Compliance Component

DEFINITION	
Name	Risk Mitigation
Description	Risk Mitigation is the second step of the risk management process. It involves prioritizing, evaluating, implementing and maintaining the appropriate risk-reducing controls (risk-reducing measures) recommended from the risk assessment process (see Risk Assessment CC).
Rationale	The elimination of all risk is usually impractical or close to impossible. Therefore, it is the responsibility of management to use the most cost effective approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the agency's resources and mission.
Benefits	• Risk Mitigation enables management to reduce mission risk, when feasible. • Risk Mitigation allows managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the agency systems and data that support their missions.
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	Security Risk Management
List Product Component Name	
COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	Risk Mitigation can be achieved through any combination of the following four options: • Risk Assumption o Accept the potential risk and continue operating the IT system • Risk Avoidance o Eliminate the cause of the risk (e.g., forego certain functions of the system or shut down the system after risks are identified) • Risk Limitation o Implementing controls that minimize the adverse impact of a threat exploiting a vulnerability (e.g., use of

supporting, preventive, detective controls). Limiting the risk does not eliminate it, but reduces it to an acceptable level.

- Risk Transference
  - Transfer the risk by using other options to compensate for the loss, such as purchasing insurance

The goals and mission of an agency must be considered in selecting any of the risk mitigation options above.

Priority must be given to the threats or vulnerabilities that have the potential to cause significant mission impact or harm.

The following risk mitigation steps must be followed and documented:

• Step 1 - Prioritize Actions

Prioritize the actions to be implemented based on the risk levels presented in the risk assessment report. In allocating resources, top priority must be given to risk items with High risk rankings. These vulnerabilities or threats will require immediate corrective action to protect an agency's interest and mission.

Output from Step 1 - Actions ranked from High to Low

• Step 2 - Evaluate Recommended Control Options

Select the most appropriate control option for minimizing the risk. The feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The controls recommended in the risk assessment may not be the most appropriate and feasible options for a specific agency or system.

Output from Step 2 - List of feasible controls

• Step 3 - Conduct Cost-Benefit Analysis

Conduct a cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls to aid management in decision making and to identify cost-effective controls.

Output from Step 3 - Cost-benefit analysis

• Step 4 - Select Control(s)

Management determines the most cost-effective control(s) for reducing risk to the agency's mission based on the results of the cost-benefit analysis. The selection may combine technical, operational, and management control elements to ensure required security.

Output from Step 4 - Selected control(s)

• Step 5 - Assign Responsibility

Assign risk mitigation responsibilities to appropriate person(s) (in-house or external contracting staff) who have the required expertise and skill-sets to implement the selected control(s).

Output from Step 5 - List of assigned person(s) and their

	respective risk mitigation responsibilities NOTE: The list must include the name of the individual who made the decision to accept, avoid, limit or transfer each individual risk. • Step 6 - Develop an Action Plan Develop an action plan that, at a minimum, contains: o Risks and associated risk levels (from risk assessment report) o Recommended controls (from risk assessment report) o Prioritized actions with priority given to items with High risk levels o Selected controls determined on the basis of feasibility, effectiveness, benefits to the agency, and cost o Required resources for implementing the selected controls o List of assigned person(s) and their respective risk mitigation responsibilities o Start date for implementation o Target completion date for implementation o Maintenance requirements Output from Step 6 - Action plan • Step 7 - Implement Selected Control(s) Implement the controls as required by the action plan. Output from Step 7 - Mitigation to an acceptable level of risk
Document Source Reference #	

Standard Organization			
Name	SP 800-30 Risk Management Guide for Information Technology Systems, July 2002	*Website*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
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	Plan, control, assessment, countermeasure, prevention, threat, vulnerability, safeguard

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	08/04/2005	*Date Accepted / Rejected*	03/14/2006
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			