



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Risk Assessment
<i>Description</i>	A risk assessment is used to identify, estimate, and prioritize risk to agency operations, assets, and individuals, largely resulting from the operation and use of information systems.
<i>Rationale</i>	The purpose of a risk assessment is to identify relevant threats, internal and external vulnerabilities and impacts to the agency that may occur due to these threats and vulnerabilities.
<i>Benefits</i>	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	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Management Controls
<i>Specify the Technology Area Name</i>	Security Risk Management
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p>A Risk Assessment encompasses the following steps</p> <ul style="list-style-type: none"> • Step 1 – Prepare for the Assessment <ul style="list-style-type: none"> ○ Identify Purpose <ul style="list-style-type: none"> ▪ Response to an event or breach. ▪ Regulatory compliance ▪ Agency policy ○ Identify Scope <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> ▪ Three types of assessments:

	<ul style="list-style-type: none"> • Quantitative • Qualitative • Semi-quantitative <ul style="list-style-type: none"> • Step 2 – Conduct the Assessment <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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. <p>The Risk Assessment Report is used in the Risk Mitigation phase of the Security Risk Management process</p>
<p>Document Source Reference #</p>	<p>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)</p>

Compliance Sources			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	http://csrc.nist.gov/
<i>Contact Information</i>	inquiries@nist.gov		
KEYWORDS			
<i>List Keywords</i>	Assessment, mitigation, threat, impact, vulnerability, adversarial threats		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input type="checkbox"/> <i>Under Review</i>	<input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>
AUDIT TRAIL			
<i>Creation Date</i>	03/09/2006	<i>Date Approved / Rejected</i>	09/23/2021
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>	09/20/2021	<i>Last Date Updated</i>	09/20/2021
<i>Reason for Update</i>	Vitality		