For High-Impact Information Systems

FAMILY: CERTIFCATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

CA-1.1 – **Examine** security assessment and certification and accreditation policies and procedures; other relevant documents or records, **and**

Interview organizational personnel with security assessment and certification and accreditation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents security assessment and certification and accreditation policies and procedures.				
(ii)	The organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization.				
(iii)	Responsible parties within the organization periodically review policy and procedures.				
(iv)	The organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.				

CA-1.2 - Examine security assessment and certification and accreditation policies and procedures; other relevant documents or records, **and**

Interview organizational personnel with security assessment and certification and accreditation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.				
(ii)	The security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.				

CA-2 SECURITY ASSESSMENTS - The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

CA-2.1 – Examine security assessment policy; procedures addressing security assessments; information system security plan (for organization-defined frequency of security control assessments); security assessment plan; security assessment report; assessment evidence; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system is in the inventory of major information systems.				
(ii)	The organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.				

CA-3 INFORMATION SYSTEM CONNECTIONS - The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

CA-3.1- Examine access control policy; procedures addressing information system connections; NIST Special Publication 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records, **and**

Interview organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).				
(ii)	The organization authorizes all connections from the information system to external information systems through the use of system connection agreements.				
(iii)	The organization monitors/controls the system interconnections on an ongoing basis.				
(iv)	Information system connection agreements are consistent with NIST Special Publication 800-47.				

CA-4 SECURITY CERTIFICATION - The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

CA-4.1 – Examine certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records, **and**

Interview organizational personnel with security certification responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	desired outcome with respect to meeting the security requirements for the system.				
(ii)	The organization employs a security certification process in accordance with OMB policy and NIST Special Publications 800-37 and 800-53A.				

CA-4(1).1 – Examine certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.				

CA-5 PLAN OF ACTION AND MILESTONES - The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

CA-5.1 – Examine certification and accreditation policy and procedures; information system security plan (for organization-defined frequency of plan of action and milestones updates); security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records, **and**

Interview organizational personnel with plan of action and milestones development and implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and updates at the organization-defined frequency, a plan of action and milestones for the information system.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system.				

CA-6 SECURITY ACCREDITATION - The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

CA-6.1 - Examine certification and accreditation policy; procedures addressing security accreditation; NIST Special Publication 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records, **and**

Interview organizational personnel with security accreditation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three years.				
(ii)	A senior organizational official signs and approves the security accreditation.				
(iii)	The security accreditation process employed by the organization is consistent with NIST Special Publications 800-37.				
(iv)	The organization updates the authorization when there is a significant change to the information system.				

CA-7 CONTINUOUS MONITORING - The organization monitors the security controls in the information system on an ongoing basis.

CA-7.1 - **Examine** certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST Special Publications 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records,

and

Interview organizational personnel with continuous monitoring responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization monitors the security controls in the information system on an ongoing basis.				
(ii)	The organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A.				

CA-7.2 - **Examine** certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records, **and**

Interview organizational personnel with continuous monitoring responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization conducts security impact analyses on changes to the information system.				
(ii)	The organization documents and reports changes to or deficiencies in the security controls employed in the information system.				
(iii)	The organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.				

CA-7(1).1 - **Examine** certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records, **and**

Interview organizational personnel with continuous monitoring responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.				