity follows an effective process to properly document, test, and approve emergency changes.	Inspect evidence of proper documentation, testing, and approval of emergency changes.
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-4.1.1	Incompatible activities and transactions are identified.	Owners have identified incompatible activities and transactions, and documented them on a segregation of duty matrix.	Through inquiry of management and inspection of policies and procedures, understand how management identifies incompatible activities and transactions.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	AS-3. Implement Effective Application Configuration Management.	AS-4.1.2	Incompatible activities and transactions are identified.	Owners have appropriately considered risk acceptance when allowing segregation of duty conflicts in user roles.	Inspect list of segregation of duty conflicts to determine whether management has identified the segregation of duty conflicts appropriate for the business process and considered risk acceptance when allowing the conflicts.
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.2.1	Application controls prevent users from performing incompatible duties.	Users are prevented by the application from executing incompatible transactions, as authorized by the business owners.	<p>Through inquiry, observations, and inspection, determine how the application segregates users from performing incompatible duties.</p> <p>Obtain and inspect a listing of users with access to the application. For a selection of users (can use same selection as in AS-2.4.1, AS-2.4.3 & AS-2.6.3), inspect documentation to determine whether access to menus/screens corresponds with the user's defined duties. Evaluate whether their duties and access is appropriate to prevent employees from performing incompatible duties.</p> <p>Specifically, perform the following steps:</p> <ul style="list-style-type: none"> • Obtain a system-generated user listing for the application (and other applications, if applicable); • For a selection of users, inspect their access profiles to determine whether access is appropriate (e.g., users have update access); and • For the selection of users, inspect their access profiles to determine if any of the users have access to menus with conflicting duties.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.3.1	There is effective segregation of duties between the security administration function of the application and the user functions.	The profiles for security administrators do not have privileges to input and/or approve transactions.	Based on the inspection of user profiles, determine if: <ul style="list-style-type: none"> • individuals with security administration functions have access to input, process, or approve transactions; • security administrators have access to more than application security administration functions; and • security administrators are prevented from accessing production data.
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.4.1	User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.	Owners authorize users to have access to transactions or activities that cause segregation of duty conflicts only when supported by a business need.	Inspect user administration policy to determine whether owner approval is required to access transactions or activities in their area of responsibility. Obtain and inspect a system report of users with conflicting responsibilities within the application. From a selection of user access request forms (electronic documents/workflow, if applicable) verify that the owners have approved user access to appropriate transactions or activities.
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.4.2	User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.	Security Administrators review application user access authorizations for segregation of duties conflicts and discuss any questionable authorizations with owners.	Interview security administrators and observe and inspect relevant procedures and documentation. If the security administrator's review is documented on the request form, inspect a selection of forms to note evidence of the security administrator's review.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.4.3	User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.	Owners periodically review access to identify unauthorized segregation of duties conflicts and determine whether any authorized segregation of duties conflicts remain appropriate.	Interview owners and inspect documentation; determine whether appropriate procedures are in place identify and remove or modify access, as needed.
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.5.1	Effective monitoring controls are in place to mitigate segregation of duty risks.	Process Owner has identified the segregation of duty conflicts that can exist, and the roles and users with conflicts.	Inspect documentation of roles and users with conflicts.
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.5.2	Effective monitoring controls are in place to mitigate segregation of duty risks.	Documented monitoring controls are in place that specifically address the conflict that the control mitigates.	Identify segregation of duty conflicts (including those that were intentionally established by the entity) and review documentation to determine whether: <ul style="list-style-type: none"> • monitoring controls adequately mitigate the risks created by the segregation of duty conflict; and • monitoring controls are effective. This can be achieved by inspecting the evidence collected by management.
