Introduction to the RMF for SAPs Short

Student Guide

June 2024

Center for Development of Security Excellence

Contents

Introduction to the RMF for SAPs Short

Introduction

Every day, we hear about attacks on our information systems, or ISs, and networks. Protecting IS assets from criminal hackers and other adversaries is especially important for Special Access Programs, or SAPs, whose information may have a significant impact on national security. To protect systems, networks, and information they contain, cybersecurity specialists use the Risk Management Framework, or RMF, along with the key concepts of authentication and non-repudiation. Together, these concepts maintain information security, ensuring the information remains confidential, retains its integrity, and is available when needed. These three security objectives are commonly referred to as C-I-A.

Objective

Welcome to the Introduction to the RMF for SAPs Short. This Short will introduce you to each step of the RMF's purpose for SAP ISs.

Here is the Short's objective:

- Describe the purpose of each step of the RMF for SAP ISs.

Impact Levels

Maintaining confidentiality is critically important, but that is not the only necessary consideration. While ensuring that information is not disclosed to unauthorized entities is, of course, critically important, information must also be preserved from unauthorized modification, whether intentional or unintentional, and it must be accessible only by authorized users, in the appropriate place and form, and at the appropriate time.

The RMF process considers and addresses the security objectives:

- Confidentiality
- Integrity
- Availability

Each security objective is then assigned an impact level, based on the impact of the loss of C-I-A. Impact level ratings of low, moderate, or high are assigned for each of these security objectives.

Confidentiality

Confidentiality: Information is not disclosed to unauthorized entities or processes.

Impact Levels:

- **Moderate:** Unauthorized disclosure could have a **serious** adverse effect.
- **High:** Unauthorized disclosure could have a **severe or catastrophic** adverse effect.

Note: All SAP systems have confidentiality impact levels of Moderate or High.

Integrity

Integrity: Data is preserved from unauthorized modification, whether intentional or unintentional.

Impact Levels:

- **Low:** Unauthorized modification or destruction could have a **limited** adverse effect.
- **Moderate:** Unauthorized modification or destruction could have a **serious** adverse effect.
- **High:** Unauthorized modification or destruction could have a **severe or catastrophic** adverse effect.

Availability

Availability: Data is accessible by the authorized user, in the appropriate place and form, at the appropriate time.

Availability Impact Levels:

- **Low:** Disruption of access to or use of information processed, stored, and transmitted by the IS could have a **limited** adverse effect.
- **Moderate:** Disruption of access to or use of information processed, stored, and transmitted by the IS could have a **serious** adverse effect.
- **High:** Disruption of access to or use of information processed, stored, and transmitted by the IS could have a **severe or catastrophic** adverse effect.

Authentication and Non-Repudiation

Two key cybersecurity concepts support the confidentiality, integrity, and availability of information: authentication and non-repudiation.

Authentication is the process of determining whether someone or something is who or what it claims to be. It uses something you know, such as a password, combined with something you have, such as a common access card, or CAC, to authenticate the user's identity.

Non-repudiation establishes the "proof concept," and provides evidence of the data's origin, such as a digital signature.

Roles

The protection of ISs, networks, and the information on those systems requires the support of a large number of individuals and organizations.

These individual roles and organizations include general support and oversight roles that facilitate several **control families**, which are areas of information security that are essential to securing ISs.

A complete list of the control families can be found in the DOD Joint SAP Implementation Guide, or JSIG.

In addition, **RMF decision authorities** make authorization and risk management decisions, while **RMF assessors and owners** have oversight responsibilities and conduct assessments of ISs. Finally, **RMF implementers** are those individuals responsible for the development and maintenance of IS security.

Visit the Short Resources to access detailed descriptions of these roles in the Introduction to the RMF for SAPs Job Aid, as well as the DOD JSIG.

Support / Oversight Roles

General support and oversight roles include:

- Program Security Officer (PSO) – must be in the Government
- Government SAP Security Officer (GSSO) – must be in the Government
- Contractor Program Security Officer (CPSO)

RMF Decision Authorities

RMF decision authorities include:

- Element Head or Oversight Authority / Cognizant Authority SAP Central Office (SAPCO)
- Authorizing Official (AO)
- Delegated Authorizing Official (DAO)

RMF Assessors

RMF assessors and owners are inherently Government personnel and include:

- Security Control Assessor (SCA)
- Authorizing Official Designated Representative (AODR)
- Information Owner / Steward

RMF Implementers

RMF implementers include:

- IS Owner (ISO), typically either the:
  - Government Program Manager (GPM) or
  - Contractor Program Manager (CPM)
- IS Security Manager (ISSM) / IS Security Officer (ISSO)
- IS Security Engineer (ISSE) / IS Architect or Information Assurance Systems Architect and Engineer (IASAE)

Risk Management Framework

The RMF includes seven steps:

- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize

- Monitor

The National Institute of Standards and Technology Special Publication, or NIST SP, 800-37, outlines the tasks for each of these steps.

