NIST Risk Management Framework Quick Start Guide

ROLES AND RESPONSIBILITIES CROSSWALK

(October 1, 2021)

NIST National Institute of Standards and Technology
U.S. Department of Commerce

ITL INFORMATION TECHNOLOGY LABORATORY

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

Legend:

P:	Prepare (step)
C:	Categorize (step)
S:	Select (step)
I:	Implement (step)
A:	Assess (step)
R:	Authorize (step)
M:	Monitor (step)
ORG:	Organizational (responsibility)
SYS:	System (responsibility)

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

Index:

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
HEAD OF AGENCY	X							X		• Designate a senior accountable official for risk management, senior agency official for privacy, and chief acquisition officer • Oversee risk management process • Provide an organization-wide forum to consider all sources of risk, and to promote collaboration and cooperation • Institute a commitment to effectively manage security and privacy risk • Coordinate with risk executive (function) to establish a risk management strategy
MISSION OR BUSINESS OWNER	X							X		• Assist in development of organization-wide tailored control baselines and/or profiles (Task P-4 [*Optional*])
	X								X	• Define mission and business functions and processes that the system is intended to support
ENTERPRISE ARCHITECT	X							X		• Implement an enterprise architecture strategy that facilitates effective security and privacy solutions • Collaborate with system owners and authorizing officials to facilitate authorization boundary determinations • Coordinate with security and privacy architects on security and privacy issues
	X								X	• Determine placement of system within the enterprise architecture
SECURITY OR PRIVACY ARCHITECT								X		• Liaise between the enterprise architect and the system security or privacy engineer • Allocate controls in coordination with system owners, common control providers, and system security or privacy officers • Advise senior leadership on a range of security and privacy issues • Manage aspects of the enterprise architecture that protect information and systems from unauthorized system activity or behavior; that ensure compliance with privacy requirements; and that manage privacy risks to individuals associated with the processing of personally identifiable information

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
CHIEF ACQUISITION OFFICER				X				X		• Manage and monitor the performance of acquisition programs and activities • Establish clear lines of authority, accountability, and responsibility for acquisition decision-making • Establish procurement policies, procedures, and practices • Ensure that security and privacy requirements are defined in organizational procurements and acquisitions

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
COMMON CONTROL PROVIDER *(continues next page)*			X					X		• Tailor and supplement the common controls following organizational guidance • Document the assigned common 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 system owners that employ the common control in their system • Define the continuous monitoring strategy for the common controls
				X				X		• Provide safeguards responsible for detecting, reporting, and investigating information security incidents • Provide evaluation to information owner/steward that explains economical value of implemented controls • Implement the controls defined by the information owner/steward over the specified data
					X			X		• Determine which findings, if any, present no harm to the organization • Select control assessors based on technical expertise and level of independence • Ensure that assessors have proper access to common control information • Determine initial remediation actions and prioritization based on control assessment findings • Resolve issues found during control assessments • Review the security and privacy assessment plans to ensure appropriate assessment depth and coverage
						X		X		• Provide system owner common control information and documentation to place in authorization package assembly • Update plans for common controls to provide near-real time risk management and ongoing authorization

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **COMMON CONTROL PROVIDER**							X	X		• 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 controls • Monitor common controls • Conduct assessments of the common controls as defined in the common control provider's continuous monitoring strategy • Prepare and submit security and privacy posture reports at the organization-defined frequency • Conduct remediation activities as necessary to maintain the current authorization status • Update critical security and privacy documentation on a regular basis and distribute them to individual information owners/system owners and other senior leaders

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
CHIEF INFORMATION OFFICER	X							X		• Ensure that an effective security program is established for the organization, including expectations and requirements • Designate a Senior Agency Information Security Officer • Ensure an appropriate level of funding and resources to support a robust security program • Determine mission and business function of the organization based on organizational priorities
		X						X		• Cooperate and collaborate with system owners and the information owner or steward in the security categorization process.
			X					X		• Establish expectations for the control selection and ongoing monitoring processes to provide a more consistent identification of controls throughout the organization • Provide resources as needed to support system owners during the process of selecting controls • Maintain organizational relationships and connections • Participate in the selection and approval of organization-level common controls
					X			X		• Help guide and inform authorizing official decisions regarding assessor independence.
							X	X		• 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 systems are covered by an approved security plan, are authorized to operate, and are monitored throughout the system development life cycle

