**Security Assessment and Authorization (CA)**

**CA-1: Security Assessment and Authorization Policy and Procedures**

NIST SP 800-53 Objective:

The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

a. Formal, documented security assessment and authorization policies that address purpose,

scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Control Translation: Ensure security assessment and authorization policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Security Assessment and Authorization Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**CA-2: Security Assessments**

NIST SP 800-53 Objective: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;

- Assessment procedures to be used to determine security control effectiveness; and

- Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system organization-defined frequency 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;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

Control Translation: This control is looking for the basic outputs of the assessment and authorization process. Documentation of a previous process or the current process if it is the first one should suffice to satisfy this control. This control is related to CA-6 (Security Authorization), CA-7 (Continuous Monitoring), PM-9 (Risk Management Strategy), and SA-11 (Developer Security Testing).

Notes: These documents are well defined and should be available if the system or organization has received an ATO in the past.

How to test and evaluate: Review the security assessment and authorization policy, any procedures addressing security assessments, the security assessment plan, the security assessment report, the system security plan, and any assessment delivery notification letters or documents that show delivery of the final assessment to verify that all steps have been completed and documented for a previous assessment or are being completed for the initial assessment.

Technology specific: General

**CA-3: Information System Connections**

NIST SP 800-53 Objective: The organization:

a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;

b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

Control Translation: This control is looking for documentation of all connections outside the authorization boundary. In addition there should be some documentation describing how these connections are monitored. This control is related to AC-4 (Information Flow Enforcement), IA-3 (Device Identification and Authentication), SC-7 (Boundary Protection), and SA-9 (External Information System Services).

Notes: Assessment of this control can be complicated by confusion of what constitutes an external system. It is important to ensure that you have a clear definition of external and if this is anything outside of the assessment boundary or if this truly refers to 3rd party systems.

How to test and evaluate: Review the access control policy, procedures addressing information system connections, system and communications protection policy, information system Interconnection Security Agreements (ISA), Memorandum of Understanding (MOU), Service Level Agreements (SLA), security plan, information system design documentation, and the security assessment report for evidence of connections and monitoring.

Technology specific: General

**CA-5: Plan of Action and Milestones**

NIST SP 800-53 Objective: The organization:

a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones at the organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Control Translation: This control is looking for the remediation process in effect for issues discovered during previous assessments. An assessor will need to see both the creation of POAMs as well as the update and closure of POAMs. This control is related to PM-4 (Plan of Action and Milestones Process).

Notes: It is common to see POAMs created, but never updated or closed. Make sure to guide the client through this process when creating POAMs and if you are assessing make sure to check this area.

How to test and evaluate: Review the procedures addressing plan of action and milestones, security plan, security assessment plan, security assessment report, assessment evidence, plan of action and milestones tracking documents or technology for evidence of both the creation and tracking of POAMs from discovery through closure.

Technology specific: General

**CA-6: Security Authorization**

NIST SP 800-53 Objective: The organization:

a. Assigns a senior-level executive or manager to the role of authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization at the organization-defined frequency

Control Translation: This control is looking for who (or what role) is the assigned authorizing official for the system and that this official is completing their responsibilities of sign-off and updates to the system authorization. This control is related to CA-2 (Security Assessments), CA-7 (Continuous Monitoring), PM-9 (Risk Management Strategy), and PM-10 (Security Authorization Process).

Notes: There should be a signed document for each ATO.

How to test and evaluate: Review the procedures addressing security authorization as well as the security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement, and authorization letter/memo) ensuring that the role or individual responsible for final approval is defined and that they are attending to authorizations.

Technology specific: General

**CA-7: Continuous Monitoring**

NIST SP 800-53 Objective: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. A configuration management process for the information system and its constituent components;

b. A determination of the security impact of changes to the information system and environment of operation;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and

d. Reporting the security state of the information system to appropriate organizational officials at the organization-defined frequency.

Control Translation: This control is looking for both a continuous monitoring plan and documentation of this plan being implemented. This control is related to CA-2 (Security Assessments), CA-5 (Plan of Action and Milestones), CA-6 (Security Authorization), CM-3 (Configuration Change Control), and CM-4 (Security Impact Analysis).

Notes: System scanning is not sufficient for continuous monitoring. The organization will have to define what they are monitoring and on what schedule. This includes controls that will need to be re-assessed during the ATO period and their frequency. Reporting of the outcomes of these controls can occur in many ways including via a meeting, email, or a formal report and briefing. Many clients do not realize these differences.

How to test and evaluate: Review a continuous monitoring plan, security assessment and authorization policy, procedures addressing configuration management, security plan, security assessment report, plan of action and milestones, information system monitoring records, configuration management records, security impact analyses, and status reports reviewing for evidence that the continuous monitoring plan is being implemented over time.

Technology specific: General