4.1 Application Level General Controls (AS)	Critical Element AS-4: Segregate user access to conflicting transactions and activities and monitor segregation.	AS-4.5.3	Effective monitoring controls are in place to mitigate segregation of duty risks.	Management has documented evidence of monitoring of control effectiveness.	Review evidence of monitoring of control effectiveness.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.1.1	Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.	Determine the critical functions performed by the application and identify the IT resources, including key data and programs, required to perform them.	Perform the following procedures for AS-5.1.1 to AS-5.1.3. Review the policies and methodology, and the BIA (if conducted) used to determine the application’s critical functions and supporting IT resources, the outage impacts and allowable outage times, and the recovery priorities. Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of the results.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.1.3	Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.	Develop recovery priorities that will help determine recovery strategies.	Perform the following procedures for AS-5.1.1 to AS-5.1.3. Review the policies and methodology, and the BIA (if conducted) used to determine the application’s critical functions and supporting IT resources, the outage impacts and allowable outage times, and the recovery priorities. Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of the results.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.2.1	Take steps to prevent and minimize potential damage and interruption.	Backup files of key application data are created on a prescribed basis.	Review written policies and procedures for backing up and storing application data and programs.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.2.2	Take steps to prevent and minimize potential damage and interruption.	Current application programs are copied and available for use.	Examine the backup storage site.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.2.3	Take steps to prevent and minimize potential damage and interruption.	Backup files of application data and programs are securely stored offsite and retrievable for contingency plan implementation.	Interview program and information technology officials and determine their assessment of the adequacy of backup policy and procedures.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.3.1	Develop and document an application Contingency Plan.	Develop a time-based application Contingency Plan.	Review the application contingency plan and broader scoped related plans.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.3.2	Develop and document an application Contingency Plan.	Incorporate the application Contingency Plan into related plans, such as the Disaster Recovery, Business Continuity, and Business Resumption Plans.	Determine whether the broader-scoped plans have incorporated the application contingency plan. Compare the plan with guidance provided in NIST SP 800-34 . Interview program, information technology, and security administration officials and determine their input and assessment of the reasonableness of the plan.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.3.3	Develop and document an application Contingency Plan.	Contingency operations provide for an effective control environment by restricting and monitoring user access to application data and programs, including: <ul style="list-style-type: none"> • Users are identified and authenticated; • Users are properly authorized before being able to perform sensitive transactions; • Audit and monitoring capabilities are operating. 	Interview program, information technology, and security administration officials. Determine their assessment for providing an effective control environment during contingency operations. Review the contingency plan and any test results for control related issues.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.4.1	Periodically test the application contingency plan and adjust it as appropriate.	The application contingency plan is periodically tested and test conditions include disaster simulations.	Review policies on testing. Determine when and how often contingency plans are tested.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.4.2	Periodically test the application contingency plan and adjust it as appropriate.	The following areas are included in the contingency test: <ul style="list-style-type: none"> • System recovery on an alternate platform from backup media; • Coordination among recovery teams; • Internal and external connectivity; • System performance using alternate equipment; • Restoration of normal operations; • Notification procedures. 	Determine if technology is appropriately considered in periodic tests of the contingency plan and resultant adjustments to the plan. Review test results. Observe a disaster recovery test.
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency	AS-5.4.3	Periodically test the application contingency plan and adjust it as appropriate.	Test results are documented and a report, such as a lessons-learned report, is developed and provided to senior management.	Review the final test report. Interview senior management to determine whether they are aware of the test results.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
	planning.				
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.4.4	Periodically test the application contingency plan and adjust it as appropriate.	The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.1.1	A transaction data strategy is properly defined, documented, and appropriate.	Data management procedures exist that include transaction data strategy, data design, data definitions, data quality standards, ownership and monitoring procedures. Data strategy should be unique to each data type.	Inquire of management and inspect documented policies and procedures related to data strategy. Inspect transaction data strategy.
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.2.1	Source documentation and input file data collection and input preparation and entry is effectively controlled.	Procedures are established to provide reasonable assurance that all inputs into the application have been authorized, accepted for processing, and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. Such procedures may include one or more of the following: <ul style="list-style-type: none"> • batch totals; • sequence checking; • reconciliations; • control totals. 	Through inquiry, observations, and inspection, obtain an understanding of policies and procedures related to source document and input file collection and preparation, and determine whether the procedures are documented and properly designed. Observe and inspect input preparation policies and procedures and relevant controls, noting procedures taken when exceptions are identified. Inspect a selection of reports used by management to determine whether the necessary inputs are accepted for processing, and inquire of review procedures used. Inquire as to how source documents and input files are tracked and maintained and inspect relevant documentation.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.3.1	Access to data input is adequately controlled.	Procedures are implemented to control access to application input routines and physical input media (blank and completed).	Review procedures over control of data input to determine whether they are adequate. Coordinate this step with AS-2.
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.4.1	Input data are approved.	Documented approval procedures exist to validate input data before entering the system. Approval procedures are followed for data input.	Inspect documented procedures for approval of input data. Inspect a selection of source documents and input files and determine whether the source data were approved for input.
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.5.1	Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.	Appropriate edits are used to reasonably assure that data are valid and recorded in the proper format, including: <ul style="list-style-type: none"> • authorization or approval codes; • field format controls; • required field controls; • limit and reasonableness controls; • valid combination of related data field values; • range checks • mathematical accuracy • master file matching • duplicate processing controls; and • balancing controls. 	Through inquiry, observations, and inspection, understand edits used to reasonably assure that input data is accurate, valid, and in the proper format prior to being accepted by the application. The edits and procedures should address both manual and automated input processes. Identify the key data input screens. Consider such factors as known errors and the frequency of use. If available, use analytical reports to support reasoning for screen selection. For the key manual input layouts identified, perform the following steps as applicable: <ul style="list-style-type: none"> • Observe an authorized data entry clerk inputting transactions, noting edits and validations for the various transaction entries. • Observe key transaction fields to determine whether they have

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
					<p>adequate edit/validation controls over data input.</p> <ul style="list-style-type: none"> Obtain screen prints of appropriate scenarios and document the result. <p>For key automated inputs, observe and inspect data validation processes, completion controls, and exception reports in place. Inquire of management regarding procedures used to reject and resubmit data for processing, and procedures to provide reasonable assurance that data is not processed multiple times. Note: audit procedures apply only to the current environment at the time of test. Supplemental audit procedures would need to be applied at other points during the year to obtain evidence that the control was operating effectively.)</p>
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.5.2	Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.	Edit and validation overrides are restricted to authorized personnel. Procedures exist to monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow up of overrides is performed. Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.5.3	Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.	Table maintenance procedures include edit and validation controls to help assure that only valid changes are made to data tables.	Through inquiry, observations, and inspection, obtain an understanding of table maintenance procedures relative to data edits and validation. Observe an authorized person attempting to make invalid changes to tables, and confirm edits and validations are performed on changes.