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
RISK EXECUTIVE (FUNCTION) OR SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT *(continues next page)*	X							X		*(Risk Executive [function])* • Assess ongoing organization-wide security and privacy risk • Develop and implement an organization-wide strategy for continuously monitoring control effectiveness • Provide input to head of agency to determine organizational risk management strategy • Identify, document, and publish organization-wide common controls • Develop organization-wide tailored control baselines and/or profiles (Task P-4 [*Optional*]) • Coordinate with the senior accountable official for risk management to prioritize organizational systems with the same impact level (Task P-6 [*Optional*]) • Participate in organization-wide forums to consider all types and sources of risk
	X							X		*(Senior Accountable Official for Risk Management)* • Implement a comprehensive continuous monitoring program to maintain the initial system or common control authorizations as well as security and privacy reporting requirements and recipients • Identify, document, and publish organization-wide common controls • Provide input to head of agency to determine organizational risk management strategy • Assess ongoing organization-wide security and privacy risk • Review, approve, and publish organization-wide tailored control baselines and/or profiles (Task P-4 [*Optional*]) • Align information security management processes with strategic, operational, and budgetary planning processes • Lead the risk executive (function)

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **RISK EXECUTIVE (FUNCTION) OR SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT**		X						X		• Provide oversight to the categorization process to that 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 systems • Promote collaboration and cooperation among organizational entities • Facilitate the sharing of security risk-related information among authorizing officials • Coordinate with system owner for organizational system impact levels and system prioritization • Coordinate with the authorizing official to ensure that the categorization decision is appropriate for the organizational risk management strategy and satisfies requirements for high value assets
			X					X		• Define the organization's risk management strategy and ensure the selection of controls is consistent with the strategy • Promote the use of common controls to more effectively use organizational resources • Integrate the organization's risk management strategy into the enterprise architecture • Promote collaboration and cooperation among organizational entities
						X		X		• Provide input to the authorization official on whether the risk of operating a system is acceptable • Provide information to the authorizing official that is considered in the final determination of risk from the operation or use of the system or the provision of common controls
							X	X		• 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 systems • Promote collaboration and cooperation among organizational entities • Facilitate the sharing of security risk-related information among authorizing officials

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SENIOR AGENCY INFORMATION SECURITY OFFICER *(continues next page)*	X							X		• Support an organization-wide forum to consider all sources of risk • Coordinate with senior agency official for risk management • Coordinate with senior agency official for privacy to ensure coordination between privacy and information security programs • Serve as liaison between organization risk management roles and system level risk management roles • Identify, document, and publish organization-wide common controls
		X						X		• 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/system owners • Lead the organization-wide categorization process to ensure consistent impact levels for the organization’s systems • Acquire or develop categorization tools or templates • Provide security categorization training
			X					X		• Develop organization-wide control selection guidance • Assign responsibility for common controls to individuals or organizations • Establish and maintain a catalog of the organization’s common controls • Review the common controls periodically and, when necessary, update the common control selections • Define and disseminate organization-defined parameter values for relevant controls • Acquire/develop and maintain tools, templates, or checklists to support the control selection process and the development of system security plans • Develop a continuous monitoring strategy for the organization • Provide training on selecting controls and documenting them in the security plan • Lead the organization’s process for selecting controls consistent with the organizational guidance

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **SENIOR AGENCY INFORMATION SECURITY OFFICER**						X		X		• Recommend potential response actions to authorizing official • Provide input to the authorizing official on appropriate risk determinations • Provide input to the authorization official if the risk of operating a system is acceptable or not • Assist with assembly of the authorization package by providing input to system owner as needed • Provide input to the authorizing official to determine risk from the operation or use of the system or common control provisions • Serve as liaison between authorizing official and the chief information officer • Serve as authorizing official designated representative, if needed
							X	X		• Establish, implement, and maintain the organization’s continuous monitoring program • Develop organizational guidance for continuous monitoring of 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/system owners on how to develop and implement continuous monitoring strategies for their systems

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SENIOR AGENCY OFFICIAL FOR PRIVACY *(continues next page)*	X							X		• Assign individuals to specific roles associated with privacy risk management and ensure no conflict of interest in privacy risk management roles • Assess ongoing, organization-wide privacy risk • Provide input and review to organization-wide tailored privacy control baselines (Task P-4 [*Optional*]) • Identify, document, and publish organization-wide common privacy common controls • Support establishment of criteria for determining the minimum frequency for control monitoring in collaboration with organizational officials • Identify all stages of the information life cycle • Ensure compliance with applicable privacy requirements and managing privacy risk • Coordinate with senior agency information security officer on privacy and information security activities
	X								X	• Support the definition of the privacy requirements for the system and environment of operation
		X						X		• Review and approve the security categorization results and decision for systems processing personally identifiable information prior to the Authorizing Official review
			X					X		• Designate which privacy controls will be treated as program management, common, system-specific, and hybrid privacy controls
					X			X		• Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks • Conduct assessments of privacy controls and document results, or delegate assessment functions, consistent with applicable policies

