



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Configuration Management
<i>Description</i>	Configuration Management is enforcing security configuration settings, monitoring and controlling changes to the established baseline configuration of installed hardware and software.
<i>Rationale</i>	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.
<i>Benefits</i>	<ul style="list-style-type: none"> • Provides a 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	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Operational Controls
<i>Specify the Technology Area Name</i>	Hardware & Software Maintenance
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p>Security configuration management 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.</p> <p>The Configuration Management process consists of four phases:</p> <ol style="list-style-type: none"> 1. Planning – developing policy and procedures to incorporate Security Configuration Management into existing information technology and security programs, and then disseminating the policy throughout the organization. 2. Identifying and Implementing Configurations – The approved baseline configuration for an information system and associated components represents the most secure state consistent with

	<p>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.</p> <p>3. Controlling Configuration Changes – Through the use of Security Change Management practices, organizations ensure that changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation.</p> <p>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.</p>		
<i>Document Source Reference #</i>	NIST SP 800-128		
Compliance Sources			
<i>Name</i>	National Institute of Standards and Technology (NIST),	<i>Website</i>	http://csrc.nist.gov/
<i>Contact Information</i>	http://csrc.nist.gov/		
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
KEYWORDS			
<i>List Keywords</i>	Change, installation, validation, baseline, testing, deployment, evaluation, planning, identifying, implementing, monitoring, configuration, controlling		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>			
COMPONENT SUB-CLASSIFICATION			
<i>Sub-Classification</i>	<i>Date</i>	<i>Additional Sub-Classification Information</i>	
<input type="checkbox"/> <i>Technology Watch</i>			
<input type="checkbox"/> <i>Variance</i>			
<input type="checkbox"/> <i>Conditional Use</i>			
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			

Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input checked="" type="checkbox"/> <i>Under Review</i>	<input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>
AUDIT TRAIL			
<i>Creation Date</i>	04/05/2007	<i>Date Approved / Rejected</i>	11/20/2007
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>	03/12/2015	<i>Last Date Updated</i>	07/15//2015
<i>Reason for Update</i>	Vitality		