Compliance Component

Definition

Name	Security-Focused Configuration Management
Description	Security-Focused Configuration Management (SecCM) enforces security configuration settings, monitors and controls changes to the established baseline configuration of installed hardware and software.
Rationale	Documenting information system changes and assessing the potential impact of these changes on the security of a system is essential for tracking changes and maintaining continuity.
Benefits	• Provides comprehensive and continuous documentation of hardware and software changes. • Provides a list of changes to be used when identifying security-related problems. • Provides a means of recovery in case of a malfunction.

Associated Architecture Levels

Specify the Domain Name	Security
Specify the Discipline Name	Operational Controls
Specify the Technology Area Name	Hardware & Software Maintenance
Specify the Product Component Name	

Compliance Component Type

Document the Compliance Component Type	Guideline
Component Sub-type	

Compliance Detail

State the Guideline, Standard or Legislation	**SecCM** involves documentation of the configuration of installed hardware and software at given points in time, systematically controlling changes to the configuration, and maintaining the integrity and traceability of the configuration throughout the system lifecycle. SecCM is a five step process: 1. **Planning** – Planning includes developing policy and procedures to incorporate SecCM into existing information technology and security programs, and then disseminating the policy throughout the organization. 2. **Identifying and Implementing Configurations** – After the planning and preparation activities are completed, a secure baseline configuration for the information system is developed, reviewed, approved, and implemented. The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. For a typical information system, the secure baseline may address configuration

settings, software loads, patch levels, how the information system is physically or logically arranged, how various security controls are implemented, and documentation.

3. **Controlling Configuration Changes** – In this phase of SecCM, the emphasis is put on the management of change to maintain the secure, approved baseline of the information system. Through the use of SecCM practices, organizations ensure that changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation.

4. **Monitoring** – Validates that the information system is adhering to organizational policies, procedures, and the approved secure baseline configuration. Monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk.

5. **Using Security Content Automation Protocol -** Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which information about software flaws and secure configurations can be communicated. SCAP-enabled tools can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings against an expected baseline, and examining systems for signs of compromise.

This document will be reviewed at least annually or as needed.

Document Source Reference #	NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (October 2019)

Compliance Sources

Name	National Institute of Standards and Technology (NIST), Computer	*Website*	http://csrc.nist.gov/
Contact Information	http://csrc.nist.gov/		
Name		*Website*	
Contact Information			

KEYWORDS

List Keywords	Change, installation, validation, baseline, testing, deployment, evaluation, planning, identifying, implementing, monitoring, configuration, controlling, SecCM, SCAP

COMPONENT CLASSIFICATION

Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		

☐ *Conditional Use*		

Rationale for Component Classification

Document the Rationale for Component Classification	

Migration Strategy

Document the Migration Strategy	

Impact Position Statement

Document the Position Statement on Impact	

Current Status

Provide the Current Status	☐ *In Development*	☒ *Under Review*	☐ *Approved*	☐ *Rejected*

Audit Trail

Creation Date	04/05/2007	*Date Approved / Rejected*	11/19/2024
Reason for Rejection			
Last Date Reviewed	09/19/2024	*Last Date Updated*	11/19/2024
Reason for Update	Vitality		