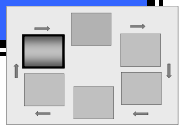
MONITOR STEP – ROLES AND RESPONBILITIES



NIST RISK MANAGEMENT FRAMEWORK

	Title	Role	Responsibilities
Executive Responsibilities	Risk Executive (Function)	Overseer	• Provide oversight to the risk management process to ensure organizational risk to mission and business success is considered in decision making • Provide an organization-wide forum to consider all sources of risk, including aggregated risk from individual information systems • Promote collaboration and cooperation among organizational entities • Facilitate the sharing of security risk-related information among authorizing officials
	CIO	Leader	• Ensure an effective continuous monitoring program is established for the organization • Establish expectations/requirements for the organization's continuous monitoring process • Provide funding, personnel, and other resources to support continuous monitoring • Maintain high-level communications and working group relationships among organizational entities • Ensure that information systems are covered by an approved security plan, are authorized to operate, and are monitored throughout the system development life cycle
Organizational Responsibilities	Senior Agency Information Security Officer/Information Security Program Office	Coordinator	• Establish, implement, and maintain the organization's continuous monitoring program • Develop organizational guidance for continuous monitoring of information systems • Develop configuration guidance for the organization's information technologies • Consolidate and analyze plans of action and milestones to determine organizational security weaknesses and deficiencies • Acquire/develop and maintain automated tools to support security authorization and continuous monitoring • Provide training on the organization's continuous monitoring process • Provide support to information owners/information system owners on how to develop and implement continuous monitoring strategies for their information systems
	Common Control Provider	Monitor	• Develop and document a continuous monitoring strategy for their assigned common controls • Participate in the organization's configuration management process • Establish and maintain an inventory of components associated with the common control • Conduct security impact analyses on all changes that affect their common controls • Conduct security assessments of the common security controls as defined in the common control provider's continuous monitoring strategy • Prepare and submit security status reports at the organization-defined frequency • Conduct remediation activities as necessary to maintain the current authorization status • Update critical security documents on a regular basis and distribute them to individual information owners/ information system owners and other senior leaders

	Title	Role	Responsibilities
System Responsibilities	Authorizing Official	Approver	• Ensure the security posture of the organization's information systems is maintained • Review security status reports and critical security documents and determine if the risk to the organization of operating the system remains acceptable • Determine whether significant information system changes require reauthorization actions for the information system under their purview • Reauthorize information systems when required
	Information Owner/ Information System Owner	Monitor	• Develop and document a continuous monitoring strategy for their information systems • Participate in the organization's configuration management process • Establish and maintain an inventory of the information system's components • Conduct security impact analyses on all changes to their information systems • Conduct security assessments of security controls according to their continuous monitoring strategies • Prepare and submit security status reports at the organization-defined frequency • Conduct remediation activities as necessary to maintain the current authorization status • Update the selection of security controls for the information system when events occur that indicate the baseline set of security controls is no longer adequate to protect the system • Update critical security documents on a regular basis • Review reports from common control providers to verify that the common control continues to provide adequate protection for the information system
	Information System Security Officer	Supporter	• Support the information owner/information system owner to complete security responsibilities • Participate in the formal configuration management process
	Information System Security Engineer	Advisor	• Provide advice on the continuous monitoring of the information system • Provide advice on the impacts of system changes to the security of the system • Participate in the configuration management process • Participate in any acquisition/development activities that are required to implement a system change • Implement approved system changes
	User	Advisor	• Identify changes to mission, business, or operational security requirements • Report any weaknesses in, or new requirements for, current system operations • Submit and justify system change requests to the information owner/information system owner or through the organization's formal configuration management process
	Security Control Assessors	Assessor	• Develop a security assessment plan for each subset of security controls that will be assessed • Submit the security assessment plan for approval prior to conducting the assessment • Conduct the assessment of security controls as defined in the security assessment plan • Update the security assessment report on a regular basis with the continuous monitoring assessment results