2.5 AUTHORIZATION BOUNDARIES

The authorization boundary establishes the scope of protection for an information system (i.e., what the organization agrees to protect under its direct management or within the scope of its responsibilities).[41] The authorization boundary includes the people, processes, and information technologies (i.e., system elements) that are part of each system supporting the organization's missions and business functions. Authorization boundaries that are too expansive (i.e., include too many system elements or components) make the risk management process unnecessarily complex. Conversely, authorization boundaries that are too limited (i.e., include too few system elements or components) increase the number of systems that must be separately managed and therefore, may unnecessarily inflate the information security and privacy costs for the organization.

The authorization boundary for a system is established during the RMF *Prepare Task – System level*, Task P-11. Organizations have flexibility in determining what constitutes the authorization boundary for a system. The set of system elements included within an authorization boundary defines the system (i.e., the scope of the authorization). When a set of system elements is identified as an authorization boundary for a system, the elements are generally under the same direct management.[42] Other considerations for determining the authorization boundary include identifying system elements that:

- Support the same mission or business functions;
- Have similar operating characteristics and security and privacy requirements;
- Process, store, and transmit similar types of information (e.g., categorized at the same impact level);[43] or
- Reside in the same environment of operation (or in the case of a distributed system, reside in various locations with similar operating environments).

The scope of the authorization boundary is revisited periodically as part of the continuous monitoring process carried out by the organization. While the above considerations may be useful to organizations in determining authorization boundaries for purposes of managing risk, the considerations are not intended to limit the organization's flexibility in establishing authorization boundaries that promote effective security and privacy with the available resources of the organization.

The process of establishing authorization boundaries carries significant risk management implications and is therefore an organization-wide activity that requires coordination among key participants. The process considers mission and business requirements, security and privacy

[41] Information systems are discrete sets of information resources organized for the collection, processing, use, sharing, maintenance, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology. Information systems may or may not include hardware, firmware, and software.

[42] For information systems, direct management control involves budgetary, programmatic, or operational authority and associated *responsibility* and *accountability*. Direct management control does not necessarily imply that there is no intervening management.

[43] If a system contains information at multiple impact levels, the system is categorized at the highest impact level. See [FIPS 199] and [FIPS 200].

requirements, and the costs to the organization. Appendix G provides additional information and considerations for determining authorization boundaries, including boundaries for complex systems and software applications.

EFFECTIVE AUTHORIZATION BOUNDARIES

Establishing meaningful authorization boundaries for *systems* and *common controls* is one of the most important risk management activities carried out by an organization. The authorization boundary defines the specific scope of an authorizing official's responsibility and accountability for protecting information resources and individuals' privacy—including the use of systems, components, and services from external providers. Establishment of meaningful authorization boundaries is a foundation for assuring mission and business success for the organization.

2.6 REQUIREMENTS AND CONTROLS

Before executing the RMF, it is important to understand the concept of security and privacy requirements and the relationship between requirements and controls. The term *requirements* can be used in different contexts. In the context of federal information security and privacy policies, the term is generally used to refer to information security and privacy obligations imposed on organizations. For example, OMB Circular A-130 imposes a series of information security and privacy requirements with which federal agencies must comply when managing information resources. In addition to the use of the term requirements in the context of federal policy, the term *requirements* is used in this guideline in a broader sense to refer to an expression of the set of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and corresponding security and privacy requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). The term *requirements*, as used in this guideline, includes both legal and policy requirements, as well as an expression of the broader set of stakeholder protection needs that may be derived from other sources. All of these requirements, when applied to a system, help determine the required characteristics of the system—encompassing security, privacy, and assurance.

Organizations may choose to divide security and privacy requirements into more granular categories depending on where the requirements are employed in the SDLC and for what purpose. Organizations may use the term *capability requirement* to describe a capability that the system or organization must provide to satisfy a stakeholder protection need. In addition, organizations may refer to system requirements that pertain to particular hardware, software, and firmware components of a system as *specification requirements*—that is, capabilities that implement all or part of a control and that may be assessed (i.e., as part of the verification, validation, testing, and evaluation processes). Finally, organizations may use the term *statement of work* requirements to refer to actions that must be performed operationally or during system development.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the

protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include technical aspects, administrative aspects, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of *derived requirements* or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for particular controls within the SDLC.

CONTEXT-DEPENDENT REQUIREMENTS

Security and privacy requirements and risks identified by the organization, lead to the need for security and privacy controls to respond to the risk. The controls selected by the organization subsequently lead to both specification requirements and statement of work requirements in the systems engineering context. This is an important aspect of how systems engineers develop, derive, and decompose requirements as part of the SDLC process. Thus, organizations manage security and privacy requirements at various levels of granularity and specificity during the life cycle of the system. Controls play an important part in the life cycle by providing high-level statements of protection capability that can be refined and expanded upon by the organization.

2.7 SECURITY AND PRIVACY POSTURE

The purpose of the RMF is to help ensure that, throughout the SDLC, information systems, organizations, and individuals are adequately protected, and that authorizing officials have the information needed to make credible, risk-based decisions regarding the operation or use of systems or the provision of common controls. A key aspect of risk-based decision making for authorizing officials is understanding the security and privacy posture of information systems and the common controls that are available for inheritance by those systems. The security and privacy posture represents the status of information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to manage the defense of the organization in its operation or use of systems; comply with applicable privacy requirements and manage privacy risks; and react as the situation changes.

The security and privacy posture of information systems and organizations is determined on an ongoing basis by assessing and continuously monitoring system-specific, hybrid, and common controls.[44] The control assessments and monitoring activities provide evidence that the controls selected by the organization are implemented correctly, operating as intended, and satisfying the security and privacy requirements in response to laws, executive orders, regulations, directives, policies, standards, or mission and business requirements. Authorizing officials use the security and privacy posture to determine if the risk to organizational operations and assets,

[44] Monitoring of controls is part of an organization-wide risk management approach defined in [SP 800-39].

individuals, other organizations, or the Nation are acceptable based on the organization's risk management strategy and organizational risk tolerance.[45]

2.8 SUPPLY CHAIN RISK MANAGEMENT

Organizations are becoming increasingly reliant on products, systems, and services provided by external providers to carry out missions and business functions. Organizations are responsible and accountable for the risk incurred when using such component products, systems, and services.[46] Relationships with external providers can be established in a variety of ways, for example, through joint ventures, business partnerships, various types of formal agreements (e.g., contracts, interagency agreements, lines of business arrangements, licensing agreements), or outsourcing arrangements.

The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing amount of risk to an organization. Risk may increase based on the likelihood of occurrence and adverse impact from threat events such as the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain, including the failure to build in security or privacy capabilities that enable an organization to better manage risk in its environment.

Supply chain risks can be endemic or systemic within a system element, system, organization, sector, or nation. While the singular use of a system element or service within a system may present an acceptable risk to an organization, its common or extended use throughout a system, organization, sector or nation can raise the risk to an unacceptable level. These risks are often associated with the global and distributed nature of product and service supply chains and an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed. This includes the processes, procedures, and practices used to assure the integrity, security, resilience, privacy capabilities, and quality of the acquired products, systems, and services.

To address supply chain risks, organizations develop an SCRM policy, which is an important vehicle for directing SCRM activities. Guided and informed by applicable laws, executive orders, directives, policies, and regulations, the SCRM policy supports applicable organizational policies (e.g., acquisition and procurement, information security and privacy, logistics, quality, and supply chain). The policy addresses the goals and objectives in the organization's strategic plan, missions and business functions, and the internal and external customer requirements. It also defines the integration points for SCRM with the risk management and the SDLC processes for the organization. Finally, the SCRM policy defines the SCRM roles and responsibilities within the organization, any dependencies among those roles, and the interaction among the roles. SCRM roles specify the responsibilities for procurement, conducting risk assessments, collecting supply chain threat intelligence, identifying and implementing risk-based mitigations, and performing monitoring functions.

[45] See RMF *Prepare-Organization Level* step, Task P-2.

[46] [OMB A-130] defines supply chain risk and requires federal agencies to consider supply chain security issues for all resource planning and management activities throughout the SDLC so that risks are appropriately managed.

[FISMA] and [OMB A-130] require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Security and privacy requirements for external providers including the controls for systems processing, storing, or transmitting federal information are expressed in contracts or other formal agreements. The RMF can be effectively used to manage supply chain risk.[47] The conceptual view of the system in Figure 5 can guide and inform security, privacy, and risk management activities for all elements of the supply chain. Every step in the RMF can be executed by nonfederal external providers except for the *Authorize* step—that is, the acceptance of risk is an inherent federal responsibility for which senior executives are held responsible and accountable. The authorization decision is directly linked to the management of risk related to the acquisition and use of component products, systems, and services from external providers.[48] [OMB A-130] also requires organizations to develop and implement SCRM plans.[49]

Managing supply chain risk is a complex, multifaceted undertaking requiring a coordinated effort across an organization—building trust relationships and communicating with both internal and external stakeholders. SCRM activities involve identifying and assessing applicable risks, determining appropriate mitigating actions, developing appropriate SCRM plans to document selected mitigating actions, and monitoring performance against SCRM plans. Because supply chains differ across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored plans provide the basis for determining whether a system is "fit for purpose" and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations to focus their resources on the most critical missions and business functions based on mission and business requirements and their risk environment.