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.6.1	Input values to data fields that do not fall within the tolerances or parameters determined by the management result in an automated input warning or error.	Parameters and tolerances are configured and error conditions and messages are defined. (These restrictions can be configured based on limits on transaction amounts or based on the nature of transactions) If a workflow is used so that documents can be released only by personnel with appropriate approval authority, then these requirements should be appropriately designed in the system. Management regularly reviews the restrictions placed on data input and validates that they are accurate and appropriate.	Inspect configuration of parameters and tolerance levels defined by the entity to identify whether the application accepts the data with warning or rejects the data, if the conditions are not met. Determine whether management review and follow-up of warnings are adequate. Inspect the workflow rules and validate that the releasing authority is at an appropriate level. Inspect evidence of management's regular review of relevant tolerances and parameters, and any correctional activities taken.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.7.1	Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected.	Procedures are established to reasonably assure that all inputs into the application have been accepted for processing and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. The procedures specifically require the exceptions to be resolved within a specific time period.	Inspect documented procedures related to data entry error handling procedures. Inquire of management to determine which key management reports are used to monitor input errors. Select input error reports and inspect to note evidence of management review. As applicable, inspect subsequent data input reports to note where data was corrected and resubmitted for processing.
4.2 Business Process Controls (BP)	Critical Element BP-1: Transaction Data Input is complete, accurate, valid, and confidential.	BP-1.8.1	Errors are investigated and resubmitted for processing promptly and accurately.	Data input errors are identified in suspense or error reports and resolved or resubmitted in a timely manner (within the period specified in the procedures).	Inspect a selection of recent suspense or error reports (can use selection used in BP-1.7.1 provided information included will satisfy audit objectives for both audit procedures) and note whether suspense items are being corrected in a timely manner. Inspect the open items and note management's reasons for not correcting them in a timely manner.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.1.1	Application functionality is designed to process input data, with minimal manual intervention.	Application processing of input data is automated and standardized. Design documentation supporting the processing design exists for validation and change control purposes. The version of application, data and files to be processed are appropriate and current.	Inspect configuration and/or design documentation noting automatic and manual processing of transaction and information flow. Verify that proper versions of application, data and file are used.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.2.1	Processing errors are identified, logged and resolved.	System entries use transaction logs to reasonably assure that all transactions are properly processed and identify the transactions that were not completely processed.	Inspect a selection of application, transaction and error logs, noting whether all transactions were properly processed and missing or duplicate transactions were identified, including reruns and restarts.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.2.2	Processing errors are identified, logged and resolved.	Procedures are in place to identify and review the incomplete execution of transactions, analyze and take appropriate action.	Inspect selected incomplete transactions and validate that management has adequately investigated and corrected the errors or omissions. Conduct a test with controlled group of live data and analyze the results with the expected values. Follow up with any exceptions.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.2.3	Processing errors are identified, logged and resolved.	Procedures exist to monitor, in a timely manner, overrides applied to transaction processing.	Observe and inspect existing procedures for reviewer overrides or bypassing data processing routines. If an override log exists, observe and inspect to determine whether adequate review and follow up of overrides is performed. Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.3.1	Transactions are executed in accordance with the predetermined parameters and tolerances, specific to entity's risk management.	Document processing and posting conditions (parameters and tolerances) are configured, including system errors and actions, if the conditions are not met.	Inspect configuration of parameters and tolerances levels defined by the entity to identify whether the application processes the data with warning or rejects the data, if the conditions are not met.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.3.2	Transactions are executed in accordance with the predetermined parameters and tolerances, specific to entity's risk management.	Management regularly reviews the restrictions to validate the accuracy and appropriateness.	Inspect management review procedures, noting management action when the application processes data or rejects it. In both cases, management should clearly analyze the impact on the downstream transactions.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.4.1	Transactions are valid and are unique (not duplicated).	The application performs on-line edit and validation checks against data being processed.	Perform the following procedures for BP-2.4.1 to BP-2.4.4. Inspect design document to identify key data validation and edit checks. Inspect configuration to verify that the identified edit and validations checks are appropriately set, and transactions are rejected/suspended when data/processing errors occur. Also verify that warning and error messages are designed when the processing is incomplete.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.4.3	Transactions are valid and are unique (not duplicated).	Transactions with errors are rejected or suspended from processing until the error is corrected.	Perform the following procedures for BP-2.4.1 to BP-2.4.4. Inspect design document to identify key data validation and edit checks. Inspect configuration to verify that the identified edit and validations checks are appropriately set, and transactions are rejected/suspended when data/processing errors occur. Also verify that warning and error messages are designed when the processing is incomplete.