Compliance Component

DEFINITION

Name	Initiation Phase
Description	The Initiation Phase of security system life cycle is an initial description of the system's basic security needs, and the associated costs and assurance provided by the security controls.
Rationale	The initiation phase provides a high-level description of the assurance requirements and the security controls to protect a system.
Benefits	• Generates the information needed to determine the best overall security solution for the system • Analysis of security costs at initiation results in a more realistic estimate of total system costs.

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	System Life Cycle Security
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	Specific decisions about security must be made to assure that the system is secure. • Study the agency's software development process. Obtain copies of the materials used by systems design and development during the SDLC. Talk to the systems development staff about how the process works. Develop some ideas of how security can be integrated into this process. • Consider the security structure at the agency. Is it highly centralized, or a decentralized structure with security officers throughout the agency whose expertise can be used in integrating security into the SDLC? The security structure will influence the details of the process that is implemented. • Meet with management. Discuss the benefits of integrating security into the SDLC.

	• Meet with systems staff to discuss the details of how best to integrate security into the agency's SDLC. • Continue to work with system's staff to keep policy up-to-date, and to keep pace with changes in your systems development lifecycle. An agency must perform the following: 1. Security Categorization – define levels (i.e., low, moderate, or high) of potential impact to agencies or individuals should there be a security breach o Security categorization standards assist agencies in making the appropriate selection of security controls for their information systems. 2. Preliminary Risk Assessment – results in an initial description of the basic security needs of the system. o Define the threat environment in which the system will operate (e.g. public, private) o Determine the security requirements of the proposed system (e.g. HIPAA, state laws, etc.) 3. Determine the security controls that will be needed to mitigate the risks o The security implications of alternative architectures and technologies should be considered. 4. Estimate total life cycle costs, including implementation costs and in-service management costs, of the security controls. o Conduct a thorough market analysis, alternatives analysis, and affordability assessment to determine the best security solution for obtaining needed capability o Quantify the cost, schedule, performance, and benefit baselines for that solution.		
Document Source Reference #	NIST SPECIAL PUBLICATION 800-64 REV. 1,		
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS

List all Keywords	Costs, assurance, estimates, integrate, SDLC, impact, risk, environment, schedule, performance, baseline.

COMPONENT CLASSIFICATION

Provide the Classification	□ *Emerging* ☒ *Current* □ *Twilight* □ *Sunset*

Rationale for Component Classification

Document the Rationale for Component Classification	

Conditional Use Restrictions

Document the Conditional Use Restrictions	

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	09/07/06	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			