The determination that the risk from acquiring products, systems, or services from external providers is acceptable depends on the level of assurance[50] that the organization can gain from the providers. The level of assurance is based on the degree of control the organization can exert on the external provider regarding the controls needed for the protection of the product, system, or service and the evidence brought forth by the provider as to the effectiveness of those controls.

The degree of control is established by the specific terms and conditions of the contract or service-level agreement. Some organizations have extensive control through contract vehicles or other agreements that specify the security and privacy requirements for the external provider. Other organizations, in contrast, have limited control because they are purchasing commodity

---

[47] *Supply chain risk* means risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation [OMB A-130]. When system elements process PII, SCRM practices address both information security and privacy risk.

[48] While *authorization* (i.e., the acceptance of risk) of federal information systems is an inherent federal responsibility, it is a foundational concept that can be used by senior executives in nonfederal organizations at all levels in the supply chain to manage security and privacy risk.

[49] [SP 800-161] provides guidance on SCRM plans.

[50] The level of assurance provided by an external provider can vary, ranging from those who provide high assurance (e.g., business partners in a joint venture that share a common business model and goals) to those who provide less assurance and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

services or commercial off-the-shelf products. The level of assurance can also be based on many other factors that convince the organization that the requisite controls have been implemented and that a credible determination of control effectiveness exists. For example, an authorized external cloud service provided to an organization through a well-established line-of-business relationship may provide a level of trust in the service that is within the risk tolerance of the organization. Ultimately, the responsibility for responding to risks from the use of component products, systems, and services from external providers remains with the organization and the authorizing official. Organizations require that an appropriate *chain of trust* be established with external providers when dealing with the issues associated with system security or privacy risks.

SUPPLY CHAIN RISK MANAGEMENT STRATEGIES AND PLANS

Organizations have flexibility on how the details of SCRM strategies and plans are documented. SCRM strategy details for Levels 1 and 2 (organization and mission/business process levels), can be documented in the information security program plan for the organization or in a separate organization-level and/or mission/business process-level SCRM strategy. SCRM plan details for Level 3 (information system level) can be documented in the information system security plan or in a separate system-level SCRM plan. An SCRM strategy template is provided in [SP 800-161].

CHAPTER THREE

THE PROCESS

EXECUTING THE RISK MANAGEMENT FRAMEWORK TASKS

This chapter describes the steps and associated tasks that comprise the RMF and the selected individuals or groups (defined organizational roles) that carry out such tasks.[51] Organizations align their risk management roles with complementary or similar roles defined for the SDLC whenever possible, and consistent with missions and business functions. RMF tasks are executed concurrently with, or as part of, the SDLC processes in the organization. Executing RMF tasks concurrently with SDLC processes helps to ensure that organizations are effectively integrating the process of managing information security and privacy risks into SDLC processes. Moreover, the expected outputs required by the RMF (e.g., security and privacy plans, assessment reports, plans of action and milestones), can be routinely obtained from the SDLC processes in place within organizations and may not need to be developed solely for RMF implementation.

RMF ALIGNMENT WITH THE SDLC

The best RMF implementation is one that is indistinguishable from the routine SDLC processes carried out by organizations. That is, RMF tasks are closely aligned with the ongoing activities in the SDLC processes, ensuring the seamless integration of security and privacy protections into organizational systems—and taking maximum advantage of the artifacts generated by the SDLC processes to produce the necessary evidence in authorization packages to facilitate credible, risk-based decision making by senior leaders in organizations.

The process of implementing RMF tasks may vary from organization to organization. While the tasks appear in sequential order, there can be many points in the risk management process that require divergence from the sequential order, including the need for iterative cycles between initial task execution and revisiting tasks. For example, control assessment results can trigger a set of remediation actions by system owners and common control providers, which can in turn require the reassessment of selected controls. Monitoring controls can generate a cycle of tracking changes to the system and its environment of operation; assessing the information security and privacy impact; reassessing controls, taking remediation actions, and reporting the security and privacy posture of the system and the organization.

There may be other opportunities to diverge from the sequential nature of the tasks when it is more effective, efficient, or cost-effective to do so. For example, while the control assessment tasks are listed after the control implementation tasks, organizations may begin the assessment of controls as soon as they are implemented but prior to the complete implementation of all

[51] Appendix D describes the roles and responsibilities of key participants involved in organizational risk management and the execution of the RMF. Many risk management roles defined in this publication have counterpart roles defined in the SDLC process.

controls described in the system security plans and privacy plans. Assessing controls as soon as they are implemented may result in organizations assessing the physical and environmental protection controls within a facility prior to assessing the controls implemented in the hardware, firmware, or software components of the system (which may be implemented later). Regardless of the task ordering, the final action before a system is placed into operation is the explicit acceptance of risk by the authorizing official.

The RMF steps and associated tasks can be applied to new development systems and existing systems at appropriate phases in the SDLC. For new and existing systems, organizations ensure that the designated tasks have been completed to prepare for the execution of the RMF. For existing systems, organizations confirm that the security categorization and (for information systems processing PII) a privacy risk assessment have been completed and are appropriate; and that the needed controls have been selected, tailored, and implemented.

Applying the RMF steps and associated tasks to existing systems can serve as a gap analysis to determine if the organization's security and privacy risks have been effectively managed. Deficiencies in controls can be addressed in the RMF steps for implementation, assessment, authorization, and monitoring in the same manner as in new development systems. If no deficiencies are discovered during the gap analysis and there is a current authorization in effect, the organization can move directly to the continuous monitoring step in the RMF. If a current authorization is not in effect, the organization continues in the usual sequence with the assessment, authorization, and monitoring steps.

TASK DELEGATION

The roles specified in the *Primary Responsibility* section for each RMF task are responsible for ensuring that the task is completed. The roles with primary responsibility may complete a task or may delegate completion of a task to one or more *supporting* roles except where delegation is specifically prohibited or disallowed in the task *Discussion* section or Appendix D. If completion of a task is delegated, the role with primary responsibility for that task remains accountable for task completion.

TIPS FOR STREAMLINING RMF IMPLEMENTATION

- Use the tasks and outputs of the Organization-Level and System-Level *Prepare* Step to promote a consistent starting point within organizations to execute the RMF.
- Maximize the use of *common controls* to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of *shared* or *cloud-based* systems, services, and applications where applicable, to reduce the number of organizational authorizations.
- Employ *organizationally-tailored control baselines* to increase the speed of security and privacy plan development, promote consistency of security and privacy plan content, and address organization-wide threats.
- Employ *organization-defined controls* based on security and privacy requirements generated from a systems security engineering process.
- Maximize the use of *automated tools* to manage security categorization; control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for *low-impact* systems if those systems cannot adversely affect higher-impact systems through system connections.
- Maximize the *reuse* of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings.
- Reduce the *complexity* of the IT/OT infrastructure by eliminating unnecessary systems, system elements, and services — employ *least functionality* principle.
- Make the transition to *ongoing authorization* and use *continuous monitoring* approaches to reduce the cost and increase the efficiency of security and privacy programs.

DEVELOPING WELL-DEFINED SECURITY AND PRIVACY REQUIREMENTS

The RMF is an SDLC-based process that can be effectively used to help ensure that security and privacy requirements are satisfied for information systems or organizations. Defining clear, consistent, and unambiguous security and privacy requirements is an important element in the successful execution of the RMF. The requirements are defined early in the SDLC in collaboration with the senior leaders and are integrated into the acquisition and procurement processes. For example, organizations can use the [SP 800-160 v1] life cycle-based systems engineering process to define an initial set of security and privacy requirements, which in turn, can be used to select a set of controls* to satisfy the requirements. The requirements or the controls can be stated in the Request for Proposal or other contractual agreement when organizations acquire systems, system components, or services. Requirements can also be added throughout the life cycle, such as with the agile development methodology where new features are continuously deployed.

The NIST *Cybersecurity Framework* [NIST CSF] (i.e., Core, Profiles) can also be used to identify, align, and deconflict security requirements and to subsequently inform the selection of security controls for an organization. Cybersecurity Framework Profiles can provide a link between cybersecurity activities and organizational mission/business objectives, which supports risk-based decision-making throughout the RMF. While Profiles may be used as a starting point to inform control selection and tailoring activities, further evaluation is needed to ensure the appropriate controls are selected. Some organizations may choose to use the Cybersecurity Framework in concert with the NIST *Systems Security Engineering* publications—identifying, aligning, and deconflicting requirements across a sector, an industry, or an organization—and subsequently employing a systems engineering approach to further refine the requirements and obtain trustworthy secure solutions to help protect the organization's operations, assets, individuals.

