PNNL-28347

Pacific Northwest
NATIONAL LABORATORY

Risk Management Framework Process Map

Prepared for the Federal Energy Management Program

November 2018

ME Mylrea
SNG Gourisetti
M Touhiduzzaman
MD Watson
JE Castleberry

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

Acronyms and Abbreviations

AO	Authorizing Official
ISO	Information System Owner
ISSO	Information System Security Officer
NIST	National Institute of Standards & Technology
POA&M	Plan of Action and Milestones
RAR	Risk Assessment Report
RMF	Risk Management Framework
SAR	Security Assessment Report
SCA	Security Control Assessor
SCTM	Security Controls Traceability Matrix
SP	Special Publication
SSP	System Security Plan

Contents

Figures

Tables

1.0 Introduction

The purpose of this document is to provide an overview of the Risk Management Framework (RMF) codified in National Institute of Standards & Technology (NIST) Special Publication (SP) 800-37r1 for the Federal Energy Management Program (FEMP). This document, while accurate, is not an authoritative source on the management of federal information systems. However, the concepts and process discussed herein are representative of the data points used to compare the RMF with NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, otherwise known as the *cybersecurity framework*.

2.0 The Risk Management Framework

The RMF is a six-step process meant to guide individuals responsible for mission processes, whose success is dependent on information systems, in the development of a cybersecurity program. Among other things, the RMF promotes near-real-time risk management of information systems; links risk management processes at the system level with the organization's strategic goals and risk function; and establishes responsibility for security controls for information systems within the organization's defined boundary (NIST 2010). Figure 1 shows the iterative nature of the six-step RMF process.

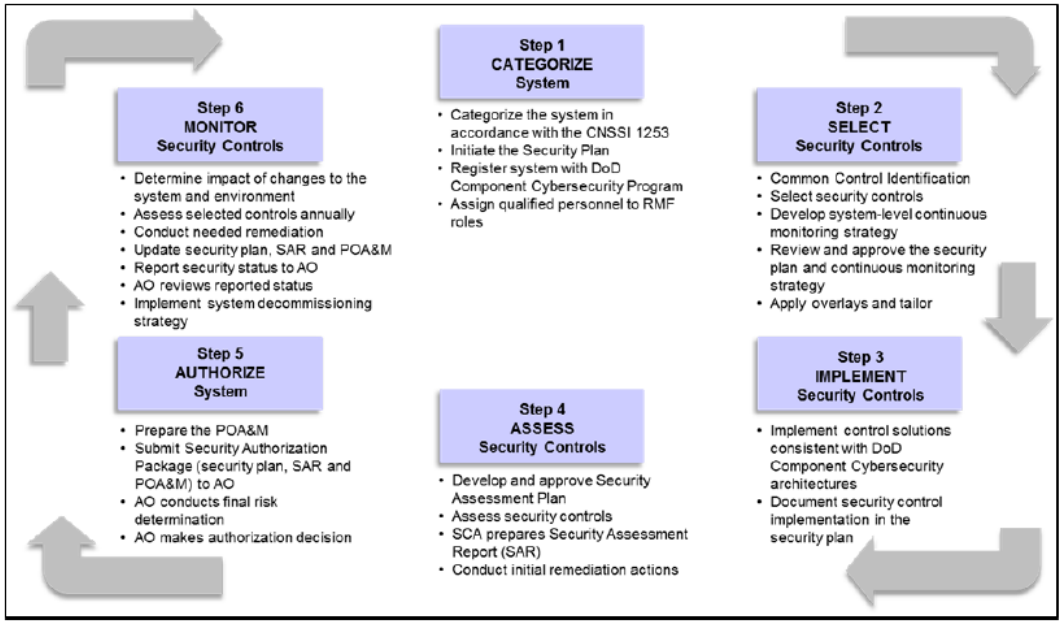

Figure 1. RMF for Information and Platform Information Technology Systems (NIST, 2010)

The RMF is a living, comprehensive process that requires an appropriate amount of due diligence to be effective. Figure 2 depicts the available NIST authored guidance documents to assist in each step of the RMF process.