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **SENIOR AGENCY OFFICIAL FOR PRIVACY**						X		X		• Review authorization packages for systems processing personally identifiable information to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions • Collaborate with the authorizing official or designated representative to analyze the information in the authorization package provided by the control assessor, system owner, or common control provider, and finalize the determination of risk
							X	X		• Establish and maintain a privacy continuous monitoring program to ensure compliance with privacy requirements and manage privacy risks

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
AUTHORIZING OFFICIAL OR AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE *(continues next page)*	X								X	• Determine the authorization boundary of the system.
		X							X	• Review and approve the security category and impact level assigned to the information types and system • Ensure that the security category selected for the system is consistent with the mission and business functions of the organization, and protect those missions and business functions • Coordinate with senior agency official for risk management or the risk executive (function) to ensure that categorization decisions for the system is commensurate with the organizational risk management strategy and satisfies requirements for high-value assets • Provide guidance system owner for any limitations on baseline tailoring activities for the system that occur at the RMF Select step
			X						X	• Review the security and privacy plans to determine if the plans are complete, consistent, and satisfy the stated security and privacy requirements for the system • Determine if the security and privacy plans correctly identify the potential risk to organizational operations, assets, individuals, other organizations, and the Nation and recommend changes to the plans if insufficient • Approve the selected set of controls, including all tailoring and supplementation decisions, any use restrictions, and the minimum assurance requirements • Determine the need to reauthorize the system after significant events occur that may trigger changes to the system's controls

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **AUTHORIZING OFFICIAL OR AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE**					X				X	• Define the level of independence required for the control assessor(s) • Determine confidence in independent assessor's ability to provide relevant information about the security and privacy posture of the system to support risk-based decisions • Determine risk to organizational operations and assets, individuals, and other organizations based on assessment results • Review and approve security and privacy assessment plan • Decide which findings are significant and require immediate action • Approve use of any previous assessment results

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide

Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **AUTHORIZING OFFICIAL OR AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE**						X			X	• Collaborate with the senior agency information security officer and the senior agency official for privacy (for systems processing personally identifiable information), analyzes the information in the authorization package to finalize the risk determination • Coordinate with the chief information officer to ensure adequate protection of resources to meet system supporting mission and business functions supporting organization priorities • Analyze the relevant security and privacy information provided by security/privacy personnel (or a reporting tool if utilized) to determine the current security and privacy posture of the system when in ongoing authorization • Review assessment reports and plans of action and milestones for risk mitigation prior to authorization • Review the information with the specific time-driven authorization frequency defined by the organization as part of the continuous monitoring strategy and determines if the risk of continued system operation or the provision of common controls remains acceptable • Identify and implement a preferred course of action in response to the risk determination • Consult with senior accountable official for risk management or risk executive (function) prior to making final authorization decision for the system or common controls • Determine acceptance of risk; risk acceptance cannot be delegated to other officials • Issue an authorization decision for the system or for organization-designated common controls • Convey the authorization decision to the system owner or common control provider, and other organizational officials, as appropriate • Determine the authorization termination date for systems not in ongoing authorization *(continues next page)*

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **AUTHORIZING OFFICIAL OR AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE**						X			X	• Provide the terms and conditions for authorization decision with any applicable specific limitations or restrictions placed on the operation of the system or the controls that must be followed by the system owner or common control provider • Issue the final authorization decision for the system • Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk to designated organization officials
AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE						X			X	• Conduct and coordinate response actions on behalf of authorizing official except signing of authorization decision document (acceptance of risk) • Serve as alternate for authorizing official for risk determination and mitigation and authorization reporting

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **AUTHORIZING OFFICIAL OR AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE**							X		X	• Ensure the security and privacy posture of the organization's systems is maintained • Review security and privacy posture reports and critical security documents and determine if the risk to the organization of operating the system remains acceptable • Determine whether significant system changes require reauthorization actions for the system under their purview • Reauthorize systems when required