* See Section 2.3 for specific guidance on privacy control selection and managing privacy risk.

ORGANIZATION AND SYSTEM PREPARATION

Preparation can achieve effective, efficient, and cost-effective execution of risk management processes. The primary objectives of the *Prepare* step include:

- Facilitate better communication between senior leaders and executives in the C-suite and system owners and operators—
  - aligning organizational priorities with resource allocation and prioritization at the system level; and
  - conveying acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance.
- Promote organization-wide identification of common controls and the development of organizationally-tailored control baselines, to reduce the workload on individual system owners and the cost of system development and protection.
- Reduce the complexity of the IT infrastructure by consolidating, standardizing, and optimizing systems, applications, and services through the application of enterprise architecture concepts and models.
- Identify, prioritize, and focus resources on high value assets (as defined in [OMB M-19-03]), that require increased levels of protection.
- Facilitate system readiness for system-specific tasks.

These objectives, if achieved, significantly reduce the information technology footprint and the attack surface of organizations, promote IT modernization objectives, and prioritize security and privacy activities to focus protection strategies on the most critical assets and systems.

Finally, certain tasks in the *Prepare* step at the organization level are designated as *optional*. These tasks are included to provide organizations additional options to help make their RMF implementations more effective, efficient, and cost-effective.

3.1 PREPARE [52]

Purpose

The purpose of the ***Prepare*** step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.

PREPARE TASKS—ORGANIZATION LEVEL [53]

Table 1 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *organization* level. Applicable Cybersecurity Framework constructs are also provided.

TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: **ID.AM-6**; **ID.GV-2**]
TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: **Profile**]
TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

[52] The *Prepare* step is intended to leverage activities already being conducted within security, privacy, and supply chain programs to emphasize the importance of having organization-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization.

[53] For ease of use, the preparatory activities are grouped into organization-level preparation and information system-level preparation.

RISK MANAGEMENT ROLES

TASK P-1 Identify and assign individuals to specific roles associated with security and privacy risk management.

Potential Inputs: Organizational security and privacy policies and procedures; organizational charts.

Expected Outputs: Documented Risk Management Framework role assignments.

Primary Responsibility: Head of Agency; Chief Information Officer; Senior Agency Official for Privacy.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer.

Discussion: The roles and responsibilities of key participants in risk management processes are described in Appendix D. The roles and responsibilities may include personnel that are internal or external to the organization, as appropriate. Since organizations have different missions, functions, and organizational structures, there may be differences in naming conventions for risk management roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles). In either situation, the basic risk management functions remain the same. Organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles. For example, authorizing officials cannot occupy the role of system owner or common control provider for systems or common controls they are authorizing. In addition, combining multiple roles for security and privacy requires care because the two disciplines may require different expertise, and in some circumstances, the priorities may be competing. Some roles may be allocated to a group or an office rather than to an individual, for example, control assessor, risk executive (function), or system administrator.

References: [SP 800-160 v1] (Human Resource Management Process); [SP 800-181]; [NIST CSF] (Core [Identify Function]).

RISK MANAGEMENT STRATEGY

TASK P-2 Establish a risk management strategy for the organization that includes a determination of risk tolerance.

Potential Inputs: Organizational mission statement; organizational policies; organizational risk assumptions, constraints, priorities and trade-offs.

Expected Outputs: Risk management strategy and statement of risk tolerance inclusive of information security and privacy risk.

Primary Responsibility: Head of Agency.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Discussion: Risk tolerance is the degree of risk or uncertainty that is acceptable to an organization. Risk tolerance affects all parts of the organization's risk management process, having a direct impact on the risk management decisions made by senior leaders or executives throughout the organization and providing important constraints on those decisions. The risk management strategy guides and informs risk-based decisions including how security and privacy risk is framed, assessed, responded to, and monitored. The risk management strategy may be composed of a single document, or separate security and privacy risk management documents.[54] The risk management strategy makes explicit the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and

[54] A separate supply chain risk management strategy document is called a *supply chain risk management plan*.

operational decisions. This strategy includes the strategic-level decisions and considerations for how senior leaders and executives are to manage security and privacy risks (including supply chain risks) to organizational operations, organizational assets, individuals, other organizations, and the Nation. The risk management strategy includes an expression of organizational risk tolerance; acceptable risk assessment methodologies and risk response strategies; a process for consistently evaluating security and privacy risks organization-wide; and approaches for monitoring risk over time. As organizations define and implement the risk management strategies, policies, procedures, and processes, it is important that they include SCRM considerations. The risk management strategy for security and privacy connects security and privacy programs with the management control systems established in the organization's Enterprise Risk Management strategy.[55]

References: [SP 800-30]; [SP 800-39] (Organization Level); [SP 800-160 v1] (Risk Management, Decision Management, Quality Assurance, Quality Management, Project Assessment and Control Processes); [SP 800-161]; [IR 8062]; [IR 8179] (Criticality Analysis Process B); [NIST CSF] (Core [Identify Function]).

RISK ASSESSMENT—ORGANIZATION

TASK P-3 Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.

Potential Inputs: Risk management strategy; mission or business objectives; current threat information; system-level security and privacy risk assessment results; supply chain risk assessment results; previous organization-level security and privacy risk assessment results; information sharing agreements or memoranda of understanding; security and privacy information from continuous monitoring.

Expected Outputs: Organization-level risk assessment results.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: Chief Information Officer; Mission or Business Owner; Authorizing Official or Authorizing Official Designated Representative.

Discussion: Risk assessment at the organizational level leverages aggregated information from system-level risk assessment results, continuous monitoring, and any strategic risk considerations relevant to the organization. The organization considers the totality of risk from the operation and use of its information systems, from information exchange and connections with other internally and externally owned systems, and from the use of external providers. For example, the organization may review the risk related to its enterprise architecture and information systems of varying impact levels residing on the same network and whether higher impact systems are segregated from lower impact systems or systems operated and maintained by external providers. The organization may also consider the variability of environments that may exist within the organization (e.g., different locations serving different missions/business processes) and the need to account for such variability in risk assessments. Risk assessments of the organization's supply chain may be conducted as well. Risk assessment results may be used to help organizations establish a Cybersecurity Framework Profile.

References: [SP 800-30]; [SP 800-39] (Organization Level, Mission/Business Process Level); [SP 800-161]; [IR 8062].

[55] See [OMB A-123].

ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (Optional)

TASK P-4 Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles.

Potential Inputs: Documented security and privacy requirements directing the use of organizationally-tailored control baselines; mission or business objectives; enterprise architecture; security architecture; privacy architecture; organization- and system-level risk assessment results; list of common control providers and common controls available for inheritance; NIST Special Publication 800-53B control baselines.[56]

Expected Outputs: List of approved or directed organizationally-tailored control baselines; [NIST CSF] Profiles.

Primary Responsibility: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function).

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Discussion: To address the organizational mission or business need for specialized sets of controls to reduce risk, organizationally-tailored control baselines may be developed for organization-wide use.[57] An organizationally-tailored baseline provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established control baselines described in [SP 800-53B]. The tailoring process can also be guided and informed by the requirements engineering process described in [SP 800-160 v1]. Organizations can use the tailored control baseline concept when there is divergence from the specific assumptions used to create the initial control baselines in [SP 800-53B]. This would include, for example, situations when the organization has specific security or privacy risks, has specific mission or business needs, or plans to operate in environments that are not addressed in the initial baselines.

Organizationally-tailored baselines and overlays complement the NIST control baselines by providing an opportunity to add or eliminate controls to accommodate organizational requirements while continuing to protect information commensurate with risk. Organizations can use tailored baselines and overlays to customize control baselines by describing control applicability and by providing interpretations for specific technologies; types of missions or business functions, operations, systems, environments of operation, and operating modes; and statutory or regulatory requirements. Multiple customized baselines may be useful for organizations with heterogeneous systems (e.g., organizations that maintain systems with different operating or processing characteristics, or mission or business characteristics).

Organizationally-tailored baselines can establish organization-defined control parameter values for assignment or selection statements in controls and control enhancements that are agreeable to specific communities of interest and can also extend the supplemental guidance where necessary. Tailored baselines may be more stringent or less stringent than the baselines identified in [SP 800-53B] and are applied to multiple systems.

Tailored baselines developed outside the organization may also be mandated for use by certain laws, executive orders, directives, regulations, policies, or standards. In some situations, tailoring actions may

[56] NIST Special Publication 800-53 (Revision 5), separates the control catalog from the control baselines that have been included historically in that publication. A new companion publication, NIST Special Publication 800-53B, *Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations* defines the recommended baselines. NIST Special Publication 800-53B is referenced throughout the RMF in the relevant tasks.