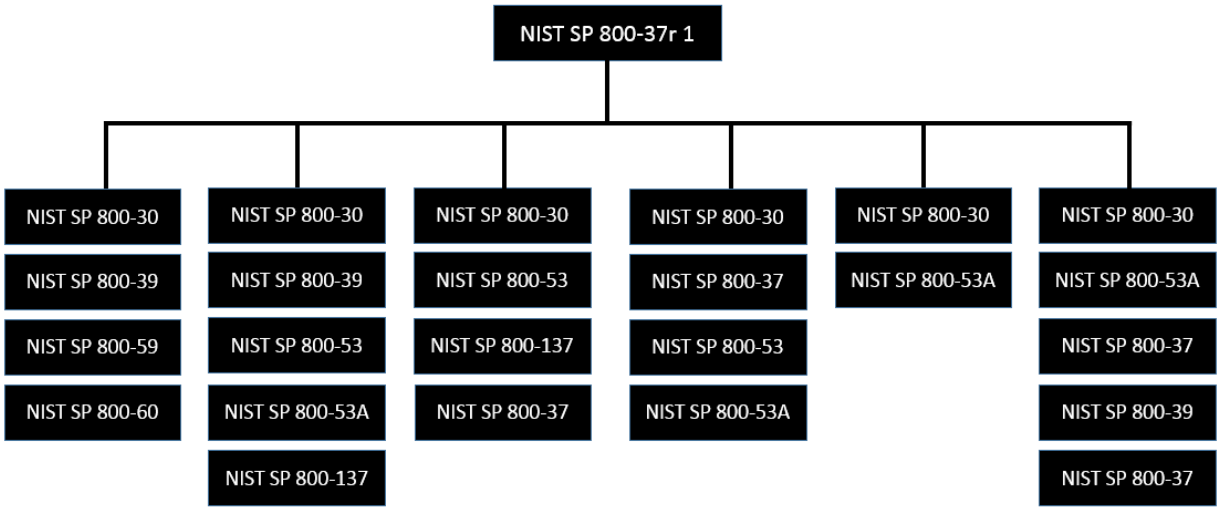

Figure 2. Document Mapping for RMF

A core concept to the RMF is risk management. The RMF makes use of NIST SP 800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View*. Enterprise risk management involves a multitiered approach connecting strategic goals with the daily operations of information systems. Figure 3 depicts this structured risk management process (NIST 2011b).