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.4.4	Transactions are valid and are unique (not duplicated).	The application communicates the processing error to the users either on-line (if on-line entry) or via an exception report.	Inspect the error communication methodology and assess whether all processing errors are communicated to the users.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.5.1	The transactions appropriately authorized.	Transactions are matched with management's general or specific authorizations.	Review the adequacy of controls over authorization of transactions.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.6.1	Data from subsidiary ledgers are in balance with the general ledger (step applicable to financial-related audits only).	Periodic reconciliation is performed and exceptions are appropriately handled.	Inspect periodic procedures to determine whether reconciliations are performed and documented with evidence. For a selection of reconciliations, examine supporting evidence for adequacy. Through inquiry, observations, and inspection, determine if the system is configured to auto balance, where possible.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.7.1	User-defined processing is adequately controlled.	Appropriate policies and procedures over user-defined processing are implemented.	Review policies and procedures over user-defined processing.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.7.2	User-defined processing is adequately controlled.	Controls over user-defined processing are adequate.	Assess the operating effectiveness of user-defined processing.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.9.1	An adequate audit and monitoring capability is implemented.	Management has procedures in place to reconcile the data input with the data processed by the application.	Inspect procedures regarding reconciliation of transactions.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.9.2	An adequate audit and monitoring capability is implemented.	Monitoring procedures should provide details of data to be added/modified during the processing, and expected result. System audit logs should be reviewed for exception.	Inspect operations activity at selected times and check for evidence that reconciliations are being performed.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.9.3	An adequate audit and monitoring capability is implemented.	Management maintains a process log and the log is reviewed for unusual or unauthorized activity.	Inspect the processing log and note whether the unusual or unauthorized activity was followed up properly and promptly.
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.9.4	An adequate audit and monitoring capability is implemented.	Procedures exist to monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.2.1	Output generation and distribution are aligned with the reporting strategy.	Management has procedures place to reasonably assure that content availability of output and data are consistent with end users' needs, sensitivity, laws regulations, and confidentiality of data and valid user access.	Inspect management procedures for defining and assigning output/reports. Select key output/reports in the area of audit scope and verify the user access to the output/reports.
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.2.3	Output generation and distribution are aligned with the reporting strategy.	User access to output data aligned with the user's role and confidentiality/sensitivity of information.	Review user access to selected output data and assess the appropriateness of access.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.3.1	System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.	Management has identified reports to track processing results.	<p>Perform the following procedures for BP-3.3.1 to BP-3.3.3.</p> <p>Inquire of user management and personnel to determine the key reports used to track processing results.</p> <p>Obtain and inspect reports identified by management in the above test to determine whether the reports exist and are reviewed on a timely basis.</p> <p>Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.</p>
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.3.2	System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.	Management has documented procedures to (1) review processed results, where applicable and (2) monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	<p>Perform the following procedures for BP-3.3.1 to BP-3.3.3.</p> <p>Inquire of user management and personnel to determine the key reports used to track processing results.</p> <p>Obtain and inspect reports identified by management in the above test to determine whether the reports exist and are reviewed on a timely basis.</p> <p>Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.3.3	System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.	Procedures are in place to review critical output data or control reports on a timely basis.	<p>Perform the following procedures for BP-3.3.1 to BP-3.3.3.</p> <p>Inquire of user management and personnel to determine the key reports used to track processing results.</p> <p>Obtain and inspect reports identified by management in the above test to determine whether the reports exist and are reviewed on a timely basis.</p> <p>Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.</p>
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.4.1	Output/ reports are in compliance with applicable laws and regulations.	Output reports for compliance with applicable laws and regulations are accurate, complete.	<p>Inspect a selection of output/reports for compliance with applicable laws and regulations.</p> <p>Identify laws and regulations that are to be complied with and verify that the reports are in compliance.</p>
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.1.1	Master data are appropriately designed.	An entry is required in all key fields, such as address and account number.	Inspect master data configuration for required field values.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.1.2	Master data are appropriately designed.	Null values or invalid values are not accepted in the required fields.	Observe user input of invalid values, or blank values, and note any exceptions.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.1.3	Master data are appropriately designed.	For financial applications, account assignments (asset, liability, income and expense) are accurately defined.	Inspect master data configuration for account groups and assignments.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.2.1	Changes to master data configuration are appropriately controlled.	Policies and procedures are established for master data configuration management, which include change rules that identify data fields that are excluded from changes (for example, master data number).	Review the master data policies and procedures for change management.