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 (RMF).

Organization-Level Tasks & Roles

P-1, Risk Management Roles

- Identify and assign individuals to roles
  - Primary Roles: Head of Agency, Chief Information Officer, & Senior Agency Official for Privacy

Potential Inputs: *Organizational security and privacy policies and procedures; organizational charts*
Expected Outputs: *Documented Risk Management Framework role assignments*

P-2, Risk Management Strategy

- Establish a risk management strategy for the organization
  - Primary Role: Head of Agency

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

Expected Outputs: *Risk management strategy & statement of risk tolerance inclusive of information security & privacy*

P-3, Risk Assessment - Organization

- Assess organization-wide security and privacy risk and update the risk assessment
  - Primary Roles: Senior Accountable Official for Risk Management or Risk Executive

Potential Inputs: *Risk management strategy; mission objectives; risk assessment results; 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*

P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)

- Establish, document, and publish organizationally-tailored control baselines
  - Primary Roles: Mission or Business Owner & Senior Accountable Official for Risk Management or Risk Executive (Function)

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*

Expected Outputs: *List of approved or directed organizationally-tailored control baselines & NIST Cybersecurity Framework (CSF) Profiles*

P-5, Common Control Identification

- Identify, document, and publish common controls
  - Primary Roles: Senior Agency Information Security Officer & Senior Agency Official for Privacy

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 that provide a description of the common control implementation*

P-6, Impact-Level Prioritization (Optional)

- Prioritize organizational systems with the same impact level
  - Primary Roles: Senior Accountable Official for Risk Management or Risk Executive (Function)

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 are prioritized into low-, moderate-, and high-impact sub-categories*

P-7, Continuous Monitoring Strategy - Organization

- Develop and implement an organization-wide strategy
  - Primary Roles: Senior Accountable Official for Risk Management or Risk Executive (Function)

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

Expected Outputs*: Implemented organizational continuous monitoring strategy*

System-Level Tasks & Roles

P-8, Mission or Business Owner

- Identify the missions/business functions & processes
  - Primary Role: Mission or Business Owner

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, & mission/business processes that the system will support*

P-9, System Stakeholders

- Identify stakeholders
  - Primary Roles: Mission or Business Owner & System Owner

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*

P-10, Asset Identification

- Identify assets that require protection
  - Primary Role: System Owner

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*

P-11, Authorization Boundary

- Determine the authorization boundary of the system
  - Primary Role: Authorizing Official (AO)

Potential Inputs: *System design documentation; network diagrams; system stakeholder information; asset information; network and/or enterprise architecture diagrams; organizational structure*

Expected Outputs: *Documented authorization boundary*

P-12, Information Types

- Identify the types of information
  - Primary Roles: System Owner & Information Owner or Steward

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

Expected Outputs: *List of information types for the system*

P-13, Information Life Cycle

- Identify and understand all stages of the information life cycle
  - Primary Roles: Senior Agency Official for Privacy, System Owner & Information Owner or Steward

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; system design documentation; system element information; list of system information types*

Expected Outputs*: Documentation of the stages through which information passes in the system*

P-14, Risk Assessment

- System - conduct a system-level risk assessment and update the risk assessment
  - Primary Roles: System Owner, System Security Officer, & System Privacy Officer

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; organizational-level risk assessment results*

Expected Outputs: *Security and privacy risk assessment reports*

System-Level Tasks & Roles (Continued)

P-15, Requirements Definition

- Define the security and privacy requirements
  - Primary Roles: Mission or Business Owner, System Owner, Information Owner or Steward, & System Privacy Officer

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*

P-16, Enterprise Architecture

- Determine the placement of the system within the enterprise architecture
  - Primary Roles: Mission or Business Owner, Enterprise Architect, & Security & Privacy Architect

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

Expected Outputs: *Updated enterprise architecture, security architecture, privacy architecture, plans to use cloud-based systems, & shared systems, services, or applications*

P-17, Requirement Allocation

- Allocate security requirements to the system
  - Primary Roles: Security Architect, Privacy Architect, System Security Officer, & System Privacy Officer

Potential Inputs: *Organization- and system-level risk assessment results; documented security and privacy requirements; 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, & the environment of operation*

P-18, System Registration

- Register the system with organizational program or management offices
  - Primary Role: System Owner

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

Expected Outputs: *Registered system in accordance with organizational policy*

For more Information visit the CS101 Risk Management Framework Prepare Step Course Resources:
https://www.cdse.edu/Training/elearning/CS101-resources/