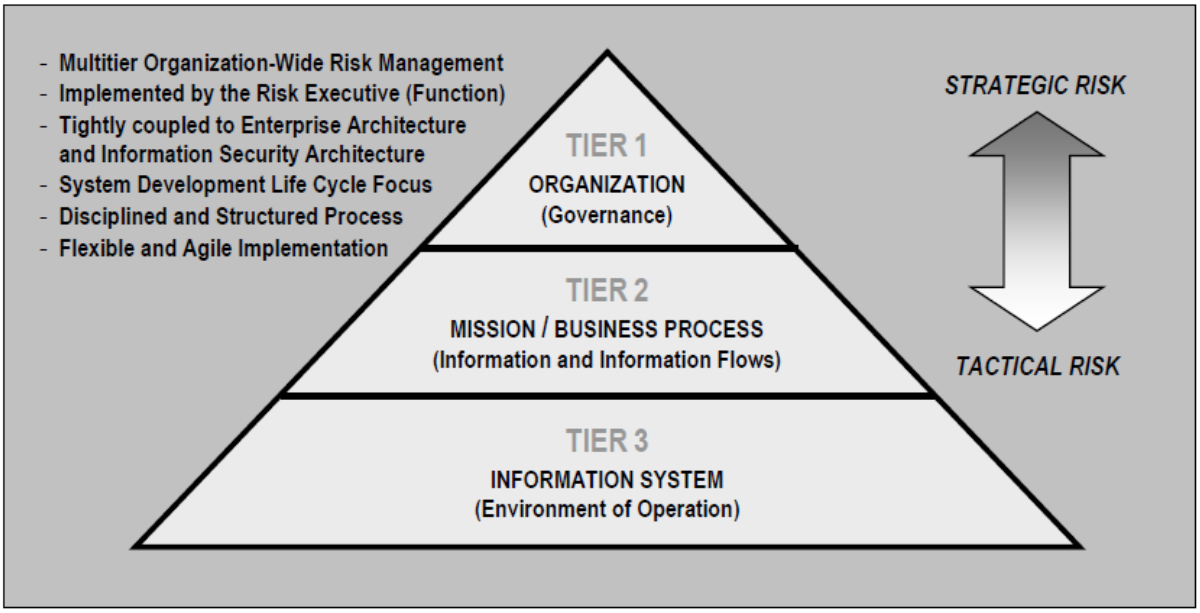

Figure 3. Multi-Tiered Risk Management Strategy

Tier 1 frames the organization risk and informs all other activities. This is where leaders set priorities and create policies to achieve strategic objectives. Tier 1 includes, among other things, governance of the organization to set priorities; the risk executive function to manage organization-wide risks; determination of the risk management strategy to provide a common framework at all levels of the organization; and the investment strategy to achieve mission and risk priorities, anticipate risk response needs, and limit strategic investments to align with organizational priorities. Tier 1 sets the direction for Tier 2 managers.

Tier 2 focuses on developing risk-informed mission processes to meet leadership's stated goals. Tier 2 includes the identification and development of risk-aware mission processes to achieve strategic goals; the administration of an enterprise architecture to enable mission processes; and establishment of a consistent information system architecture to cost-effectively ensure resilience of mission-critical information system assets. Tier 2 builds an organizational infrastructure conducive to the successful execution of activities at Tier 3.

Tier 3 uses the mission processes developed in Tier 2 and the goals set in Tier 1 to conduct the day-to-day activities that make the organization successful. Tier 3 addresses risk from an information system perspective. These activities are the culmination of the organization's risk management strategy and ensure that individual systems are secure, reliable, and available to execute mission processes.

In October 2018, NIST announced the final draft of NIST SP 800-37, revision 2 that modifies the RMF process. The modification is discussed in Appendix A; however, because most organizations will be slow to transition to version 2, this paper focuses on the initial version of the RMF.

3.0 RMF Roles and Responsibilities

The RMF identifies 13 roles and responsibilities of key participants in the organization's risk management. It is not necessary for each role to exist within the organization, but the duties performed must be accomplished diligently and be assigned to individuals or groups that do not have conflicting interests.

Risk management roles and responsibilities include the following:

- Chief Executive Officer—Responsible for the organization's success.
- Risk Executive—Responsible for the organization's risk program.
- Chief Information Officer—Responsible for designating a senior information security officer; developing and maintain information security policies, procedures, and control techniques; overseeing personnel; and assisting senior leaders on all security responsibilities.
- Information Owner—Responsible for statutory, management, or operational authority and the establishment of policies and procedures governing its generation, collection, processing, dissemination, and disposal.
- Senior Information Security Officer—Responsible for carrying out the chief information officer security responsibilities and serving as the primary interface between senior managers and information system owners.
- Authorizing Official (AO) or Designated Representative—Responsible for accepting an information system into an operational environment at a known risk level.
- Common Control Provider—Responsible for developing, implementing, assessing, and monitoring common security controls.
- Information System Owner (ISO)—Responsible for procuring, developing, integrating, modifying, operating, and maintaining an information system.
- Information System Security Officer (ISSO)—Responsible for ensuring that the appropriate operational security posture is maintained for an information system.

- Information Security Architect—Responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture.
- Information System Security Manager (ISSM)—Responsible for conducting information system security management activities as designated by the ISSO. They develop and maintain the system-level cybersecurity program.
- Security Control Assessor (SCA)—Responsible for conducting a thorough assessment of the management, operational, and technical security controls of an information system.

4.0 RMF Step 1—Categorize Information System

To categorize an information system, first categorize the information on the system, according to the potential impact of a loss of confidentiality, integrity, and availability. Table 1 lists the subtasks under Step 1, shows who is responsible, and describes each subtask's deliverable.

