Compliance Component

DEFINITION	
Name	Risk Framework
Description	Risk framing is the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an agency's approach for managing risk.
Rationale	Risk framing is informed by the agencies' governance structure, financial posture, legal/regulatory environment, investment strategy, culture, and trust relationships established within and among agencies.
Benefits	The guidance produced by the risk framing step, and the underlying assumptions, constraints, risk tolerances, and priorities/trade-offs used to develop that guidance, may be inappropriate to one or more agency missions or business functions. In addition, the risk environment has the potential to change over time. Thus, the risk management process allows for feedback to the risk framing step from the other steps in the process.

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 Assumptions** - Identify assumptions that affect how risk is assessed, responded to, and monitored within the agency. The agency should identify, characterize, and provide representative examples of threat sources, vulnerabilities, consequences/impacts, and likelihood determinations promote a common terminology and frame of reference for comparing and addressing risks across disparate mission/business areas. 2. **Risk Constraints** - Identify constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the agency. The execution of the risk management process can be constrained in various ways, some of which are direct and obvious, while others are indirect. Financial limitations can constrain the set of risk management activities directly (e.g., by limiting the total resources available for investments in risk assessments or in safeguards or countermeasures) or indirectly (e.g., by eliminating activities which, while involving relatively small investments in risk response, entail curtailing or discarding investments in legacy information systems or information technology). The agency might also discover that the need to continue to depend on legacy information systems may constrain the risk management options available to the agency. Constraints can also include legal, regulatory, and/or contractual requirements.

	3. **Risk Tolerance** - The level of risk that the agency is willing to accept in pursuit of strategic goals and objectives. The agency defines information security-related risk tolerance agency-wide considering all missions/business functions. The agency can use a variety of techniques for identifying information security risk tolerance (e.g., by establishing zones in a likelihood-impact trade space or by using a set of representative scenarios). The agency also defines tolerance for other types of organizational and operational risks (e.g., financial, risk, safety risk, compliance risk, or reputation risk). 4. **Priorities and Trade-Offs** - Identify priorities and trade-offs considered by the agency in managing risk. Risk is experienced at different levels, in different forms, and in different time frames. The agency will have to make trade-offs among and establish priorities for responding to such risks. Agencies tend to have multiple priorities that at times conflict, which generates potential risk. Approaches employed by the agency for managing portfolios of risks reflect organizational culture, risk tolerance, as well as risk-related assumptions and constraints. These approaches are typically embodied in the strategic plans, policies, and roadmaps of agencies which may indicate preferences for different forms of risk response.
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, Program Management-28 Risk Framing*

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	*Website*	Security and Privacy Controls for Information Systems and Organizations (nist.gov)
Contact Information			
Name		*Website*	
Contact Information			

KEYWORDS	
List Keywords	Risk, Framework, Assumptions, Constraints, Tolerance, Priorities, Trade-Off

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			