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.2.2	Changes to master data configuration are appropriately controlled.	Changes to the master data design are approved by appropriate personnel.	Inspect a selection of change requests and verify that appropriate approvals are obtained. Inspect master data configuration for change rules, if the rules are configured. If the change rules are automatic, then the user should be prevented from making unauthorized configuration changes.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.2.3	Changes to master data configuration are appropriately controlled.	Changes to the master data records should be limited to non-key fields.	Inspect a selection of master data change reports and verify that changes are limited to management defined non-key fields.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.3.1	Only valid master records exist.	Master data is reviewed on a regular basis, duplicates are identified and removed or blocked, and unused data is identified and blocked.	<p>Inquire of management regarding their master data review procedures.</p> <p>Inspect policies and procedures on master data review, including duplicate master data entry and resolution, and unused master records.</p> <p>Inspect evidence of the most recent management review and action.</p> <p>Inspect list of accounts/records blocked for posting or use.</p> <p>Inspect duplicate master record report and management's use of it.</p>
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.3.2	Only valid master records exist.	Automatic application controls (duplicate checks, system warnings) are configured to prevent and/or identify potential duplicate master records.	Inspect application configuration for automatic controls and determine whether the controls prevent erroneous processing or simply warn of potential errors.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.4.1	Master data are complete and valid.	<p>Policies and procedures for master data maintenance are documented and include:</p> <ul style="list-style-type: none"> • approval requirements; • data quality criteria; • data owner; • supporting documents; • backup procedures in the event of a disaster or data corruption error; • Archival policies. 	<p>Inspect master data maintenance policies and procedures for appropriateness.</p> <p>Inquire of responsible personnel.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.4.2	Master data are complete and valid.	The master data maintenance process includes a formal create/change request from the requestor and approval from the data owner.	Select master data created or changed, and inspect relevant documentation, noting appropriate approvals and compliance with policies and procedures. Obtain system report of users with master data maintenance access. For a selection of users with conflicting responsibilities, inspect user profiles noting evidence of segregation of duty consideration and review when conflicts are noted.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.4.3	Master data are complete and valid.	Segregation of duties conflicts are considered and resolved before providing access to master data transactions.	Inspect procedures for identifying, segregation of duty exceptions, and review compliance.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.4.4	Master data are complete and valid.	Edit reports are reviewed by appropriate data owners on a periodic basis to review new master data and changes made to existing master data.	Inspect evidence of proper review of edit reports by owners.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.5.1	Master data are consistent among modules.	Periodic review and reconciliation procedures are in place to ensure that master data are consistent between different application modules.	Inspect evidence of management reconciliation and review for effectiveness. Through inquiry and inspection, determine whether the frequency of management reconciliation of master data is appropriate.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.6.1	Master data additions, deletions, and changes are properly managed and monitored by data owners.	Master data policies and procedures require data owners to be responsible for the creation, deletion, and change of master data and also changes to data characteristics.	Review policies and procedures and inquire of data owner concerning application of specific monitoring procedures.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.6.2	Master data additions, deletions, and changes are properly managed and monitored by data owners.	Data owners monitor master data design changes, and approve and monitor creation, deletion and changes to master data on a regular basis.	<p>Obtain and inspect evidence of monitoring by data owners, including related reports.</p> <p>Inquire of management regarding ongoing monitoring of master data changes.</p> <p>Obtain and inspect evidence of management review of master data design changes, and determine whether changes are approved and reviewed.</p>
4.3 Interface Controls (IN)	Critical Element IN-1: Implement an effective interface strategy and design.	IN-1.1.1	An interface strategy is developed for each interface used in the application.	An interface strategy exists for each interface that includes the interface method, data fields being interfaced, controls to reasonably ensure a complete and accurate interface, schedule, assignment of responsibilities, system balancing requirements and security requirements.	<p>Obtain a list of all interfaces to and from the application audited.</p> <p>Inspect the interface strategy document noting the details of each interface and determine whether it contains appropriate information.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.3 Interface Controls (IN)	Critical Element IN-1: Implement an effective interface strategy and design.	IN-1.2.1	An interface design is developed for each interface used in the application that includes appropriate detailed specifications.	An interface design exists for each interface and includes appropriate specifications based on the business requirements, including: <ul style="list-style-type: none"> • validations and edits; • ownership of the interface process; • error correction and communication methods. 	Inspect interface design documents of each interface and determine whether it contains appropriate information.
4.3 Interface Controls (IN)	Critical Element IN-1: Implement an effective interface strategy and design.	IN-1.2.2	An interface design is developed for each interface used in the application that includes appropriate detailed specifications.	Mapping tables are used to convert data from the source system to the target system. Controls are in place to reasonably assure that mapping tables are only changed when authorized and that historical data on mappings is retained with the previous mapping table.	Determine whether the interfaces use mapping tables. Verify that controls over mapping tables will be established.
