**Configuration Management (CM)**

**CM-1: Configuration Management Policy and Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the configuration

Control Translation: Ensure configuration management policy and procedures are in place.

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

How to test and evaluate: Examine SSP and Configuration Management 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

**CM-2: Baseline Configuration**

NIST SP 800-53 Objective: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Control Translation: You should look for a source code repository or another method of maintaining baseline documentation and configurations. Also check This control is related to CM-3 (Configuration Change Control), CM-6 (Configuration Settings), CM-8 (Information System Component Inventory), and CM-9 (Configuration Management Plan).

Notes: Also look at how many baselines and how often they are updated for each technology. You will need this for later controls.

How to test and evaluate: Examine SSP, Configuration Management Plan , Baseline configuration checklists, documented baseline configuration settings for automated mechanisms reviewing for all technologies that may have a baseline configuration. Validate that baselines are created for each component in accordance with defined frequencies. Look for documents that show the configuration and how a new user would be able to replicate this configuration in a replacement or new device. In addition you may have to prove that a group of devices all use the same configuration.

Technology specific: All

**CM-3: Configuration Change Control**

NIST SP 800-53 Objective: The organization:

a. Determines the types of changes to the information system that are configuration controlled;

b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;

c. Documents approved configuration-controlled changes to the system;

d. Retains and reviews records of configuration-controlled changes to the system;

e. Audits activities associated with configuration-controlled changes to the system; and

f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Control Translation: Review the entire change control process looking for documentation of types of changes that run through this process, who makes any approvals and how they give them, what documentation is created, how the documentation is maintained and retained, and how audits of these records are completed and how often. This control is related to CM-4 (Security Impact Analysis), CM-5 (Access Restrictions for Change), CM-6 (Configuration Settings), and SI-12 (Information Output Handling and Retention).

Notes: Make sure to carefully cover all of these areas. It is common to have some of them satisfied but have one or two that are out of compliance.

How to test and evaluate: Examine SSP, configuration management policy; configuration management plan; procedures addressing information system configuration change control; or change control records and tickets. Look for documentation for all areas of the configuration change control tests.

Technology specific: All

**CM-4: Security Impact Analysis**

NIST SP 800-53 Objective: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Control Translation: Testing should show a review of the SSP controls affected by each change and how each change will be implemented. This review will show how the organization reviews for potential impacts. This control is related to CA-2 (Security Assessments), CA-7 (Continuous Monitoring), CM-3 (Configuration Change Control), CM-9 (Configuration Management Plan), SI-2 (Flaw Remediation)

Notes: Just having a CM process does not guarantee that the organization is considering security control impacts of changes. This is a specific analysis that needs to be completed.

How to test and evaluate: Examine SSP, Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; or change control records. Look for documentation specifically related to reviewing changes for potential security impacts.

Technology specific: All

**CM-5: Access Restrictions for Change**

NIST SP 800-53 Objective: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Control Translation: This control is primarily looking for records of access and authorization for changes made to the system and ensuring the ability to make changes to the system is limited to authorized individuals (i.e. administrators). Review both physical and logical access mechanisms for the system, software libraries, and any other areas in the system where changes can be made. This control is related to AC-3 (Access Enforcement), AC-6 (Least Privilege), and PE-3 (Physical Access Control).

Notes: All technologies should have their own answers unless there is a centralized system for making changes.

How to test and evaluate: Review physical and logical access control mechanisms, workflow automation, media libraries, abstract layers (3rd party change interfaces), and change windows. Review configuration management policies, CM Plans, procedures that address access restrictions for changes and the System SSP.

Technology specific: All

**CM-6: Configuration Settings**

NIST SP 800-53 Objective:

The organization:

a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using checklists that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Control Translation: Control is looking for documentation of mandatory configuration settings, implementation of configuration settings, documentation and definition of exceptions of the mandatory settings, and monitoring and controlling of the configuration settings.

Notes: Look for either configuration settings as defined by the organization or defined by the software creator or another outside entity.

How to test and evaluate: Control review for several things. Review configuration checklists for documentation of mandatory config. settings, review for implementation of security configuration checklists, review documentation and procedures for exceptions from the mandatory configuration settings, review mechanisms and controls for monitoring changes to the configuration settings and checklists. Review SSP, Configuration Management policy, CM Plan, procedures addressing configuration settings for the information system, information system configuration settings and associated documentation, and security configuration checklists. This control is related to CM-2 (Baseline Configuration), CM-3(Configuration Change Control), and SI-4 (Information System Monitoring).

Technology specific: All

**CM-7: Least Functionality**

NIST SP 800-53 Objective: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services.

Control Translation: This control is looking for covering both the essential services that a technology would provide as well as what ports and configurations will be to support those essential services.

Notes: Most often this control is satisfied via network scans or vulnerability scans, however a documented configuration is the other half of this control test.

How to test and evaluate: Review system scans and network scans as well as documented configurations to prove the essential functions, ports, protocols, and/or services have been decided and are configured as documented on the system. Review the SSP, configuration management policy, CM plan, procedures addressing least functionality in the information system, information system configuration settings and associated documentation, and security configuration checklists. This control is related to RA-5 (Vulnerability Scanning).

Technology specific: All

**CM-8: Information System Component Inventory**

NIST SP 800-53 Objective: The organization develops, documents, and maintains an inventory of information system components that:

a. Accurately reflects the current information system;

b. Is consistent with the authorization boundary of the information system;

c. Is at the level of granularity deemed necessary for tracking and reporting;

d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and

e. Is available for review and audit by designated organizational officials.

Control Translation: This control is looking for a complete and up-to-date inventory of system components. This control is related to CM-2 (Baseline Configuration), CM-6 (Configuration Settings).

Notes: The inventory list just must be tested to ensure that it meets all of the listed requirements.

How to test and evaluate: Review an inventory list for all components in the system including for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.

Technology specific: General

**CM-9: Configuration Management Plan**

NIST SP 800-53 Objective: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and

c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Control Translation: This control covers the CM Plan and important sections including staffing and procedures and configuration items as a part of the SDLC. This control is related to SA-10 (Developer Configuration Management).

Notes: This control should be fairly straightforward looking for each of the individual requirements.

How to test and evaluate: Review the CM Plan for a section covering roles and responsibilities, a section defining configuration items under the SDLC, and a section establishing how to identify configuration items under the SDLC. Review the SSP, configuration management policy, CM plan, and procedures addressing configuration management planning.

Technology specific: General