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
INFORMATION OWNER OR STEWARD *(continues next page)*	X								X	• Identify the types of information to be processed, stored, and transmitted by the system • Coordinate with the senior agency official for privacy to identify all parts of the information life cycle for personally identifiable information • Coordinate with system owners and provide input on protection needs, security and privacy requirements
		X							X	• Assist the system owner to categorize the system based on FIPS 199, NIST SP 800-60, and organizational guidance
			X						X	*(or System Owner)* • Select, tailor, and supplement the controls following organizational guidance, documenting the decisions in the security and privacy plans with appropriate rationale for the decisions • Determine the suitability of common controls for use in the system • Determine the need for use restrictions in the system • Document the tailored and supplemented set of controls in the security and privacy plans in sufficient detail to enable a compliant implementation of the control • Define the continuous monitoring strategy for the system • Obtain approval for the tailored and supplemented controls, common controls, compensating controls, use restrictions, and assurance requirements prior to their implementation • Review the controls periodically and, when necessary, update the control selections • Maintain and update the system security and privacy plans

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **INFORMATION OWNER OR STEWARD**				X					X	*(or system owner)* • Implement and verify controls to ensure the confidentiality, integrity and availability of the system; manage privacy risks; and ensure compliance with applicable privacy requirements • Provide the appropriate level of authority to implement the controls to the system • Review and approve access to the system based on need • Coordinate exceptions to implemented controls • Document control implementation to allow for traceability of decisions prior to and after deployment of the system • Coordinate the control assessment in parallel with development to facilitate early detection of weak or inefficient controls • Refer to authorization package to determine adequacy of implemented common controls • Identify compensating or additional controls to enhance protection levels not met by inherited common controls • Ensure the system is protected from unauthorized disclosure, modification or deletion • Provide the appropriate level of authority to implement the controls to the system • Approve access, based on necessity, to the system • Coordinate exceptions to implemented controls • Document control implementation to allow for traceability of decisions prior to and after deployment of the system • Provide input to system owners regarding the security and privacy requirements and controls for the system • Offer controls for inheritance (as needed)

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **INFORMATION OWNER OR STEWARD**					X				X	*(or System Owner)* • Understand what information will be assessed and how that information will be assessed • Understand how the information that is going to be evaluated will be affected during the assessment • Review the security and privacy assessment plans for consistency with the information security and privacy requirements • Determine which findings, if any, present no harm to the organization • Select control assessors based on technical expertise and level of independence • Ensure that assessors have proper access to the system and/or operating environment • Determine initial remediation actions and prioritization based on control assessment findings • Resolve issues found during control assessments • Review the security and privacy assessment plans to ensure appropriate assessment depth and coverage • Provide support for security and privacy assessment activities • Ensure security and privacy assessments activities are proceeding as planned • Determine if any previous assessments results are available and may be relevant • Ensure that control assessments are conducted in parallel with the development/acquisition and implementation phases of the life cycle • Ensure that the control assessor provide a complete control assessment report

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **INFORMATION OWNER OR STEWARD**						X			X	*(or System Owner)* • Provide input to plan of action and milestone development for information protection • Assemble the authorization package with common control provider and senior agency official for privacy for submission to authorizing official for final authorization decision • Present the authorizing official via automated reports (if applicable) the authorization package for those systems under ongoing authorization • Receive authorization decision from authorizing official on system operations. Authorization decision includes whether system is authorized to operate or not via final authorization package. • Receive guidance from authorizing official when to conduct an authorization or re-authorization • Report and track exploitable deficiencies (i.e., vulnerabilities) in the system or controls found out during the assessment and continuous monitoring that have significant security or privacy risk to the authorizing official • Take system off-line to address system deficiencies and revise authorization package to authorizing official's satisfaction if system is issued authorization to operate.

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **INFORMATION OWNER OR STEWARD**							X		X	*(or System Owner)* • Develop and document a continuous monitoring strategy for their systems • Participate in the organization's configuration management process • Establish and maintain an inventory of the system's components • Conduct risk assessments on all changes to their systems • Conduct control assessments 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 controls for the system when events occur that indicate the baseline set of controls is no longer adequate to protect the system • Update critical security and privacy documents on a regular basis • Review reports from common control providers to verify that the common control continues to provide adequate protection for the system

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SYSTEM OWNER *(continues next page)*	X								X	• Identify stakeholders who have an interest in the system • Identify assets that require security and privacy protection • Assist senior agency official for privacy to identify systems that process personally identifiable information • Identify the types of information to be processed, stored, and transmitted by the system • Conduct a system-level risk assessment and continually update the risk assessment • Define the protection needs and security and privacy requirements for the system • Register the system with organizational program or management offices