Table 1. RMF Step 1 – Categorize Information System

Supporting Tasks	Primary Responsibility	References	Deliverable(s)
Task 1-1—Categorize the information system and document the results in the System Security Plan (SSP).	ISO or Information Owner/Steward	NIST SP 800-30, NIST SP 800-39, NIST SP 800-59, NIST SP 800-60, CNSSI 1253, FIPS 199	Draft SSP with System Categorization filled in
Task 1-2—Describe the information system (including system boundary) and document the description in the SSP.	ISO	NIST SP 800-37	Updated SSP to include a description of the information system
Task 1-3—Register the information system with the appropriate organizational program management offices.	ISO	eMASS https://emass-army.csd.disa.mil/	Document or enter in the information technology registry with the official system name, system owner, and categorization

5.0 RMF Step 2—Select Security Controls

Using appropriate baseline and overlays, select security controls, and then tailor as required to prevent security breaches of an information system. Table 2 lists the Step 2 sub-tasks, the role responsible for the sub-task, and the expected deliverable.

Table 2. RMF Step 2—Select Security Controls

Supporting Tasks	Primary Responsibility	Reference	Deliverable(s)
Task 2-1—Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in the SSP.	ISO, ISSM/ISSO, SCA	NIST SP 800-30, NIST SP 800-53, CNSSI 1253, FIPS 199, FIPS 200	Document the common controls in the SSP/ Security Controls Traceability Matrix (SCTM)
Task 2-2—Select the security controls for the information system (i.e., baseline, overlays, tailored) and document the controls in the SSP.	ISO	NIST SP 800-30, NIST SP 800-53, CNSSI 1253, FIPS 199, FIPS 200	Document the selected security controls in the SSP, draft Risk Assessment Report (RAR)
Task 2-3 — Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.	ISO	NIST SP 800-30, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-137, CNSSI 1253	Documented and approved Continuous Monitoring Plan/Strategy including frequency of monitoring for each control
Task 2-4 — Review and approve the draft SSP by the AO.	AO, ISSM/ISSO	NIST SP 800-30, NIST SP 800-53, CNSSI 1253	Documented and approved draft SSP

6.0 RMF Step 3—Implement Security Controls

Implement security controls selected in Step 2 on the information system. Table 3 lists the Step 3 subtasks, deliverables, and responsible role.

Table 3. RMF Step 3—Implement Security Controls

Supporting Tasks	Primary Responsibility	References	Deliverable(s)
Task 3-1—Implement security controls specified in the SSP.	ISO	NIST SP 800-37, NIST SP 800-30, NIST SP 800-53, NIST SP 800-53A, CNSSI 1253, web: SCAP.NIST.GOV, FIPS 200	
Task 3-2—Document the security control implementation as appropriate in the SSP, providing a functional description of the control implementation.	ISO; ISSM/ISSO	NIST SP 800-53, CNSSI 1253	Updated SSP with information describing how security controls are implemented

7.0 RMF Step 4—Assess Security Controls

Determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements. Table 4 lists the Step 4 subtasks, deliverables, and responsible roles.

Table 4. RMF Step 4—Assess Security Controls

Supporting Tasks	Primary Responsibility	References	Deliverable(s)
Task 4-1—Develop, review, and approve a plan to assess the security controls.	ISSM/ISSO, SCA	NIST SP 800-53A	Security Assessment Plan
Task 4-2—Assess the security controls in accordance with the assessment procedures defined in the Security Assessment Plan. Document the security control implementation, as appropriate, in the SSP, providing a functional description of the control implementation.	SCA	NIST SP 800-53A	Individual test results for each test or matrix for all tests

Supporting Tasks	Primary Responsibility	References	Deliverable(s)
Task 4-3—Prepare the Security Assessment Report (SAR), documenting the issues, findings, and recommendations for the security control assessment.		NIST SP 800-53A	SAR
Task 4-4 — Conduct initial remedial actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate.	ISO, SCA, ISSM/ISSO	NIST SP 800-30, NIST SP 800-53A	Updated RAR

8.0 RMF Step 5—Authorize Information System

Determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements. Table 5 lists the Step 5 subtasks, deliverables, and responsible roles.