Let's explore the purpose, roles, and tasks associated with each of these steps.

Prepare Step

The Prepare step focuses on planning to manage security and privacy risks using the RMF.

Purpose: Carry out essential activities to prepare to manage the organization's security and privacy risks.

Prepare Roles

The roles engaged in the Prepare step include:

- Head of Agency
- Chief Information Officer
- Mission or Business Owner
- Senior Accountable Official for Risk Management or Risk Executive (function)
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Prepare Tasks

Within the Prepare step, there are 18 tasks. For this Short, we will focus on the seven organizational level tasks.

P-1 Risk Management Roles: Identify and assign individuals to specific roles associated with security and privacy risk management.

- **Primary Responsibility:**
  - Head of Agency
  - Chief Information Officer
  - Senior Agency Official for Privacy
- **Output:** Documented Risk Management Framework role assignments

P-2 Risk Management Strategy: Establish a risk management strategy for the organization that includes a determination of risk tolerance.

- **Primary Responsibility:** Head of Agency
- **Outputs:**
  - Risk management strategy
  - Statement of risk tolerance inclusive of information security and privacy risk

P-3 Risk Assessment—Organization: Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.

- **Primary Responsibility:**
  - Senior Accountable Official for Risk Management or Risk Executive (function)
  - Senior Agency Information Security Officer
  - Senior Agency Official for Privacy
- **Output:** Organization-level risk assessment results

P-4 Organizationally-Tailored Control Baselines and Cybersecurity Framework

(CSF) Profiles (optional): Establish, document, and publish organizationally-tailored control baselines and/or CSF profiles.

- with security and privacy risk management.
- **Primary Responsibility:**
  - Mission or Business Owner
  - Senior Accountable Official for Risk Management or Risk Executive (function)
- **Outputs:**
  - List of approved or directed organizationally-tailored control baselines
  - NIST CSF profiles

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

- **Primary Responsibility:**
  - Senior Agency Information Security Officer
  - Senior Agency Official for Privacy
- **Outputs:**
  - List of common control providers and common controls available for inheritance
  - Security and privacy plans / system security plan (SSP) or equivalent documents, providing a description of the common control implementation, including inputs, expected behavior, and expected outputs

P-6 Impact-Level Prioritization (Optional): Prioritize organizational systems with the same impact level.

- **Primary Responsibility:** Senior Accountable Official for Risk Management or Risk Executive (function)
- **Output:** Organizational systems prioritized into low-, moderate-, and high-impact subcategories

P-7 Continuous Monitoring (ConMon) Strategy—Organization: Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.

- **Primary Responsibility:** Senior Accountable Official for Risk Management or Risk Executive (function)
- **Output:** An implemented organizational ConMon strategy

Categorize Step

Purpose: Categorize the IS based on an analysis of the impact due to a loss of confidentiality, integrity, and availability.

RMF decision authorities categorize the IS. The information processed, stored, and transmitted by the system is analyzed to determine which security controls must be implemented. This analysis leads to a defined impact level of low, moderate, or high. These impact levels determine which security controls must be implemented.

It is important to recognize that all SAP systems have confidentiality impact levels of moderate or high. The impact level is moderate if it will have a serious adverse effect. The impact level is high if it will have a severe or catastrophic adverse effect.

Categorize Roles

The roles engaged in the Categorize step include:

- AO
- ISO
- SCA
- ISSO / ISSM
- ISSE
- Senior Agency Official for Privacy

Categorize Tasks

Within the Categorize step, there are 3 tasks.

C-1 System Description: Document the characteristics of the system.

- **Primary Responsibility:** ISO
- **Output:** Documented system description

C-2 Security Categorization: Categorize the system and document the security categorization results.

- **Primary Responsibility:**
  - ISO
  - Information Owner / Steward
- **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

C-3 Security Categorization Review and Approval: Review and approve the security categorization results and decision.

- **Primary Responsibility:**
  - AO
  - AODR
  - Senior Agency Official for Privacy
- **Output:** Approval of security categorization for the system

Select Step

Purpose: Select, tailor, and document the controls needed to protect the IS and organization, commensurate with risk.

RMF implementers select an initial set of baseline security controls for the IS based on the security categorization of the system. They apply overlays and tailor controls as needed, based on an organizational assessment of risk and local conditions. Security controls are documented in the security controls traceability matrix, or SCTM, which is part of the system security plan, or SSP.

Select Roles

The roles engaged in the Select step include:

- AO
- ISO

- SCA
- ISSO / ISSM
- ISSE

Select Tasks

Within the Select step, there are 6 tasks.

S-1 Control Selection: Select the controls for the system and the environment of operation.

- **Primary Responsibility:**
  - Common Control Provider (CCP)
  - ISO
  - ISSM / ISSO
  - ISSE
  - SCA
- **Output:** Controls selected for the system and the environment of operation

S-2 Control Tailoring: Tailor the controls selected for the system and the environment of operation.