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

INDEX

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
(continued from previous page) **SYSTEM OWNER**		X							X	• Categorize system based and document results with input from information owner or steward • Collaborate with senior leaders and executives to ensure system categorization is based on mission and business impacts of the organization • Review security risk assessment results to help determine security categorization • Coordinate with information owner to determine impact levels for each information type and each security objective • Determine overall system categorization based on high water mark of information type impact levels • Ensure security categorization is documented in the system security plan and cross-referenced in a privacy plan, if applicable • Review impact-prioritization and coordinate with senior accountable official for risk management or risk executive (function) in control selection and tailoring decisions • Initiate and repeat categorization process and submits adjusted results to authorizing official if initial security categorization decision is not approved • Update system registration with approved security categorization and characterization information • Document characteristics of the system (e.g., system design and requirements documentation; authorization boundary information; list of security and privacy requirements allocated to the system, system elements, and the environment of operation; system element information) in appropriate documentation (e.g., system security plan) • Ensure level of detail for system documentation is commensurate with security categorization and security and privacy risk assessments

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SYSTEM SECURITY OR PRIVACY OFFICER	X								X	• Coordinate with the system owner to determine the authorization boundary and information types • Conduct system-level security and privacy risk assessments
			X						X	• Support the system owner in selecting controls for the system • Participate in the selection of the organization's common controls and in determining their suitability for use in the system • Review the controls regarding their adequacy in protecting the information and system
				X					X	• Assist in the determination of an appropriate level of security commensurate with the impact level • Advise the system owner regarding security and privacy requirements
					X				X	• Oversee implementation of remediation action • Review the security and privacy assessment plans to coordinate assessment activities • May act as the control assessor for low impact systems • Coordinate security and privacy assessment activities • Coordinate security and privacy assessment report detail with the assessor
							X		X	• Support the information owner/system owner to complete security responsibilities • Participate in the formal configuration management process

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SYSTEM SECURITY OR PRIVACY ENGINEER			X						X	• Provide advice in describing the system and its functions, information types, operating environments, and security and privacy requirements • Review the adequacy of the controls and their ability to protect the system and its information, manage privacy risk, and ensure compliance with applicable privacy requirements • Assist in tailoring the controls
				X					X	• Ensure the confidentiality, integrity, and availability of the system by designing and implementing a secure system • Ensure system compliance with privacy requirements and management of the privacy risks to individuals associated with the processing of PII • Implement secure and privacy-enhancing networking and computing environments • Provide security and privacy planning to support the system • Implement security and privacy requirements for the proper handling of data within the system • Recommend system-level solutions to resolve security and privacy requirements • Coordinate the most effective way to implement common controls in organizational systems
					X				X	• Verify that the system protects individual's privacy and against identified • Review and analyze security and privacy assessment reports • Design remediation plan • Verify remediation
							X		X	• Provide advice on the continuous monitoring of the system • Provide advice on the impacts of system changes to the security and privacy posture 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

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

INDEX

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SYSTEM ADMIN.	X								X	• Identify assets that require protection
				X					X	• Implement the controls in the security and privacy plans • Document changes to planned control implementations based on the “as-implemented” state of controls.
USER			X						X	• Identify mission, business, or operational security requirements • Report any weaknesses in, or new requirements for, current system operations
							X		X	• Identify changes to mission, business, or operational security and privacy requirements • Report any weaknesses in, or new requirements for, current system operations • Submit and justify system change requests to the information owner/system owner or through the organization’s formal configuration management process
CONTROL ASSESSOR *(internal or independent)*					X					• Develop security and privacy assessment plan(s) • Conduct assessment of the controls used in and/or inherited by a system • Create security and privacy assessment report(s) reflecting effectiveness of employed and inherited controls • Reassess any weak or deficient controls that have been corrected • Note: the senior agency official for privacy is responsible for assessing privacy controls. At the discretion of the organization, privacy controls may be assessed by an independent assessor
							X			• Develop a security and privacy assessment plan(s) for each subset of controls that will be assessed • Submit the security and privacy assessment plan(s) for approval prior to conducting the assessment • Conduct the assessment of controls as defined in the security and privacy assessment plan(s) • Update the security and privacy assessment report(s) on a regular basis with the continuous monitoring assessment results

Steps—**P:** Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility**—**ORG**: Organizational; **SYS**: System

NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

PREPARE
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR

NIST
RMF
RISK MANAGEMENT FRAMEWORK

nist.gov/rmf