[57] Tailored control baselines may also be referred to as *overlays*. An organizationally-tailored control baseline is analogous to an organization-wide overlay since an overlay is a tailored baseline that services a community of interest, in this case, the organization.

be restricted or limited by the developer of the tailored baseline or by the issuing authority for the tailored baseline. Tailored baselines (or overlays) have been developed by communities of interest for cloud and shared systems, services, and applications; industrial control systems; privacy; national security systems; weapons and space-based systems; high value assets;[58] mobile device management; federal public key infrastructure; and privacy risks.

Organizations may also benefit from developing one or more Cybersecurity Framework *Profiles*. A Cybersecurity Framework Profile uses the Subcategories in the Framework Core to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.[59] The prioritized list of cybersecurity outcomes developed at the organization and mission/business process levels can be helpful in facilitating consistent, risk-based decisions at the system level. The Subcategories identified in the applicable Cybersecurity Framework Profiles can also be used to guide and inform the development of the tailored control baselines described above.

References: [SP 800-53]; [SP 800-53B]; [SP 800-160 v1] (Business or Mission Analysis and Stakeholder Needs and Requirements Definition Processes); [NIST CSF] (Core, Profiles).

COMMON CONTROL IDENTIFICATION

TASK P-5 Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.

Potential Inputs: Documented security and privacy requirements; existing common control providers and associated security and privacy plans; information security and privacy program plans; organization- and system-level security and privacy risk assessment results.

Expected Outputs: List of common control providers and common controls available for inheritance; security and privacy plans (or equivalent documents) providing a description of the common control implementation (including inputs, expected behavior, and expected outputs).

Primary Responsibility: Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Common Control Provider; System Owner.

Discussion: Common controls are controls that can be inherited by one or more information systems.[60] Common controls can include controls from any [SP 800-53] control family, for example, physical and environmental protection controls, system boundary and monitoring controls, personnel security controls, policies and procedures, acquisition controls, account and identity management controls, audit log and accountability controls, or complaint management controls for receiving privacy inquiries from the public. Organizations identify and select the set of common controls and allocate those controls to the organizational entities designated as common control providers. Common controls may differ based upon a variety of factors, such as hosting location, system architecture, and the structure of the organization. The organization-wide list of common controls takes these factors into account. Common controls can also be identified at different levels of the organization (e.g., corporate, department, or agency level; bureau or subcomponent level; or individual program level). Organizations may establish one or more lists of common controls that can be inherited by information systems. A requirement may not be fully met by a common control. In such cases, the control is considered a hybrid control and is noted as such by the organization, including specifying which parts of the control requirement are provided for inheritance by the common control and which parts are to be provided at the system level.

[58] See [OMB M-19-03].

[59] See [NIST CSF], Section 2.3.

[60] Common controls are *authorized* by designated authorizing officials before the controls are made available for inheritance by organizational systems. See Appendix F for a description of the different types of authorizations.

When there are multiple sources of common controls, organizations specify the common control provider (i.e., who is providing the controls and through what venue, for example, shared services, specific systems, or within a specific type of architecture) and which systems or types of systems can inherit the controls. Common control listings are communicated to system owners, so they are aware of the security and privacy capabilities that are available from the organization through inheritance. System owners are not required to assess common controls that are inherited by their systems or document common control implementation details; that is the responsibility of the common control providers. Likewise, common control providers are not required to have visibility into the system-level details of those systems that are inheriting the common controls they are providing.

Risk assessment results can be used when identifying common controls to determine if the controls available for inheritance satisfy the security and privacy requirements for organizational systems and the environments in which those systems operate (including the identification of potential single points of failure). When the common controls provided by the organization are determined to be insufficient for the information systems inheriting those controls, system owners can supplement the common controls with system-specific or hybrid controls to achieve the required protection for their systems or accept greater risk with the acknowledgement and approval of the organization.

Common control providers execute the RMF steps to implement, assess, and monitor the controls designated as common controls. Common control providers may also be system owners when the common controls are resident within an information system. Organizations select senior officials or executives to serve as authorizing officials for common controls. The senior agency official for privacy is responsible for designating common privacy controls and for documenting them in the organization's privacy program plan. Authorizing officials are responsible for accepting security and privacy risk resulting from the use of common controls inherited by organizational systems.

Common control providers are responsible for documenting common controls in security and privacy plans (or equivalent documents prescribed by the organization); ensuring that the common controls are implemented and assessed for effectiveness by qualified assessors and that assessment findings are documented in assessment reports; producing a plan of action and milestones for common controls determined to have unacceptable deficiencies and targeted for remediation; receiving authorization for the common controls from the designated authorizing official; and monitoring control effectiveness on an ongoing basis. Plans, assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to system owners and can be used by authorizing officials to guide and inform authorization decisions for systems inheriting common controls. For information about the authorization of common controls, see Task R-4 and Appendix F.

References: [SP 800-53].

IMPACT-LEVEL PRIORITIZATION (Optional) [61]

TASK P-6 Prioritize organizational systems with the same impact level.

Potential Inputs: Security categorization information for organizational systems; system descriptions; organization- and system-level risk assessment results; mission or business objectives; Cybersecurity Framework Profiles.

Expected Outputs: Organizational systems prioritized into low-, moderate-, and high-impact sub-categories.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).

[61] Organizations can use this task in conjunction with the optional RMF *Prepare-Organization Level* step, Task P4, to develop organizationally-tailored baselines for the more granular impact designations, for example, organizationally-tailored baselines for low-moderate systems and high-moderate systems.

Supporting Roles: Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative.

Discussion: This task is carried out *only* after organizational systems have been categorized (see Task C1). This task requires organizations to first apply the high-water mark concept to each of their information systems categorized in accordance with [FIPS 199] and [FIPS 200].[62] The application of the high-water mark concept results in systems designated as low impact, moderate impact, or high impact. Organizations desiring additional granularity in their impact designations for risk-based decision making can use this task to prioritize their systems within each impact level.[63] For example, an organization may decide to prioritize its moderate-impact systems by assigning each moderate system to one of three new subcategories: *low-moderate* systems, *moderate-moderate* systems, and *high-moderate* systems. The high-moderate systems assume a higher priority than the moderate-moderate systems and low-moderate systems assume a lower priority than the moderate-moderate systems. The prioritization of its moderate systems gives organizations an opportunity to make more informed decisions regarding control selection and the tailoring of control baselines when responding to identified risks.

Impact-level prioritization can also be used to determine those systems that are critical or essential to organizational missions and business operations and therefore, organizations can focus on the factors of complexity, aggregation, and system interconnections. Such systems can be identified, for example, by prioritizing high-impact systems into *low-high* systems, *moderate-high* systems, and *high-high* systems. Impact-level prioritizations can be conducted at any level of the organization and are based on security categorization data reported by individual system owners. Impact-level prioritization may necessitate the development of organizationally-tailored baselines to designate the appropriate set of controls for the additional, more granular impact levels.

Cybersecurity Framework *Profiles* can be used by organizations to support the impact-level prioritization task. The mission and business objectives and prioritized outcomes defined in applicable Cybersecurity Framework Profiles can help distinguish relative priority between systems with the same impact level. Cybersecurity Framework Profiles can be organized around the priority of mission/business objectives of an organization, and those objectives are assigned a relative priority among them. For example, human and environmental safety objectives may be the two most important objectives relevant to a Profile's context. In this example, when performing Task P-6, a system that relates to a human safety objective may be prioritized higher than a system that has the same impact levels but does not relate to the human safety objective.

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-39] (Organization and System Levels); [SP 800-59]; [SP 800-60 v1]; [SP 800-60 v2]; [SP 800-160 v1] (System Requirements Definition Process); [IR 8179] (Criticality Analysis Process B); [CNSSI 1253]; [NIST CSF] (Core [Identify Function]; Profiles).

CONTINUOUS MONITORING STRATEGY—ORGANIZATION

TASK P-7 Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.

Potential Inputs: Risk management strategy; organization- and system-level risk assessment results; organizational security and privacy policies.

Expected Outputs: An implemented organizational continuous monitoring strategy.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).

[62] Organizations operating National Security Systems follow the categorization guidance in [CNSSI 1253] which does not apply the *high-water mark* concept.

[63] Organizations can also elect to use an alternative, organization-defined categorization approach to add additional granularity to the impact levels defined in [FIPS 199].

Supporting Roles: Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Authorizing Official or Authorizing Official Designated Representative.

