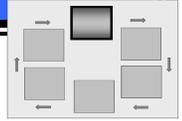


# DRAFT

## CATEGORIZE STEP – ROLES AND RESPONSIBILITIES

### NIST RISK MANAGEMENT FRAMEWORK



	Title	Role	Responsibilities
<b>Executive Responsibilities</b>	Risk Executive (Function)	Overseer	<ul style="list-style-type: none"> <li>• Provide oversight to the categorization process to ensure organizational risk to mission and business success is considered in decision making</li> <li>• Provide an organization-wide forum to consider all sources of risk, including aggregated risk from individual information systems</li> <li>• Promote collaboration and cooperation among organizational entities</li> <li>• Facilitate the sharing of security risk-related information among authorizing officials</li> </ul>
	CIO	Leader	<ul style="list-style-type: none"> <li>• Ensure an effective categorization process is established and implemented for the organization</li> <li>• Establish expectations/requirements for the organization's categorization process</li> <li>• Provide resources to support information and information system categorization</li> <li>• Establish organizational relationships and connections</li> <li>• Ensure the information system's categorization is approved prior to selecting and implementing the security controls</li> </ul>
<b>Organizational Responsibilities</b>	Senior Agency Information Security Officer/Information Security Program Office	Coordinator	<ul style="list-style-type: none"> <li>• Establish and implement the organization-wide categorization guidance</li> <li>• Coordinate with the enterprise architecture group to integrate organizational information types into the enterprise architecture</li> <li>• Define organization-specific information types (additional to NIST SP 800-60) and distribute them to information owners/information system owners</li> <li>• Lead the organization-wide categorization process to ensure consistent impact levels for the organization's information systems</li> <li>• Acquire or develop categorization tools or templates</li> <li>• Provide security categorization training</li> </ul>
	Common Control Provider	Categorizer	<ul style="list-style-type: none"> <li>• 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</li> <li>• Document the categorization decision in a system security plan or equivalent document</li> <li>• Gain approval for the categorization decision</li> <li>• Maintain the categorization decision</li> </ul>

# DRAFT

	Title	Role	Responsibilities
<b>System Responsibilities</b>	Authorizing Official	Approver	<ul style="list-style-type: none"><li>Review and approve the security category and impact level assigned to the information types and information system</li></ul>
	Information Owner/ Information System Owner	Categorizer	<ul style="list-style-type: none"><li>Categorize the information system based on FIPS 199, NIST SP 800-60, and organizational guidance</li><li>Document the categorization decision</li><li>Gain approval for the categorization decision</li><li>Maintain the categorization decision</li></ul>
	ISSO	Supporter	<ul style="list-style-type: none"><li>Support the information owner/information system owner to complete security responsibilities</li></ul>
	Information System Security Engineer	Advisor	<ul style="list-style-type: none"><li>Provide advice in establishing or validating the system boundary</li><li>Provide advice in describing the information system, its functions, and information types</li></ul>
	User	Advisor	<ul style="list-style-type: none"><li>Identify mission, business, and operational security requirements</li><li>Identify data elements and information types contained in the information system</li><li>Identify how the information types are used to support the mission/business requirements</li></ul>
	Security Control Assessors	NA	<ul style="list-style-type: none"><li>Not involved in this step</li></ul>