# Select Step – Roles and Responsibilities

## NIST Risk Management Framework

<table>
<thead>
<tr>
<th>Title</th>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Executive Responsibilities</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Risk Executive (Function) | Overseer | - Define the organization’s risk management strategy with respect to the selection of security controls  
- Promote the use of common controls to more effectively use organizational resources  
- Promote collaboration and cooperation among organizational entities |
| CIO | Leader | - Establish expectations for the security control selection and ongoing monitoring processes to provide a more consistent identification of security controls throughout the organization  
- Provide resources as needed to support information system owners when selecting security controls  
- Ensure the organization’s risk management strategy is integrated into the enterprise architecture  
- Participate in the selection and approval of organizational level common security controls  
- Maintain organizational relationships and connections |
| **Organizational Responsibilities** | | |
| Senior Information Security Officer/Information Security Program Office | Coordinator | - Develop organization-wide security control selection guidance consistent with the organization’s risk management strategy  
- Assign responsibility for common controls to individuals or organizations  
- Establish and maintain a catalog of the organization’s common security controls  
- Review the common security controls periodically and, when necessary, update the common security control selections  
- Define and disseminate organization-defined parameter values for relevant security controls  
- Acquire/develop and maintain tools, templates, or checklists to support the security control selection process and the development of system security plans  
- Develop an organization-wide continuous monitoring strategy  
- Provide training on selecting security controls and documenting them in the security plan  
- Lead the organization’s process for selecting security controls consistent with the organizational guidance |
| Common Control Provider | Selector | - Tailor and supplement the common security controls following organizational guidance  
- Document the assigned common security controls for the organization in sufficient detail to enable a compliant implementation of the control and maintain the documentation  
- Disseminate the security documentation associated with the common controls to information system owners that employ the common control in their information system  
- Define the continuous monitoring strategy for the common controls |
<table>
<thead>
<tr>
<th>Title</th>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Authorizing Official                      | Approver      | • Review the security plan to determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system  
• 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  
• Approve the selected set of security controls, including all tailoring and supplementation decisions, any use restrictions, and the minimum assurance requirements |
| Information Owner/Steward/Information System Owner | Selector      | • Select, tailor, and supplement the security controls following organizational guidance, documenting the decisions in the security plan with appropriate rationale for the decisions  
• Determine the suitability of common controls for use in the information system  
• Determine the need for use restrictions in the information system  
• Determine the assurance measures that meet the NIST SP 800-53 minimum assurance requirements selected for the system  
• Document the tailored and supplemented set of security controls in the security plan in sufficient detail to enable a compliant implementation of the control  
• Define the continuous monitoring strategy for the information system  
• Obtain approval for the tailored and supplemented security controls, common controls, compensating controls, use restrictions, and assurance requirements prior to their implementation  
• Review the security controls periodically and, when necessary, update the security control selections  
• Maintain and update the system security plan |
| ISSO                                      | Supporter     | • Support the information system owner in selecting security controls for the information system  
• Participate in the selection of the organization’s common security controls and in determining their suitability for use in the information system  
• Review the security controls regarding their adequacy in protecting the information and information system |
| Information System Security Engineer      | Advisor       | • Provide advice in describing the system and its functions, information types, operating environments, and security requirements  
• Review the adequacy of the security controls and their ability to protect the information system and its information  
• Assist in tailoring the security controls  
• Assist in determining the assurance measures that can be used to meet the minimum assurance requirements |
| 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       | • Identify mission, business, or operational security requirements  
• Report any weaknesses in, or new requirements for, current system operations |
| Security Control Assessor/Assessment Team  | Assessor      | • Not involved in selecting security controls |