Discussion: An important aspect of risk management is the ability to monitor the security and privacy posture across the organization and the effectiveness of controls implemented within or inherited by organizational systems on an ongoing basis.[64] An effective organization-wide continuous monitoring strategy is essential to efficiently and cost-effectively carry out such monitoring. Continuous monitoring strategies can also include supply chain risk considerations, for example, regularly reviewing supplier foreign ownership, control, or influence (FOCI), monitoring inventory forecasts, or requiring on-going audits of suppliers. The implementation of a robust and comprehensive continuous monitoring program helps an organization understand the security and privacy posture of its information systems. It also facilitates ongoing authorization after the initial system or common control authorizations. This includes the potential for changing missions or business functions, stakeholders, technologies, vulnerabilities, threats, risks, and suppliers of systems, components, or services.

The organizational continuous monitoring strategy addresses monitoring requirements at the organization, mission/business process, and information system levels. The continuous monitoring strategy identifies the minimum monitoring frequency for implemented controls across the organization; defines the ongoing control assessment approach; and describes how ongoing assessments are to be conducted (e.g., addressing the use and management of automated tools, and instructions for ongoing assessment of controls for which monitoring cannot be automated). The continuous monitoring strategy may also define security and privacy reporting requirements including recipients of the reports. The criteria for determining the minimum frequency for control monitoring is established in collaboration with organizational officials (e.g., senior accountable official for risk management or risk executive [function)]; senior agency information security officer; senior agency official for privacy; chief information officer; system owners; common control providers; and authorizing officials or their designated representatives). An organizational risk assessment can be used to guide and inform the frequency of monitoring.

The use of automation facilitates a greater frequency and volume of control assessments as part of the monitoring process. The ongoing monitoring of controls using automated tools and supporting databases facilitates near real-time risk management for information systems and supports ongoing authorization and efficient use of resources. The senior accountable official for risk management or the risk executive (function) approves the continuous monitoring strategy including the minimum frequency with which controls are to be monitored.

References: [SP 800-30]; [SP 800-39] (Organization, Mission or Business Process, System Levels); [SP 800-53]; [SP 800-53A]; [SP 800-137]; [SP 800-161]; [IR 8011 v1]; [IR 8062]; [NIST CSF] (Core [Identify, Detect Functions]); [CNSSI 1253].

MISSION/BUSINESS PROCESS (LEVEL 2) CONSIDERATIONS

Mission/business process considerations are addressed in the RMF *Prepare-Organization Level* step and the RMF *Prepare-System Level* step by specifying mission/business process concerns; by identifying the mission or business owners in primary or supporting roles; and by identifying the mission or business objectives. Task P-8 and Task P-9 from the RMF *Prepare-System Level* step are mission/business process level tasks conducted with a system-level specific focus.

[64] Monitoring for control effectiveness is a form of control assessment. [SP 800-53A], [SP 800-137], and [IR 8011 v1] provide additional information on monitoring, conducting control effectiveness assessments, and automating control effectiveness assessments respectively.

PREPARE TASKS—SYSTEM LEVEL

Table 2 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *system* level. Applicable Cybersecurity Framework constructs are also provided.

TABLE 2: PREPARE TASKS AND OUTCOMES—SYSTEM LEVEL

Tasks	Outcomes
TASK P-8 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **ID.BE**]
TASK P-9 SYSTEM STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]
TASK P-10 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]
TASK P-11 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system) is determined.
TASK P-12 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-13 INFORMATION LIFE CYCLE	• All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [*Cybersecurity Framework*: **ID.AM-3**; **ID.AM-4**]
TASK P-14 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-15 REQUIREMENTS DEFINITION	• Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV; PR.IP**]
TASK P-16 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.
TASK P-17 REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]
TASK P-18 SYSTEM REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

MISSION OR BUSINESS FOCUS

TASK P-8 Identify the missions, business functions, and mission/business processes that the system is intended to support.

Potential Inputs: Organizational mission statement; organizational policies; mission/business process information; system stakeholder information; Cybersecurity Framework Profiles; requests for proposal or other acquisition documents; concept of operations.

Expected Outputs: Missions, business functions, and mission/business processes that the system will support.

Primary Responsibility: Mission or Business Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Owner; Information Owner or Steward; Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Organizational missions and business functions influence the design and development of the mission or business processes that are created to carry out those missions and business functions. The prioritization of missions and business functions drives investment strategies, funding decisions, resource prioritization, and risk decisions—and thus affects the existing enterprise architecture and development of the associated security and privacy architectures. Information is elicited from stakeholders to acquire a more thorough understanding of the missions, business functions, and mission/business processes of the organization from a system security and privacy perspective.

References: [SP 800-39] (Organization and Mission/Business Process Levels); [SP 800-64]; [SP 800-160 v1] (Business or Mission Analysis, Portfolio Management, and Project Planning Processes); [NIST CSF] (Core [Identify Function]); [IR 8179] (Criticality Analysis Process B).

SYSTEM STAKEHOLDERS

TASK P-9 Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

Potential Inputs: Organizational mission statement; mission or business objectives; missions, business functions, and mission/business processes that the system will support; other mission/business process information; organizational security and privacy policies and procedures; organizational charts; information about individuals or groups (internal and external) that have an interest in and decision-making responsibility for the system.

Expected Outputs: List of system stakeholders.

Primary Responsibility: Mission or Business Owner; System Owner.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Stakeholders include individuals, organizations, or representatives that have an interest in the system throughout the system life cycle—for design, development, implementation, delivery, operation, and sustainment of the system. It also includes all aspects of the supply chain. Stakeholders may reside in the same organization or they may reside in different organizations in situations when there is a common interest by those organizations in the information system. For example, this may occur during the development, operation, and maintenance of cloud-based systems, shared service systems, or any system where organizations may be adversely impacted by a breach or a compromise to the system or for a variety of considerations related to the supply chain. Communication among stakeholders is important during every step in the RMF and throughout the SDLC to ensure that security and privacy requirements are satisfied, concerns and issues are addressed expeditiously, and risk management processes are carried out effectively.

References: [SP 800-39] (Organization Level); [SP 800-64]; [SP 800-160 v1] (Stakeholder Needs and Requirements Definition and Portfolio Management Processes); [SP 800-161]; [NIST CSF] (Core [Identify Function]).

ASSET IDENTIFICATION

TASK P-10 Identify assets that require protection.

Potential Inputs: Missions, business functions, and mission/business processes the information system will support; business impact analyses; internal stakeholders; system stakeholder information; system information; information about other systems that interact with the system.

Expected Outputs: Set of assets to be protected.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Administrator.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Assets are tangible and intangible items that are of value to achievement of mission or business objectives. Tangible assets are physical in nature and include physical/environmental elements (e.g., non-digital information, structures, facilities), human elements, and technology/machine elements (e.g., hardware elements, mechanisms, and networks). In contrast, intangible assets are not physical in nature and include mission and business processes, functions, digital information and data, firmware, software, and services. Information assets can be tangible or intangible assets, and can include the information needed to carry out missions or business functions, to deliver services, and for system management/operation; controlled unclassified information and classified information; and all forms of documentation associated with the information system. Intangible assets can also include the image or reputation of an organization, and the privacy interests of the individuals whose information will be processed by the system. The organization defines the scope of stakeholder assets to be considered for protection. The assets that require protection are identified based on stakeholder concerns and the contexts in which the assets are used. This includes the missions or business functions of the organization; the other systems that interact with the system; and stakeholders whose assets are utilized by the mission or business functions or by the system. Assets can be documented in the system security and privacy plans.

References: [SP 800-39] (Organization Level); [SP 800-64]; [SP 800-160 v1] (Stakeholder Needs and Requirements Definition Process); [IR 8179] (Criticality Analysis Process C); [NIST CSF] (Core [Identify Function]); [NARA CUI].

AUTHORIZATION BOUNDARY

TASK P-11 Determine the authorization boundary of the system.

Potential Inputs: System design documentation; network diagrams; system stakeholder information; asset information; network and/or enterprise architecture diagrams; organizational structure (charts, information).

Expected Outputs: Documented authorization boundary.

Primary Responsibility: Authorizing Official.

Supporting Roles: Chief Information Officer; System Owner; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Enterprise Architect.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Authorization boundaries establish the scope of protection for information systems (i.e., what the organization agrees to protect under its management control or within the scope of its

responsibilities). Authorization boundaries are determined by authorizing officials with input from the system owner based on mission, management, or budgetary responsibility (see Appendix F). A clear delineation of authorization boundaries is important for accountability and for security categorization, especially in situations where lower-impact systems are connected to higher-impact systems, or when external providers are responsible for the operation or maintenance of a system. Each system includes a set of elements (i.e., information resources)[65] organized to achieve one or more purposes and to support the organization's missions and business processes. Each system element is implemented in a way that allows the organization to satisfy specified security and privacy requirements. System elements include human elements, technology/machine elements, and physical/environmental elements.

