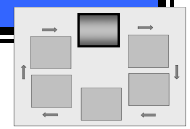
CATEGORIZE STEP – ROLES AND RESPONSIBILITIES

NIST RISK MANAGEMENT FRAMEWORK



	Title	Role	Responsibilities
Executive Responsibilities	Risk Executive (Function)	Overseer	• Provide oversight to the categorization 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 categorization process is established and implemented for the organization • Establish expectations/requirements for the organization's categorization process • Provide resources to support information and information system categorization • Establish organizational relationships and connections • Ensure the information system's categorization is approved prior to selecting and implementing the security controls
Organizational Responsibilities	Senior Agency Information Security Officer/Information Security Program Office	Coordinator	• Establish and implement the organization-wide categorization guidance • Coordinate with the enterprise architecture group to integrate organizational information types into the enterprise architecture • Define organization-specific information types (additional to NIST SP 800-60) and distribute them to information owners/information system owners • Lead the organization-wide categorization process to ensure consistent impact levels for the organization's information systems • Acquire or develop categorization tools or templates • Provide security categorization training
	Common Control Provider	Categorizer	• Determine the most appropriate and cost-effective security category and impact level for the common controls to best accommodate the information systems using the controls • Document the categorization decision in a system security plan or equivalent document • Gain approval for the categorization decision • Maintain the categorization decision

	Title	Role	Responsibilities
System Responsibilities	Authorizing Official	Approver	• Review and approve the security category and impact level assigned to the information types and information system
	Information Owner/ Information System Owner	Categorizer	• Categorize the information system based on FIPS 199, NIST SP 800-60, and organizational guidance • Document the categorization decision • Gain approval for the categorization decision • Maintain the categorization decision
	ISSO	Supporter	• Support the information owner/information system owner to complete security responsibilities
	Information System Security Engineer	Advisor	• Provide advice in establishing or validating the system boundary • Provide advice in describing the information system, its functions, and information types
	User	Advisor	• Identify mission, business, and operational security requirements • Identify data elements and information types contained in the information system • Identify how the information types are used to support the mission/business requirements
	Security Control Assessors	NA	• Not involved in this step