Compliance Component

DEFINITION	
Name	Risk Response
Description	Risk response is how the agency responds to risk once it is determined based on the results of risk assessments.
Rationale	The purpose of the risk response component is to provide a consistent, agency-wide, response to risk in accordance with the organizational risk framework.
Benefits	i) developing alternative courses of action for responding to risk ii) evaluating the alternative courses of action iii) determining appropriate courses of action consistent with agencies' risk tolerance iv) implementing risk responses based on selected courses of action

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

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**Risk Response** - identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to agency operations and assets, individuals, other agencies, and the State, resulting from the operation and use of information systems. **1. Identification** - Identify alternative courses of action to respond to risk determined during the risk assessment. Organizations can respond to risk in a variety of ways. These include: **i)** Risk Acceptance - the appropriate risk response when the identified risk is within the agencies' risk tolerance. **ii)** Risk Avoidance - may be the appropriate risk response when the identified risk exceeds the agencies' risk tolerance. **iii)** Risk Mitigation - the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred. **iv)** Risk Transfer - the appropriate risk response when the agency desires and have the means to shift risk liability and responsibility to other organizations. **v)** Combination of the above **2. Evaluation of Alternatives** - The evaluation of alternative courses of action can include:

	i) Expected effectiveness in achieving desired risk response (and how effectiveness is measured and monitored). ii) Anticipated feasibility of implementation including mission/business impact, political, legal, social, financial, technical, and economic considerations. 3. **Decision** - Decisions on the most appropriate course of action include some form of prioritization. Some risks may be of greater concern than other risks. In that case, more resources may need to be directed at addressing higher-priority risks than at other lower-priority risks. A key part of the risk decision process is the recognition that regardless of the decision, there still remains a degree of residual risk that must be addressed. The agency determines acceptable degrees of residual risk based on their risk tolerance and the specific risk tolerances of particular decision makers. 4. **Implementation** - Once a course of action is selected, the agency implements the associated risk response. Some risk response measures are tactical in nature (e.g., applying patches to identified vulnerabilities in organizational information systems) and may be implemented rather quickly. Other risk response measures may be more strategic in nature and reflect solutions that take much longer to implement. Therefore, organizations apply, and tailor as appropriate to a specific risk response course of action, the risk response implementation considerations in the risk response strategies (part of the risk management strategy developed during the risk framing step).
Document Source Reference #	NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View* (Mar. 2011) NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations. Risk Assessment-7 | Risk Response*

Compliance Sources			
Name	NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*	*Website*	NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
Contact Information			
Name	NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations. Risk Assessment-7 | Risk Response*	*Website*	Security and Privacy Controls for Information Systems and Organizations (nist.gov)
Contact Information			
Name		*Website*	
Contact Information			

KEYWORDS	
List Keywords	Risk, Response, Identification, Evaluation, Decision, Implementation

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	08/03/2023	*Date Approved / Rejected*	10/31/2023	
Reason for Rejection				
Last Date Reviewed	09/21/2023	*Last Date Updated*	10/31/2023	
Reason for Update				