The term system is used to define the set of system elements, system element interconnections, and the environment that is the focus of the RMF implementation (see Figure 5). The system is included in a single authorization boundary to ensure accountability. For systems processing PII, the privacy and security programs collaborate to develop a common understanding of authorization boundaries. To conduct effective risk assessments and select appropriate controls, privacy and security programs provide a clear and consistent understanding of what constitutes the authorization boundary. Understanding the authorization boundary and what will occur beyond it may influence controls selected and how they are implemented. For example, if a function of the system includes sharing PII externally, robust encryption controls may be selected for PII transmitted from the system.

Similarly, for systems either partially or wholly managed, maintained, or operated by external providers, an agreement clearly describing authorization boundaries ensures accountability. Privacy and security programs collaborate with providers to develop a common understanding of authorization boundaries. Formal agreements with external providers (e.g. contracts) may be used to delineate what constitutes authorization boundaries. Understanding such boundaries facilitates the selection of appropriate controls to manage supply chain risk.

References: [SP 800-18]; [SP 800-39] (System Level); [SP 800-47]; [SP 800-64]; [SP 800-160 v1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]).

INFORMATION TYPES

TASK P-12 Identify the types of information to be processed, stored, and transmitted by the system.

Potential Inputs: System design documentation; assets to be protected; mission/business process information; system design documentation.

Expected Outputs: A list of information types for the system.

Primary Responsibility: System Owner; Information Owner or Steward.

Supporting Role: Mission or Business Owner; System Security Officer; System Privacy Officer.[66]

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Identifying the types of information needed to support organizational missions, business functions, and mission/business processes is an important step in developing security and privacy plans for the system and a precondition for determining the security categorization. [NARA CUI] defines the information types that require protection as part of its Controlled Unclassified Information (CUI) program, in accordance with laws, regulations, or governmentwide policies. Organizations may define additional information types needed to support organizational missions, business functions, and mission/business

[65] System elements are implemented via hardware, software, or firmware; physical structures or devices; or people, processes, and procedures. The term *system component* is used to indicate system elements that are implemented specifically via hardware, software, and firmware.

[66] System Privacy Officer is only a primary role when the information system processes PII.

processes that are not defined in the CUI Registry or in [SP 800-60 v2]. Identified information types are confirmed by the information owners or stewards and documented in the system security and privacy plans.

References: [OMB A-130]; [NARA CUI]; [SP 800-39] (System Level); [SP 800-60 v1]; [SP 800-60 v2]; [NIST CSF] (Core [Identify Function]).

INFORMATION LIFE CYCLE

TASK P-13 Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.

Potential Inputs: Missions, business functions, and mission/business processes the system will support; system stakeholder information; authorization boundary information; information about other systems that interact with the system (e.g., information exchange/connection agreements); system design documentation; system element information; list of system information types.

Expected Outputs: Documentation of the stages through which information passes in the system, such as a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Such documentation includes, for example, data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries.

Primary Responsibility: Senior Agency Official for Privacy; System Owner; Information Owner or Steward.

Supporting Roles: Chief Information Officer; Mission or Business Owner; Security Architect; Privacy Architect; Enterprise Architect; Systems Security Engineer; Privacy Engineer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: The information life cycle describes the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion [OMB A-130]. Identifying and understanding how each information type is processed during all stages of the life cycle helps organizations identify considerations for protecting the information, informs the organization's security and privacy risk assessments, and informs the selection and implementation of controls. Identification and understanding of the information life cycle facilitates the employment of practices to help ensure, for example, that organizations have the authority to collect or create information, develop rules related to the processing of information in accordance with its impact level, create agreements for information sharing, and follow retention schedules for the storage and disposition of information.

Using tools such as a data map enables organizations to understand how information is being processed so that organizations can better assess where security and privacy risks could arise and where controls could be applied most effectively. It is important for organizations to consider the appropriate delineation of the authorization boundary and the information system's interaction with other systems because the way information enters and leaves the system can affect the security and privacy risk assessments. The elements of the system are identified with sufficient granularity to support such risk assessments.

Identifying and understanding the information life cycle is particularly relevant for the assessment of security and privacy risks since information may be processed by a system in any of the SDLC phases. For example, in the testing and integration phase of the SDLC, processing actual (i.e., live) data would likely raise security and privacy risks, but using substitute (i.e., synthetic) data may allow an equivalent benefit in terms of system testing while reducing risk.

References: [OMB A-130]; [OMB M-13-13]; [NARA RECM]; [NIST CSF] (Core [Identify Function]); [IR 8062].

RISK ASSESSMENT—SYSTEM

TASK P-14 Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.

Potential Inputs: Assets to be protected; missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; system stakeholder information; information about other systems that interact with the system; provider information; threat information; data map; system design documentation; Cybersecurity Framework Profiles; risk management strategy; organization-level risk assessment results.

Expected Outputs: Security and privacy risk assessment reports.

Primary Responsibility: System Owner; System Security Officer; System Privacy Officer.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; Control Assessor.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: This task may require that organizations conduct security and privacy risk assessments to ensure that each type of risk is fully assessed. Assessment of security risk includes identification of threat sources[67] and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets. As a key part of the risk assessment, assets are prioritized based on the adverse impact or consequence of asset loss. The meaning of loss is defined for each asset type to enable a determination of the loss consequence (i.e., the adverse impact of the loss). Loss consequences may be tangible (e.g., monetary, industrial casualties) or intangible (e.g., reputation) and constitute a continuum that spans from partial loss to total loss relative to the asset. Interpretations of information loss may include, for example, loss of possession, destruction, or loss of precision or accuracy. The loss of a function or service may be interpreted as a loss of control, loss of accessibility, loss of the ability to deliver normal function, performance, or behavior, or a limited loss of capability resulting in a level of degradation of function, performance, or behavior. Physical consequences of compromise can include unscheduled production downtime, industrial equipment damage, casualties at the site, environmental disasters and public safety threats. Prioritization of assets is based on asset value, physical consequences, cost of replacement, criticality, impact on image or reputation, or trust by users, by collaborating organizations, or by mission or business partners. The asset priority translates to precedence in allocating resources, determining strength of mechanisms, and defining levels of assurance.

Privacy risk assessments are conducted to determine the likelihood that a given operation the system is taking when processing PII could create an adverse effect on individuals—and the potential impact on individuals.[68] These adverse effects can arise from unauthorized activities that lead to the loss of confidentiality, integrity, or availability in information systems processing PII, or may arise as a byproduct of authorized activities. Privacy risk assessments are influenced by contextual factors. Contextual factors can include, but are not limited to, the sensitivity level of the PII, including specific elements or in aggregate; the types of organizations using or interacting with the system and individuals' perceptions about the organizations with respect to privacy; individuals' understanding about the nature and purpose of the processing; and the privacy interests of individuals, technological expertise or demographic characteristics that influence their understanding or behavior. The privacy risks to individuals may affect

[67] In addition, the use of threat intelligence, threat analysis, and threat modelling can help organizations develop the security capabilities necessary to reduce organizational susceptibility to a variety of threats including hostile cyber-attacks, equipment failures, natural disasters, and errors of omission and commission.

[68] [IR 8062] introduces privacy risk management and a privacy risk model for conducting privacy risk assessments.

individuals' decisions to engage with the system thereby impacting mission or business objectives, or create legal liability, reputational risks, or other types of risks for the organization. Impacts to the organization are not privacy risks. However, these impacts can guide and inform organizational decision-making and influence prioritization and resource allocation for risk response.

Risk assessments are also conducted to determine the potential that the use of an external provider for the development, implementation, maintenance, management, operation, or disposition of a system, system element, or service could create a loss, and the potential impact of that loss. The impact may be immediate (e.g., physical theft) or on-going (e.g., the ability of adversaries to replicate critical equipment because of theft). The impact may be endemic (e.g., limited to a single system) or systemic (e.g., including any system that uses a specific type of system component). Supply chain risk assessments consider vulnerabilities which may arise related to the disposition of a system or system element and from the use of external providers. Vulnerabilities in the supply chain may include a lack of traceability or accountability leading to the potential use of counterfeits, insertion of malware, or poor-quality systems. The use of external providers may result in a loss of visibility and control over how systems, system elements, and services are developed, deployed, and maintained. A clear understanding of the threats, vulnerabilities, and potential impacts of an adverse supply chain event can help organizations appropriately balance supply chain risk with risk tolerance. Supply chain risk assessments can include information from supplier audits, reviews, and supply chain intelligence. Organizations develop a strategy for collecting information, including a strategy for collaborating with providers on supply chain risk assessments. Such collaboration helps organizations leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers.

Risk assessments are conducted throughout the SDLC and support various RMF steps and tasks. Risk assessment results are used to inform security and privacy requirements definition; categorization decisions; the selection, tailoring, implementation, and assessment of controls; authorization decisions; potential courses of action and prioritization for risk responses; and continuous monitoring strategy. Organizations determine the form of risk assessment conducted (including the scope, rigor, and formality of such assessments) and method of reporting results.

