## **SELECT STEP – ROLES AND RESPONBILITIES**

## NIST RISK MANAGEMENT FRAMEWORK

1

	l
	-

	Title	Role	Responsibilities
Executive Responsibilities	Risk Executive (Function)	Overseer	<ul> <li>Define the organization's risk management strategy with respect to the selection of security controls</li> <li>Promote the use of common controls to more effectively use organizational resources</li> <li>Promote collaboration and cooperation among organizational entities</li> </ul>
	CIO	Leader	<ul> <li>Establish expectations for the security control selection and ongoing monitoring processes to provide a more consistent identification of security controls throughout the organization</li> <li>Provide resources as needed to support information system owners when selecting security controls</li> <li>Ensure the organization's risk management strategy is integrated into the enterprise architecture</li> <li>Participate in the selection and approval of organizational level common security controls</li> <li>Maintain organizational relationships and connections</li> </ul>
Organizational Responsibilities	Senior Information Security Officer/ Information Security Program Office	Coordinator	<ul> <li>Develop organization-wide security control selection guidance consistent with the organization's risk management strategy</li> <li>Assign responsibility for common controls to individuals or organizations</li> <li>Establish and maintain a catalog of the organization's common security controls</li> <li>Review the common security controls periodically and, when necessary, update the common security control selections</li> <li>Define and disseminate organization-defined parameter values for relevant security controls</li> <li>Acquire/develop and maintain tools, templates, or checklists to support the security control selection process and the development of system security plans</li> <li>Develop an organization-wide continuous monitoring strategy</li> <li>Provide training on selecting security controls and documenting them in the security plan</li> <li>Lead the organization's process for selecting security controls consistent with the organizational guidance</li> </ul>
Reo	Common Control Provider	Selector	<ul> <li>Tailor and supplement the common security controls following organizational guidance</li> <li>Document the assigned common security controls for the organization in sufficient detail to enable a compliant implementation of the control and maintain the documentation</li> <li>Disseminate the security documentation associated with the common controls to information system owners that employ the common control in their information system</li> <li>Define the continuous monitoring strategy for the common controls</li> </ul>

	Title	Role	Responsibilities
System Responsibilities	Authorizing Official	Approver	<ul> <li>Review the security plan to determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system</li> <li>Determine if the security plan correctly identifies the potential risk to organizational operations, assets, individuals, other organizations, and the Nation and recommend changes to the plan if it is insufficient</li> <li>Approve the selected set of security controls, including all tailoring and supplementation decisions, any use restrictions, and the minimum assurance requirements</li> </ul>
	Information Owner/ Steward/Information System Owner	Selector	<ul> <li>Select, tailor, and supplement the security controls following organizational guidance, documenting the decisions in the security plan with appropriate rationale for the decisions</li> <li>Determine the suitability of common controls for use in the information system</li> <li>Determine the need for use restrictions in the information system</li> <li>Determine the assurance measures that meet the NIST SP 800-53 minimum assurance requirements selected for the system</li> <li>Document the tailored and supplemented set of security controls in the security plan in sufficient detail to enable a compliant implementation of the control</li> <li>Define the continuous monitoring strategy for the information system</li> <li>Obtain approval for the tailored and supplemented security controls, common controls, compensating controls, use restrictions, and assurance requirements prior to their implementation</li> <li>Review the security controls periodically and, when necessary, update the security control selections</li> <li>Maintain and update the system security plan</li> </ul>
	ISSO	Supporter	<ul> <li>Support the information system owner in selecting security controls for the information system</li> <li>Participate in the selection of the organization's common security controls and in determining their suitability for use in the information system</li> <li>Review the security controls regarding their adequacy in protecting the information and information system</li> </ul>
	Information System Security Engineer	Advisor	<ul> <li>Provide advice in describing the system and its functions, information types, operating environments, and security requirements</li> <li>Review the adequacy of the security controls and their ability to protect the information system and its information</li> <li>Assist in tailoring the security controls</li> <li>Assist in determining the assurance measures that can be used to meet the minimum assurance requirements</li> </ul>
	Information Security Architect	Advisor	• Ensure the selection of security controls is consistent with the enterprise architecture, including reference models and segment and solution architectures
	User	Advisor	<ul> <li>Identify mission, business, or operational security requirements</li> <li>Report any weaknesses in, or new requirements for, current system operations</li> </ul>
	Security Control Assessor/Assessment Team	Assessor	Not involved in selecting security controls

January 18, 2011