Table 5. RMF Step 5—Authorize Information System

Supporting Tasks	Primary Responsibility	Reference	Deliverable(s)
Task 5-1—Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations of the SAR, excluding any remediation actions taken.	SCA (documents initial findings); ISO (completes POA&M; adds additional items)	NIST SP 800-30, NIST SP 800-53A,OMB Memo 02-01,	POA&M
Task 5-2—Assemble the Security Authorization Package to include artifacts and submit the package to the AO for adjudication.	ISO, ISSM/ISSO, SCA	NIST SP 800-37	Security Authorization Package; artifacts include SSP, SAR, POA&M, RAR, and Continuous Monitoring Plan

Supporting Tasks	Primary Responsibility	Reference	Deliverable(s)
Task 5-3—Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation.	AO	NIST SP 800-30, NIST SP 800-39	
Task 5-4—Determine if risk to organizational operations, organizational assets, individuals, other organizations, or the nation is acceptable.	AO	NIST SP 800-39	Authorization decision document (e.g., Authority to Operate, Denied Authorization to Operate, and Interim Authorization to Test)

By the end of RMF Step 5, documents submitted in the Security Authorization Package, at a minimum, include the following:

- SSP/ SCTM—Provides an overview of security requirements, description of agreed-upon controls, and other supporting security-related information.
- RAR—Defines the organizationally established level of acceptable risk associated with the operation of an information technology system at a specific level, identifies risks, and provides an assessed residual risk level for the system.
- Continuous Monitoring Plan—Provides the strategy to routinely evaluate selected information assurance controls/metrics. Reference NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations (NIST 2011a).
- SAR — Contains security control assessment results and recommended corrective actions for security-control weaknesses and deficiencies.
- POA&M — Defines plans of action and milestones related to correcting weaknesses or deficiencies and reducing or eliminating known vulnerabilities and identifies completion dates.

9.0 RMF Step 6—Monitor Security Controls

Assess and track the security state of an information system and its operational environment on an on-going basis. Table 6 lists the Step 6 subtasks, deliverables, and responsible roles.

Table 6. RMF Step 6—Monitor Security Controls

Supporting Tasks	Primary Responsibility	Reference	Deliverable(s)
Task 6-1—Determine the security impact of proposed or actual changes to the information system and its environment of operation.	ISO, ISSO/ISSM	NIST SP 800-30, NIST SP 800-53A	Change Request
Task 6-2—Assess a selected subset of security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.	SCA, ISSO/ISSM	NIST SP 800-53A, NIST SP 800-137	Periodic Continuous Monitoring Report
Task 6-3—Conduct remediation action based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.	ISO, ISSM/ISSO	NIST SP 800-30, NIST SP 800-53, NIST SP 800-53A, CNSSI 1253	Documented evidence of correction such as scan results, registry “dump,” etc.
Task 6-4—Update the SSP, SAR, and POA&M based on the results of the continuous monitoring process.	ISO	NIST SP 800-53A	SSP, SAR, RAR, and POA&M

Supporting Tasks	Primary Responsibility	Reference	Deliverable(s)
Task 6-5—Regularly report the security status of the information system (including the effectiveness of security controls employed within and inherited by the information system) to the AO and other appropriate organizational officials, in accordance with the monitoring strategy.	ISO	NIST SP 800-53A	Periodic Continuous Monitoring Report
Task 6-6—Regularly review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the information system) in accordance with the monitoring strategy to determine whether there is risk to organizational operations, organizational assets, individuals, other organizations, or the nation.	AO	NIST SP 800-30, NIST SP 800-39	Authority to Operate
Task 6-7—Implement an information system decommissioning strategy, when needed, that executes required actions when a system is removed from service.	ISO	NIST SP 800-30, NIST SP 800-53A	Updated system inventory

10.0 References

NIST. 2010. NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. National Institute of Standards and Technology, February 2010. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=904985.