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-39] (Organization Level); [SP 800-59]; [SP 800-60 v1]; [SP 800-60 v2]; [SP 800-64]; [SP 800-160 v1] (Stakeholder Needs and Requirements Definition and Risk Management Processes); [SP 800-161] (Assess); [IR 8062]; [IR 8179]; [NIST CSF] (Core [Identify Function]); [CNSSI 1253].

REQUIREMENTS DEFINITION

TASK P-15 Define the security and privacy requirements for the system and the environment of operation.

Potential Inputs: System design documentation; organization- and system-level risk assessment results; known set of stakeholder assets to be protected; missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; system stakeholder information; data map of the information life cycle for PII; Cybersecurity Framework Profiles; information about other systems that interact with the system; supply chain information; threat information; laws, executive orders, directives, regulations, or policies that apply to the system; risk management strategy.

Expected Outputs: Documented security and privacy requirements.

Primary Responsibility: Mission or Business Owner; System Owner; Information Owner or Steward; System Privacy Officer.[69]

[69] The system privacy officer is a primary role only when the information system processes PII.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Security Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer; Security Architect; Privacy Architect; Enterprise Architect.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Protection needs are an expression of the protection capability required for the system in order to reduce security and privacy risk to an acceptable level while supporting mission or business needs. Protection needs include the security characteristics[70] of the system and the security behavior of the system in its intended operational environment and across all system life cycle phases. The protection needs reflect the priorities of stakeholders, results of negotiations among stakeholders in response to conflicts, opposing priorities, contradictions, and stated objectives, and thus, are inherently subjective. The protection needs are documented to help ensure that the reasoning, assumptions, and constraints associated with those needs are available for future reference and to provide traceability to the security and privacy requirements. Security and privacy requirements[71] constitute a formal, more granular expression of protection needs across all SDLC phases, the associated life cycle processes, and protections for the assets associated with the system. Security and privacy requirements are obtained from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). Security and privacy requirements are an important part of the formal expression of the required characteristics of the system.[72] The security and privacy requirements guide and inform the selection of controls for a system and the tailoring activities associated with those controls.

Organizations can use the Cybersecurity Framework to manage security and privacy requirements and express those requirements in Cybersecurity Framework *Profiles* defined for the organization. For instance, multiple requirements can be aligned and even deconflicted using the *Function-Category-Subcategory* structure of the Framework Core. The Profiles can then be used to inform the development of organizationally-tailored control baselines described in the RMF *Prepare-Organization Level* step, Task P-4.

References: [SP 800-39] (Organization Level); [SP 800-64]; [SP 800-160 v1] (Stakeholder Needs and Requirements Definition Process); [SP 800-161] (Multi-Tiered Risk Management); [IR 8179]; [NIST CSF] (Core [Protect, Detect, Respond, Recover Functions]; Profiles).

ENTERPRISE ARCHITECTURE

TASK P-16 Determine the placement of the system within the enterprise architecture.

Potential Inputs: Security and privacy requirements; organization- and system-level risk assessment results; enterprise architecture information; security architecture information; privacy architecture information; asset information.

Expected Outputs: Updated enterprise architecture; updated security architecture; updated privacy architecture; plans to use cloud-based systems and shared systems, services, or applications.

---

[70] For example, a fundamental security characteristic is that the system exhibits only specified behaviors, interactions, and outcomes.

[71] The term *requirements* can have discrete meanings. For example, legal and policy requirements impose obligations to which organizations must adhere. Security and privacy requirements, however, are derived from the protection needs for the system and those protection needs can derive from legal or policy requirements, mission or business needs, risk assessments, or other sources.

[72] Security and privacy requirements can also include *assurance* requirements. Assurance is having confidence about the ability of the system to remain trustworthy with respect to security and privacy across all forms of adversity resulting from malicious or non-malicious intent.

Primary Responsibility: Mission or Business Owner; Enterprise Architect; Security Architect; Privacy Architect.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; Information Owner or Steward.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Enterprise architecture is a management practice used to maximize the effectiveness of mission/business processes and information resources and to achieve mission and business success. An enterprise architecture can provide greater understanding of information and operational technologies included in the initial design and development of information systems and is a prerequisite for achieving resilience and survivability of those systems in an environment of increasingly sophisticated threats. Enterprise architecture also provides an opportunity for organizations to consolidate, standardize, and optimize information and technology assets. An effectively implemented architecture produces systems that are more transparent and therefore, easier to understand and protect. Enterprise architecture also establishes an unambiguous connection from investments to measurable performance improvements. The placement of a system within the enterprise architecture is important as it provides greater visibility and understanding about the other systems (internal and external) that are connected to the system and can also be used to establish security domains for increased levels of protection for the system.

The security architecture and the privacy architecture are integral parts of the enterprise architecture. These architectures represent the parts of the enterprise architecture related to the implementation of security and privacy requirements. The primary purpose of the security and privacy architectures is to ensure that security and privacy requirements are consistently and cost-effectively met in organizational systems and are aligned with the risk management strategy. The security and privacy architectures provide a roadmap that facilitates traceability from the strategic goals and objectives of organizations, through protection needs and security and privacy requirements, to specific security and privacy solutions provided by people, processes, and technologies.

References: [SP 800-39] (Mission/Business Process Level); [SP 800-64]; [SP 800-160 v1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]; Profiles); [OMB FEA].

REQUIREMENTS ALLOCATION

TASK P-17 Allocate security and privacy requirements to the system and to the environment of operation.

Potential Inputs: Organization- and system-level risk assessment results; documented security and privacy requirements; organization- and system-level risk assessment results; list of common control providers and common controls available for inheritance; system description; system element information; system component inventory; relevant laws, executive orders, directives, regulations, and policies.

Expected Outputs: List of security and privacy requirements allocated to the system, system elements, and the environment of operation.

Primary Responsibility: Security Architect; Privacy Architect; System Security Officer; System Privacy Officer.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Security and privacy requirements are allocated to guide and inform control selection and implementation for the organization, system, system elements, and/or environment of operation.[73] Requirements allocation identifies where controls will be implemented. The allocation of requirements conserves resources and helps to streamline the risk management process by ensuring that requirements are not implemented on multiple systems or system elements when implementation of a common control or a system-level control on a specific system element provides the needed protection capability.

References: [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-64]; [SP 800-160 v1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]; Profiles); [OMB FEA].

SYSTEM REGISTRATION

TASK P-18 Register the system with organizational program or management offices.

Potential Inputs: Organizational policy on system registration; system information.

Expected Outputs: Registered system in accordance with organizational policy.

Primary Responsibility: System Owner.

Supporting Role: Mission or Business Owner; Chief Information Officer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: System registration, in accordance with organizational policy, serves to inform the governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and the expected security and privacy implications for the organization due to the operation and use of the system. System registration provides organizations with a management and tracking tool to facilitate bringing the system into the enterprise architecture, implementation of protections that are commensurate with risk, and security and privacy posture reporting in accordance with applicable laws, executive orders, directives, regulations, policies, or standards. As part of the system registration process, organizations add the system to the organization-wide system inventory. System registration information is updated with security categorization and system characterization information upon completion of the *Categorize* step.

References: None.

[73] The environment of operation for an information system refers to the physical surroundings in which the system processes, stores, and transmits information. For example, *security requirements* are allocated to the facilities where the system is located and operates. Those security requirements can be satisfied by the physical security controls in [SP 800-53]

3.2 CATEGORIZE[74]

Purpose

The purpose of the ***Categorize*** step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

CATEGORIZE TASKS

Table 3 provides a summary of tasks and expected outcomes for the RMF *Categorize* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 3: CATEGORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK C-1 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]
TASK C-2 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] • Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [*Cybersecurity Framework*: **Profile**] • Security categorization results reflect the organization's risk management strategy.
TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

SYSTEM DESCRIPTION

TASK C-1 Document the characteristics of the system.

Potential Inputs: System design and requirements documentation; authorization boundary information; list of security and privacy requirements allocated to the system, system elements, and the environment

[74] The RMF *Categorize* step is a precondition for the selection of security controls. However, for privacy, there are other factors considered by organizations that guide and inform the selection of privacy controls. These factors are described in the RMF *Prepare-System Level* step, Task P-15.

of operation; physical or other processes controlled by system elements; system element information; system component inventory; system element supply chain information, including inventory and supplier information; security categorization; data map of the information life cycle for information types processed, stored, and transmitted by the system; information on system use, users, and roles.

Expected Outputs: Documented system description.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: A description of the system characteristics is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the SDLC. Duplication of information is avoided, whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the security categorization and the security and privacy risk assessments of the system. Information may be added to or updated in the system description as it becomes available during the system life cycle, during the execution of the RMF steps, and as any system characteristics change.