4.3 Interface Controls (IN)	Critical Element IN-1: Implement an effective interface strategy and design.	IN-1.2.3	An interface design is developed for each interface used in the application that includes appropriate detailed specifications.	If mapping tables are not used, appropriate edits and validations are present in the source system.	Review the edits and validations in the source system to determine whether they are appropriate and perform tests to assess their effectiveness.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.3 Interface Controls (IN)	Critical Element IN-1: Implement an effective interface strategy and design.	IN-2.1.1	Procedures are in place to reasonably assure that the interfaces are processed accurately, completely and timely.	<p>Procedures include a complete list of interfaces to be run, the timing of the interface processing, how it is processed and how it is reconciled. If system interconnections are used, procedures should address requirements for an Interconnection Security Agreement and Memorandum of Understanding.</p> <p>Timing for processing of the interface has been determined and is followed.</p> <p>A positive acknowledgement scheme is used to ensure that files sent from a source system are received by the target system (i.e., a "handshake" between the systems so that files are not skipped or lost). (Out of Scope or Optional)</p>	<p>Inspect documentation of interface processing procedures and, if applicable, Interconnection Service Agreements and Memorandums of Understanding.</p> <p>Observe interface processing into the application.</p> <p>Determine whether data and files from interface activities are processed according to the stated policies and in the proper accounting period.</p> <p>Determine whether all files sent from the source system are received and acknowledged by the target system.</p>
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.2.1	Ownership for interface processing is appropriately assigned.	<p>Responsibility for processing the interface and correcting any errors has been assigned to a user from the source and to a user of the target system. Actual processing may involve a technical person, if the interface is processed via an electronic media, such as a tape.</p>	<p>Identify which users are assigned responsibility for the interfaces. Evaluate whether an appropriate level of resources has been assigned to maintain interfaces.</p>
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.2.2	Ownership for interface processing is appropriately assigned.	<p>The files generated by an application interface (both source and target) are properly secured from unauthorized access and/or modifications.</p>	<p>Assess whether appropriate security is in place for all access points to the interface data are secure from unauthorized use.</p> <p>Identify individuals that will be responsible for providing security surrounding the interfaces.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.2.3	Ownership for interface processing is appropriately assigned.	Users who are processing interfaces are able to monitor the status of interfaces.	Assess whether proper access is assigned to the appropriate individuals for the monitoring of the interface status and that such individuals have access to appropriate information to monitor the status of the interface.
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.3.1	The interfaced data is reconciled between the source and target application to ensure that the data transfer is complete and accurate.	Reconciliations are performed between source and target applications to ensure that the interface is complete and accurate. Control totals agree between the source and target systems. Reports reconcile data interfaced between the two systems and provide adequate information to reconcile each transaction processed.	Inspect reports or other documents used to reconcile interface processing between source and target applications and review their content and frequency for appropriateness.
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.4.1	Errors during interface processing are identified by balancing processes and promptly investigated, corrected and resubmitted for processing.	Management maintains a log for interface processing. The log accounts for errors and exceptions, as well. (Out of scope or optional) Exception/error reports are produced, reviewed, and resolved by management on a regular basis, including correction and resubmission, as appropriate.	Through inquiry of management and review of logs, determine whether errors are properly handled. Assess the appropriateness of the frequency that exception reports are reviewed (daily, weekly, etc). Inspect evidence of such reviews having been performed.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.5.1	Rejected interface data is isolated, analyzed and corrected in a timely manner.	Error and correction facilities are utilized to track and correct errors in interface data.	Assess the adequacy of procedures in place to properly correct any rejected transactions. Inquire about procedures applied with individuals responsible for identifying and correcting errors and inspect evidence that rejected data is properly processed timely basis.
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.5.2	Rejected interface data is isolated, analyzed and corrected in a timely manner.	A mechanism is used to notify users when data is rejected (for example, an e-mail message may be sent to the user). These messages should repeat daily until they are corrected.	Determine whether error messages are generated and promptly reviewed for all rejected data and are maintained until corrected.
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.5.3	Rejected interface data is isolated, analyzed and corrected in a timely manner.	Audit trails are used to identify and follow-up on interface errors. The corrections to interface errors are included in the audit trail.	Determine whether appropriate audit trails are generated, reviewed and maintained.
