COMPLIANCE COMPONENT

DEFINITION	
Name	Risk Assessment
Description	A risk assessment is used to identify, estimate and prioritize risk to agency operations, assets and individuals resulting from the operation and use of information systems.
Rationale	The purpose of a risk assessment is to inform decision makers and support risk responses by identifying relevant threats to the agency, vulnerabilities both internal and external to the agency, impacts to the agency that may occur given the potential for threats exploiting vulnerabilities and the likelihood that harm will occur.
Benefits	Assists in identifying appropriate controls to reduce or eliminate risk, allowing agencies to make well-informed decisions and justify expenditures for Risk Mitigation.

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	Security Risk Management
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	

State the Guideline, Standard or Legislation	A Risk Assessment encompasses the following steps
	• Step 1 – Prepare for the Assessment
	  ○ Identify Purpose
	  ▪ Response to an event or breach.
	  ▪ Regulatory compliance
	  ▪ Agency policy
	  ○ Identify Scope
	  ▪ Systems or data based on regulation, compliance or agency needs.
	  ○ Identify specific assumptions, constraints, risk tolerance, and priorities/trade-offs used within agencies to make operational decisions.
	  ○ Identify information sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.
	  ○ Identify Risk Model and Analytic Approach
	  ▪ Three types of assessments:
	  • Quantitative

	• Qualitative
	• Semi-quantitative
	• Step 2 – Conduct the Assessment
	  ○ Identify threat sources of concern, including capability, intent and targeting characteristics for different kinds of threats, such as adversarial threats, internally and externally.
	  ○ Identify potential threat events, and any sources that could initiate events, such as a fire or natural disaster.
	  ○ Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.
	  ○ Determine the likelihood that a threat event would occur given the agency's potential vulnerabilities.
	  ○ Determine the adverse impacts from threat events of concern considering the characteristics of the threat sources that could initiate the events, the vulnerabilities/predisposing conditions identified, and the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
	  ○ Determine the risk to the agency from potential threat events, considering the impact that would result from the events and the likelihood of the events occurring.
	• Step 3 – Communicate and Share Risk Assessment Results
	  ○ The agency can communicate risk assessment results in a variety of ways (e.g., executive briefings, risk assessment reports, dashboards).
	  ○ Share risk-related information produced during the risk assessment with appropriate organizational personnel.
	• Step 4 – Maintaining the Risk Assessment
	  ○ Agencies monitor important risk factors on an ongoing basis to ensure that the information needed to make credible, risk-based decisions continues to be available over time. Monitoring risk factors can provide critical information on changing conditions that could potentially affect the ability of agencies to conduct core missions and business functions.
	  ○ Update existing risk assessment using the results from ongoing monitoring of risk factors.
	The Risk Assessment Report is used in the Risk Mitigation phase of the Security Risk Management process.
	This document will be reviewed annually.

Document Source Reference #	NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments (Sep 2012) (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

Compliance Sources			
Name	National Institute of Standards and Technology	*Website*	http://csrc.nist.gov/

	(NIST), Computer Security Resource Center (CSRC)		
Contact Information	inquiries@nist.gov		
KEYWORDS			
List Keywords	Assessment, mitigation, threat, impact, vulnerability, adversarial threats		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Sunset Date			
CURRENT STATUS			
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	03/09/2006	*Date Approved / Rejected*	12/10/2018
Reason for Rejection			
Last Date Reviewed	03/14/2023	*Last Date Updated*	03/16/2023
Reason for Update	Vitality		