Examples of different types of descriptive information that organizations can include in security and privacy plans include: descriptive name of the system and system identifier; system version or release number; manufacturer and supplier information; individual responsible for the system; system contact information; organization that manages, owns, or controls the system; system location; purpose of the system and missions/business processes supported; how the system is integrated into the enterprise architecture; SDLC phase; results of the categorization process and privacy risk assessment; authorization boundary; laws, directives, policies, regulations, or standards affecting individuals' privacy and the security of the system; architectural description of the system including network topology; information types; hardware, firmware, and software components that are part of the system; hardware, software, and system interfaces (internal and external); information flows within the system; network connection rules for communicating with external systems; interconnected systems and identifiers for those systems; physical or other processes, components and equipment controlled by system elements; system users (including affiliations, access rights, privileges, citizenship); system provenance in the supply chain; maintenance or other relevant agreements; potential suppliers for replacement components for the system; alternative compatible system components; number and location in inventory of replacement system components; ownership or operation of the system (government-owned, government-operated; government-owned, contractor-operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees]); incident response points of contact; authorization date and authorization termination date; and ongoing authorization status. System registration information is updated with the system characterization information (see Task P-18).

References: [SP 800-18]; [NIST CSF] (Core [Identify Function]).

SECURITY CATEGORIZATION

TASK C-2 Categorize the system and document the security categorization results.

Potential Inputs: Risk management strategy; organizational risk tolerance; authorization boundary (i.e., system) information; organization- and system-level risk assessment results; information types processed, stored, or transmitted by the system; list of security and privacy requirements allocated to the system, system elements, and environment of operation; organizational authority or purpose for operating the system; business impact analyses or criticality analyses; information about missions, business functions, and mission/business processes supported by the system.

Expected Outputs: Impact levels determined for each information type and for each security objective (confidentiality, integrity, availability); security categorization based on high-water mark of information type impact levels.

Primary Responsibility: System Owner; Information Owner or Steward.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official or Authorizing Official Designated Representative; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Security categorization determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the loss of confidentiality, integrity, or availability of information. Organizations have flexibility in conducting a security categorization using either [FIPS 200] to establish a single impact level for a system based on the high-water mark concept (for other than national security systems), or [CNSSI 1253] to establish three impact values that may vary for each of the security objectives of confidentiality, integrity, and availability (for national security systems). The security categorization process is carried out by the system owner and the information owner or steward in cooperation and collaboration with senior leaders and executives with mission, business function, or risk management responsibilities. Cooperation and collaboration helps to ensure that individual systems are categorized based on the mission and business objectives of the organization. The system owner and information owner or steward consider the results from the security risk assessment (and the privacy risk assessment when the system processes PII) as a part of the security categorization decision. The decision is consistent with the risk management strategy. The results of the categorization process influence the selection of security controls for the system. Security categorization information is documented in the system security plan or included as an attachment to the plan and can be cross-referenced in a privacy plan when the system processes PII.

The security categorization results for the system can be further refined by the organization to facilitate an impact-level prioritization of systems with the same impact level (see Task P-6). Results from the impact-level prioritization conducted by the organization can be used to help system owners in control selection and tailoring decisions.

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-39] (System Level); [SP 800-59]; [SP 800-60 v1]; [SP 800-60 v2]; [SP 800-160 v1] (Stakeholder Needs and Requirements Definition and System Requirements Definition Processes); [IR 8179]; [CNSSI 1253]; [NIST CSF] (Core [Identify Function]).

SECURITY CATEGORIZATION REVIEW AND APPROVAL

TASK C-3 Review and approve the security categorization results and decision.

Potential Inputs: Impact levels determined for each information type and for each security objective (confidentiality, integrity, availability); security categorization based on high-water mark of information type impact levels; list of high value assets for the organization.

Expected Outputs: Approval of security categorization for the system.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative; Senior Agency Official for Privacy.[75]

[75] The senior agency official for privacy participates in determining whether the information processed by the information system is considered PII, and is involved in reviewing and approving the categorization for such systems.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: For information systems that process PII, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.[76] Security categorization results and decisions are reviewed by the authorizing official or a designated representative to ensure that the security category selected for the information system is consistent with the mission and business functions of the organization and the need to adequately protect those missions and functions. The authorizing official or designated representative reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with the categorization decisions for all other organizational systems. The authorizing official collaborates with the senior accountable official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high value assets. As part of the approval process, the authorizing official can provide specific guidance to the system owner with respect to any limitations on baseline tailoring activities for the system that occur at the RMF *Select* step (see Task S-2). If the security categorization decision is not approved, the system owner initiates steps to repeat the categorization process and resubmits the adjusted results to the authorizing official or designated representative. System registration information is subsequently updated with the approved security categorization information (see Task P-18).

References: [FIPS 199]; [SP 800-30]; [SP 800-39] (Organization Level); [SP 800-160 v1] (Stakeholder Needs and Requirements Definition Process); [CNSSI 1253]; [NIST CSF] (Core [Identify Function]).

[76] The responsibilities of the senior agency official for privacy are detailed in [OMB A-130].

3.3 SELECT

Purpose

The purpose of the ***Select*** step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

SELECT TASKS

Table 4 provides a summary of tasks and expected outcomes for the RMF *Select* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 4: SELECT TASKS AND OUTCOMES

Tasks	Outcomes
TASK S-1 CONTROL SELECTION	• Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**]
TASK S-2 CONTROL TAILORING	• Controls are tailored producing tailored control baselines. [*Cybersecurity Framework*: **Profile**]
TASK S-3 CONTROL ALLOCATION	• Controls are designated as system-specific, hybrid, or common controls. • Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [*Cybersecurity Framework*: **Profile**; **PR.IP**]
TASK S-4 DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS	• Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**]
TASK S-5 CONTINUOUS MONITORING STRATEGY—SYSTEM	• A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV**; **DE.CM**]
TASK S-6 PLAN REVIEW AND APPROVAL	• Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

CONTROL SELECTION

TASK S-1 Select the controls for the system and the environment of operation.

Potential Inputs: Security categorization; organization- and system-level risk assessment results; system element information; system component inventory; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; Cybersecurity Framework Profiles.

Expected Outputs: Controls selected for the system and the environment of operation.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Discussion: There are two approaches that can be used for the initial selection of controls: a *baseline* control selection approach, or an *organization-generated* control selection approach. The baseline control selection approach uses control baselines, which are pre-defined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Control baselines serve as a starting point for the protection of individuals' privacy, information, and information systems. Federal control baselines are provided in [SP 800-53B]. The system security categorization (see Task C-2) and the security requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards (see Task P-15) can help inform the selection of security control baselines. A privacy risk assessment (see Task P-14) and privacy requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards (see Task P-15) can help inform the selection of privacy control baselines. Privacy programs use security and privacy control baselines to manage the privacy risks arising from both unauthorized system activity or behavior, as well as from authorized activities. After the pre-defined control baseline is selected, organizations tailor the baseline in accordance with the guidance provided (see Task S-2). The baseline control selection approach can provide consistency across a broad community of interest.

The organization-generated control selection approach differs from the baseline selection approach because the organization does not start with a pre-defined set of controls. Rather, the organization uses its own selection process to select controls. This may be necessary when the system is highly specialized (e.g., a weapons system or a medical device) or has limited purpose or scope (e.g., a smart meter). In these situations, it may be more efficient and cost-effective for an organization to select a specific set of controls for the system (i.e., a bottom-up approach) instead of starting with a pre-defined set of controls from a broad-based control baseline and subsequently eliminating controls through the tailoring process (i.e., top-down approach).

In both the baseline control selection approach and organization-generated control selection approach, organizations develop a well-defined set of security and privacy requirements using a life cycle-based systems engineering process (e.g., [ISO 15288] and [SP 800-160 v1] as described in the RMF *Prepare-System Level* step, Task P-15. This process generates a set of requirements that can be used to guide and inform the selection of a set of controls to satisfy the requirements (whether the organization starts with a control baseline or generates the set of controls from its own selection process). Similarly, organizations can use the [NIST CSF] to develop Cybersecurity Framework *Profiles* representing a set of organization-specific security and privacy requirements—and thus, guiding and informing control selection from [SP 800-53]. Tailoring may also be required in the organization-generated control selection approach (see Task S-2). Organizations do not need to choose one approach for the selection of controls for each of their systems, but instead, may use different approaches as circumstances dictate.

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-53]; [SP 800-53B]; [SP 800-160 v1] (System Requirements Definition, Architecture Definition, and Design Definition Processes); [SP 800-161] (Respond and Chapter 3); [IR 8062]; [IR 8179]; [CNSSI 1253]; [NIST CSF] (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

CONTROL TAILORING

TASK S-2 Tailor the controls selected for the system and the environment of operation.