4.3 Interface Controls (IN)	Critical Element IN-2: Implement effective interface processing procedures.	IN-2.6.1	Data files are not processed more than once.	Interfaces files are automatically archived or deleted from the production environment after processing.	Inspect a selection of archived interface documents and verify the date and time of processing. Observe the interfaces that are in process and inspect evidence that interface files were not processed before.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.1.1	Implement an effective data management system strategy and design, consistent with the control requirements of the application and data. The strategy addresses key concepts including: <ul style="list-style-type: none"> • database management, • middleware, • cryptography, • data warehouse, and • data reporting/ data extraction. 	The physical and logical (in terms of connectivity) location of the data storage and retrieval functions are appropriate.	Inspect documentation of the design of the data management system(s) associated with the application.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.1.2	Implement an effective data management system strategy and design, consistent with the control requirements of the application and data. The strategy addresses key concepts including: <ul style="list-style-type: none"> • database management, • middleware, • cryptography, • data warehouse, and • data reporting/ data extraction. 	The production data management system is effectively separated from non-production systems (such as testing and development) and other production systems with lesser control requirements.	Assess whether the production and nonproduction data management systems are effectively separated.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.1.3	Implement an effective data management system strategy and design, consistent with the control requirements of the application and data. The strategy addresses key concepts including: <ul style="list-style-type: none"> • database management, • middleware, • cryptography, • data warehouse, and • data reporting/ data extraction. 	The database schema is consistent with access control requirements such that the organization of data and database-hosted functions correspond to the access limitations that need to be imposed on different groups of users.	Verify that all access paths to data and sensitive data management system administrative functions have been identified and are adequately controlled.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.2.1	Detective controls are implemented in a manner that effectively supports requirements to identify and react to specific system or user activity within the data management system and its related components.	Logging and monitoring controls are in place the data management system level which effectively satisfy requirements to accurately identify historical system activity and data access.	Identify the security events that are logged and determine whether logging is adequate. Assess the adequacy of controls to monitor the audit logs.
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.2.2	Detective controls are implemented in a manner that effectively supports requirements to identify and react to specific system or user activity within the data management system and its related components.	Real-time or near real-time controls are in place to detect abnormal activity and security events.	Assess the adequacy of controls to detect abnormal activity.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.3.1	Control of specialized data management processes used to facilitate interoperability between applications and/or functions not integrated into the applications (such as ad-hoc reporting) are consistent with control requirements for the application, data and other systems that may be affected.	Data accuracy and completeness controls are in place and effective to correct and/or detect data anomalies.	<p>Perform the following procedures for DA-1.3.1 to DA-1.3.2.</p> <p>Identify and obtain an understanding of specialized data management processes used to facilitate interoperability.</p> <p>Understand how system Page 446 4.4 Data Management System Controls (DA) interconnectivity is controlled with respect to data management systems.</p> <p>Assess the adequacy of controls over specialized management processes.</p> <p>Note: These procedures should be closely coordinated with tests of general controls related to the data management systems.</p> <p>Determine whether a periodic reconciliation process is implemented to ensure the data in a data warehouse matches the data from the source system.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.4 Data Management System Controls	Critical Element DA-1; Implement an effective data management system strategy and design.	DA-1.3.2	Control of specialized data management processes used to facilitate interoperability between applications and/or functions not integrated into the applications (such as ad-hoc reporting) are consistent with control requirements for the application, data and other systems that may be affected.	The configuration of system connectivity that facilitates application to application and application to non-integrated functions is controlled to limit access appropriately.	<p>Perform the following procedures for DA-1.3.1 to DA-1.3.2.</p> <p>Identify and obtain an understanding of specialized data management processes used to facilitate interoperability.</p> <p>Understand how system Page 446 4.4 Data Management System Controls (DA) interconnectivity is controlled with respect to data management systems.</p> <p>Assess the adequacy of controls over specialized management processes. Note: These procedures should be closely coordinated with tests of general controls related to the data management systems.</p> <p>Determine whether a periodic reconciliation process is implemented to ensure the data in a data warehouse matches the data from the source system.</p>

C.2 Application Controls – Other

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.4.1	Application owners and users are aware of application security policies.	The entity has an effective process to communicate application security policies to application owners and users and reasonably assure that they have an appropriate awareness of such policies.	Obtain an understanding of how application owners and users are made aware of application security policies and assess the adequacy of the process. Interview selected application owners and users concerning their awareness of application security policies.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.4.2	Application owners and users are aware of application security policies.	Personnel policies related to the application appropriately address security and application owners and users have adequate training and experience.	Review personnel policies for appropriateness and consistency with entity-wide policies. Assess the adequacy of training and expertise for application owners and users.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.5.1	Management monitors and periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	An application security policy and procedure test plan is developed and documented.	Inquire of management, and inspect testing policies and procedures.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.5.3	Management monitors and periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	The frequency and scope of testing is commensurate with the risk and criticality of the application to the entity's mission.	Based upon the application test plan, assess whether the frequency and scope of testing is appropriate, given the risk and criticality of the application.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.5.4	Management monitors and periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	Compliance, and a report on the state of compliance, is part of the entity's security program.	Determine through inquiry and inspection if the application security plan is incorporated into the entity's security program.
4.1 Application Level General Controls (AS)	Critical Element AS-1: Implement effective application security management.	AS-1.7.2	External third party provider activities are secure, documented, and monitored.	A process is in place to monitor third party provider compliance to the entity's regulatory requirements.	Inquire of management regarding procedures used to monitor third party providers. Inspect external reports (SAS 70) or other documentation supporting the results of compliance monitoring.
