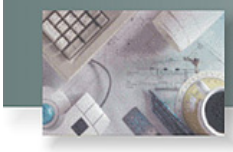

Compliance Component

DEFINITION	
Name	Implementation Phase
Description	The Implementation Phase is when the system is installed and evaluated in the agency's operational environment.
Rationale	Inspection and acceptance of the delivered system is necessary to verify that the functionality described in the specifications has been included in the deliverables.
Benefits	• System Integration – ensures that the system is integrated at the operational site. • Security Certification – ensures that the controls are effectively implemented. o Security certification also exposes and addresses the known vulnerabilities in the information system. • Security Accreditation – provides the necessary security authorization of an information system to process, store, or transmit information that is required.
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	Implementation Guidance
	• Inspect the system by performing integration and acceptance testing after delivery and installation of the information system.
	  o Testing can be done by the agency or by an independent contractor to assure that the system meets the specifications, and that the security features are operating.
	• Enable security control settings and switches in accordance with the security configuration requirements.
	  o Conduct a security certification to ensure that security

	controls were established according to the security requirements. • An appropriate agency official shall grant authorization to operate the system based on the verified effectiveness of security controls to the agreed level of assurance and the identified residual risk to agency assets or operations.		
Document Source Reference #	For a complete list of references, consult NIST SP 800-64.		
Standard Agency			
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	Management, policy, procedures, planning, sensitive, data, evaluate, test, inspect security, certification, accreditation.		
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	08/24/2006	*Date Accepted / Rejected*	

Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			