NIST. 2011a. NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. National Institute of Standards and Technology, September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

NIST. 2011b. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. National Institute of Standards and Technology, March 2011. https://csrc.nist.gov/publications/detail/sp/800-39/final

NIST. 2018. NIST Special Publication 800-37, Revision 2, *A System Life Cycle Approach for Security and Privacy*. National Institute of Standards and Technology, October 2018. https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-fpd.pdf

Appendix A

Updates to the Risk Management Framework

The National Institute of Standards & Technology (NIST) released the draft of Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. This update is based on the Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Below are the major objectives of the update:

- Establish preparatory activities at all risk management levels to provide more effective and efficient execution in RMF
- Demonstrate how NIST cybersecurity framework aligns with NIST risk management process
- Integrate the privacy risk management process documented in NISTIR 8062 into the RMF to support the privacy protection needs for which privacy programs are responsible
- Align NIST SP 800-160 to RMF for promoting the development of trustworthy, secure software systems

In version 2, one of the key changes to the RMF is to add the ***Prepare*** step. Preparation is critical at tier 1 (organization) and tier 2 (mission/business process) to execute the RMF efficiently (NIST 2018). This ***Prepare*** step involves the essential activities at the organization, mission and business process, and information system levels of the enterprise by managing security and privacy risk appropriately throughout the organization. In version 2, the ***Prepare*** step is defined as:

> *Execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.*

Figure A.1 shows the steps in the RMF according to version 2. Here, the ***Prepare*** step is carried-out iteratively throughout the RMF process.

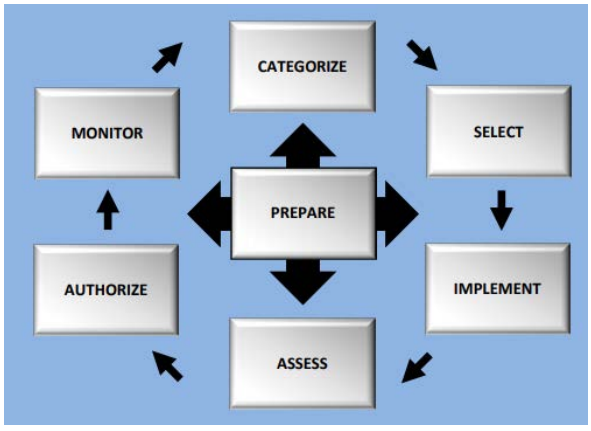

Figure A.1. Risk Management Framework

Table A.1 provides the summary of the Prepare tasks along with their outcomes and also the alignment domain of NIST cybersecurity framework. This table focuses on both the organization and system levels.

Table A.1. Prepare Task and Outcome

Level	Task	Title	Outcome	CSF align
Organization	P-1	Risk management roles	Individuals are identified and assigned key roles for executing the Risk Management Framework.	ID.AM-6; ID.GV-2
	P-2	Risk management strategy	A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established	ID.RM; ID.SC
	P-3	Risk assessment—organization	An organization-wide risk assessment is completed or an existing risk assessment is updated	ID.RA; ID.SC-2
	P-4	Organization-wide tailored control baselines and profiles (optional)	Tailored control baselines for organization-wide use are established and made available.	Profile
	P-5	Common control identification	Common controls that are available for inheritance by organizational systems are identified, documented, and published.	
	P-6	Impact-level prioritization (optional)	A prioritization of organizational systems with the same impact level is conducted.	ID.AM-5
	P-7	Continuous monitoring strategy— organization	An organization-wide strategy for monitoring control effectiveness is developed and implemented.	DE.CM; ID.SC-4
	P-8	Mission or business focus	Missions, business functions, and mission/business processes that the system is intended to support are identified.	Profile; Implementation Tiers; ID.BE
System	P-9	System stakeholders	The stakeholders having an interest in the system are identified.	ID.AM; ID.BE
	P-10	Asset identification	Stakeholder assets are identified and prioritized.	ID.AM
	P-11	Authorization boundary	The authorization boundary (i.e., system) is determined.	
	P-12	Information types	The types of information processed, stored, and transmitted by the system are identified.	ID.AM-5
	P-13	Information life cycle	Identify and understand all stages of the information life cycle	
	P-14	Risk assessment—system	A system-level risk assessment is completed or an existing risk assessment is updated.	ID.RA; ID.SC-2
	P-15	Security and privacy requirements	Security and privacy requirements are defined and prioritized.	ID.GV; PR.IP
	P-16	Enterprise architecture	The placement of the system within the enterprise architecture is determined.	
	P-17	System registration	The system is registered for purposes of management, accountability, coordination, and oversight.	ID.GV

Pacific Northwest
NATIONAL LABORATORY

www.pnnl.gov

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

U.S. DEPARTMENT OF
ENERGY