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.3.3	Security policies and procedures appropriately address ID and password management.	Each application user has only one user ID.	Through observation and inspection, determine whether each user has one, and only one, user ID to access the application.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.3.4	Security policies and procedures appropriately address ID and password management.	Multiple log-ons are controlled and monitored.	Through inquiry, observation or inspection, determine whether the application allows multiple log-ons by the same user. If so, understand and document monitoring procedures that reasonably assure that multiple logons are not used to allow application access to an unauthorized user, or to violate effective segregation of duties.
4.1 Application Level General Controls (AS)	Critical Element AS-2: Implement effective application access controls.	AS-2.11.1	Physical security controls over application resources are adequate.	Physical controls are integrated with entity-wide and system-level controls. Application resources sensitive to physical access are identified and appropriate physical security is placed over them.	Review the appropriateness of the entity's identification of application resources sensitive to physical access. Assess the adequacy of physical security over sensitive application resources.
4.1 Application Level General Controls (AS)	Critical Element AS-3: Implement Effective Application Configuration Management.	AS-3.2.1	Current configuration information is maintained.	The entity maintains information on the current configuration of the application.	Review the entity's configuration management information.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-3: Implement Effective Application Configuration Management.	AS-3.5.9	Changes are controlled as programs progress through testing to final approval.	Documentation is updated when a new or modified system is implemented.	<p>Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved.</p> <p>Review test plan standards.</p> <p>Examine a selection of recent software changes and</p> <ul style="list-style-type: none"> • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.1 Application Level General Controls (AS)	Critical Element AS-5: Implement effective application contingency planning.	AS-5.1.2	Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.	Identify the disruption impacts and allowable outage times for the application.	<p>Perform the following procedures for AS-5.1.1 to AS-5.1.3.</p> <p>Review the policies and methodology, and the BIA (if conducted) used to determine the application’s critical functions and supporting IT resources, the outage impacts and allowable outage times, and the recovery priorities.</p> <p>Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of the results.</p>
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.4.2	Transactions are valid and are unique (not duplicated).	The system produces warning or error messages.	<p>Perform the following procedures for BP-2.4.1 to BP-2.4.4.</p> <p>Inspect design document to identify key data validation and edit checks.</p> <p>Inspect configuration to verify that the identified edit and validations checks are appropriately set, and transactions are rejected/suspended when data/processing errors occur. Also verify that warning and error messages are designed when the processing is incomplete.</p>
4.2 Business Process Controls (BP)	Critical Element BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.8.1	As appropriate, the confidentiality of transaction data during processing is adequately controlled.	Management implements adequate controls to protect the confidentiality of data during processing, as appropriate.	<p>Assess the adequacy of management controls over confidentiality during processing.</p> <p>Coordinate this step with Critical Element AS-2 Implement effective application access controls.</p>

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.1.1	Outputs are appropriately defined by the management (form, sensitivity of data, user selectivity, confidentiality, etc).	Management has developed reporting strategy that includes the following: <ul style="list-style-type: none"> • content and availability that are consistent with end users’ needs, • sensitivity and confidentiality of data, • appropriate user access to output data. 	Inquire of management about a reporting strategy or policy. Obtain a copy of any formal reporting strategy or policy. Assess the adequacy of the strategy and related policies.
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.2.2	Output generation and distribution are aligned with the reporting strategy.	Management has procedures in place to monitor replication of output data used in management reports or other communications within or outside the entity.	Inquire of management on the use of data output. Inspect selected management reports or other communication to verify the accurate replication of data. Verify that the user received appropriate authorization to use the data.
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.5.1	Access to output/reports and output files is based on business need and is limited to authorized users.	Access to reports is restricted to those users with a legitimate business need for the information.	Perform the following procedures for BP-3.5.1 to BP-3.5.2. Select output/reports and output files from the audit area and inspect application access (if the output can be accessed online or other electronic form) or inspect distribution to determine whether the user has appropriate level of security clearance and is authorized to access.

Section	Title/Description (Critical Element)	FISCAM X-Reference	FISCAM Control Activities	FISCAM Control Techniques	Audit Procedures
4.2 Business Process Controls (BP)	Critical Element BP-3: Transaction data output is complete, accurate, valid, and confidential.	BP-3.5.2	Access to output/reports and output files is based on business need and is limited to authorized users.	Users should have appropriate authorization for accessing reports, including the appropriate level of security clearance, where applicable.	Perform the following procedures for BP-3.5.1 to BP-3.5.2. Select output/reports and output files from the audit area and inspect application access (if the output can be accessed online or other electronic form) or inspect distribution to determine whether the user has appropriate level of security clearance and is authorized to access.
4.2 Business Process Controls (BP)	Critical Element BP-4: Master Data Setup and Maintenance is Adequately Controlled.	BP-4.7.1	As appropriate, the confidentiality of master data is adequately controlled.	Management implements adequate controls to protect the confidentiality of master data, as appropriate.	Assess the adequacy of management controls over confidentiality of master data. Coordinate this step with Critical Element AS-2 Implement effective application access controls.