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. The SecCM process consists of four phases: 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.
Document Source Reference #	NIST SP 800-128

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

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*	05/16/2019
Reason for Rejection			
Last Date Reviewed	05/09/2019	*Last Date Updated*	05/09/2019
Reason for Update	Vitality		