Compliance Component

DEFINITION	
Name	Risk Monitoring
Description	Risk monitoring provides organizations with the means to: (i) Verify compliance (ii) Determine the ongoing effectiveness of risk response measures (iii) Identify risk-impacting changes to organizational information systems and environments of operation.
Rationale	The agency employs risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/executives develop a better understanding of the ongoing risk to the state's operations and assets.
Benefits	Analyzing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

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	1. **Risk Monitoring Strategy -** Develop a risk monitoring strategy for the agency that includes the purpose, type, and frequency of monitoring activities. Organizations implement risk monitoring programs by: a. **Compliance Monitoring** - Verify that required risk response measures are implemented and that information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines are satisfied. b. **Effectiveness Monitoring** - Determine the ongoing effectiveness of risk response measures after the measures have been implemented. c. **Change Monitoring** - Identify changes to agency information systems and the environments in which the systems operate that may affect risk including changes in the feasibility of the ongoing implementation of risk response measures. i. **Information System -** Changes can occur in agency information systems (including hardware, software, and firmware) that can introduce new risk or change existing

	risk. ii. **Environments of Operation -** The environments in which information systems operate can also change in ways that introduce new risk or change existing risk. Environmental and operational considerations include, but are not limited to, missions/business functions, threats, vulnerabilities, mission/business processes, facilities, policies, legislation, and technologies. 2. **Risk Monitoring -** Monitor agency information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes. The particular aspects of monitoring that are performed are dictated largely by the assumptions, constraints, risk tolerance, and priorities/trade-offs established by organizations during the Risk Framing step (see CC – Risk Framework).
Document Source Reference #	NIST SP 800-53, Rev. 5 - *Security and Privacy Controls for Information Systems and Organizations. CA-07(04) Continuous Monitoring | Risk Monitoring* NIST SP 800-39 - *Managing Information Security Risk: Organization, Mission, and Information System View*

Compliance Sources			
Name	NIST SP 800-53, Rev. 5 - *Security and Privacy Controls for Information Systems and Organizations. CA-07(04) Continuous Monitoring | Risk Monitoring*	*Website*	Security and Privacy Controls for Information Systems and Organizations (nist.gov)
Contact Information			
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		*Website*	
Contact Information			

KEYWORDS	
List Keywords	Risk, Monitoring, Strategy, Compliance

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	9/21/2023	*Date Approved / Rejected*	10/31/2023
Reason for Rejection			
Last Date Reviewed	9/21/2023	*Last Date Updated*	10/31/2023
Reason for Update			