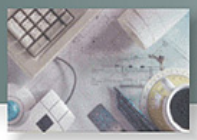

Technology Area

DEFINITION	
Name	Security Risk Management
Description	Security Risk Management is a three-step process of assessment, testing and mitigation. This allows agency 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 mission. Risk assessment includes identification and evaluation of risks, risk impacts, and recommendations for risk-reducing measures. Security testing identifies vulnerabilities and allows agencies the opportunity to mitigate them before they are exploited. Risk mitigation refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Risk management is ongoing and evolving, which emphasizes the need for continuing risk evaluations and assessments. The system owner determines whether the remaining risk is at an acceptable level or whether additional security controls should be implemented.
Rationale	Security Risk Management ensures that appropriate, cost-effective safeguards are incorporated into existing and new installations of agency systems.
Benefits	Security Risk Management helps to ensure the balance of risks, vulnerabilities, threats, countermeasures, and available resources to achieve an acceptable risk level based on the sensitivity or criticality of the individual systems.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Management Controls
Associated Compliance Components	
List the Compliance Component Names	• Risk Assessment • Security Testing • Risk Mitigation
Associated Product Components	
List the Product Component Names	

TECHNOLOGY AREA DETAIL	
Supporting Documentation	NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems NIST SP 800-30, Risk Management Guide for Information Technology Systems
Document Source Reference #	www.csrc.nist.gov/publications/nistpubs

Standard Organization / 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		
Name		*Website*	
Contact Information			
KEYWORDS			
List Keywords	Control, safeguard, mitigation, threat, impact, vulnerability, cost-benefit, ROI, plan, control, assessment, countermeasure, prevention, threat, scanning, cracking, hacking, log, war, 802.11, wireless, penetration, audit		
CURRENT STATUS			
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	09/29/05	*Date Accepted / Rejected*	03/14/2006
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			