- **Primary Responsibility:**
  - ISO
  - CCP
- **Output:** List of tailored controls for the system and environment of operation, i.e., tailored control baselines

S-3 Control Allocation: Allocate security and privacy controls to the system and to the environment of operation.

- **Primary Responsibility:**
  - Security Architect
  - Privacy Architect
  - System Security Officer
  - System Privacy Officer
- **Output:** List of security and privacy controls allocated to the system, system elements, and the environment of operation

S-4 Documentation of Planned Control Implementations: Document the controls for the system and environment of operation in security and privacy plans / SSP.

- **Primary Responsibility:** ISO or CCP
- **Output:** Security and privacy plans / SSP

S-5 ConMon Strategy – System: Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational ConMon strategy.

- **Primary Responsibility:**
  - ISO
  - CCP
- **Output:** ConMon strategy for the system including time-based trigger for ongoing authorization

S-6 Plan Review and Approval: Review and approve the security and privacy plans / SSP for the system and the environment of operation.

- **Primary Responsibility:** AO or AODR
- **Output:** Security and privacy plans / SSP approved by the authorizing official

Implement Step

Purpose: Implement the controls in the security and privacy plans / SSP for the system and document the details.

Implement Roles

The roles engaged in the Implement step include:

- ISO
- ISSO / ISSM
- ISSE

Implement Tasks

Within the Implement step, there are 2 tasks.

I-1 Control Implementation: Implement the controls in the security and privacy plans / SSP.

- **Primary Responsibility:** ISO or CCP
- **Output:** Implemented controls

I-2 Update Control Implementation Information: Document changes to planned control implementations based on the "as-implemented" state of controls.

- **Primary Responsibility:**
  - ISO or CCP
  - ISSM / ISSO / ISSE
- **Output:** Update security and privacy plan / SSP with description of how security controls are implemented

Assess Step

Purpose: Determine if controls are implemented correctly, operating as intended, and producing the desired outcome.

Based on the findings from this assessment, assessors then conduct any initial required remediation actions and develop the Security Assessment Report, or SAR.

Assess Roles

The roles engaged in the Assess step include:

- ISO
- SCA
- ISSO / ISSM
- ISSE

Assess Tasks

Within the Assess step, there are 6 tasks.

A-1 Assessor Selection: Select the appropriate assessor or assessment team for the type of control assessment to be conducted.

- **Primary Responsibility:** AO or AODR
- **Output:** Selection of assessor or assessment team responsible for conducting

the control assessment

A-2 Assessment Plan: Develop, review, and approve plan to assess implemented controls.

- **Primary Responsibility:**
  - AO
  - AODR
  - ISO in conjunction with ISSO / ISSM or ISSE
  - SCA
- **Output:** Security and privacy assessment plans

A-3 Control Assessments: Assess the controls in accordance with the assessment procedures described in the security assessment plan.

- **Primary Responsibility:** SCA
- **Output:** Completed control assessments and associated assessment evidence

A-4 Assessment Reports: Prepare the assessment reports documenting the findings and recommendations from the control assessments.

- **Primary Responsibility:** SCA
- **Output:** SAR

A-5 Remediation Actions: Conduct initial remediation actions on the controls and reassess remediated controls.

- **Primary Responsibility:**
  - AO
  - ISO or CCP
  - SCA
  - ISSO / ISSM
- **Outputs:**
  - Completed initial remediation actions based on the security and privacy assessment reports
  - Changes to implementations reassessed by the assessment team
  - Updated security and privacy assessment reports
  - Updated security and privacy plans / SSP including changes to the control implementations

A-6 Plan of Action and Milestones (POA&M): Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.

- **Primary Responsibility:** System Owner or CCP
- **Output:** A plan of action and milestones detailing the findings from the security and privacy assessment reports that are to be remediated

Authorize Step

Purpose: Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk, including supply chain risk, is acceptable.

RMF implementers seek official authorization to operate, or ATO, by submitting the Security Authorization Package. This documents the organization's risk, along with other supporting information.

RMF decision authorities authorize the IS operation based on their review of that package and related information. Authorization decisions result in either ATO; interim authority to test, or IATT; or denial of authorization to operate, or DATO.

Authorize Roles

The roles engaged in the Authorize step include:

- AO
- DAO
- ISO
- ISSO / ISSM

AuthorizeTasks

Within the Authorize step, there are 5 tasks.

R-1 Authorization Package: Assemble the authorization package and submit the package to the authorizing official for an authorization decision.

- **Primary Responsibility:**
  - ISO
  - CCP
  - Senior Agency Official for Privacy
- **Output:** Security Authorization Package, includes SSP / SCTM, SAR, POA&M, risk assessment report (RAR), and ConMon strategy plan

R-2 Risk Analysis and Determination: Analyze and determine the risk from the operation or use of the system or the provision of common controls.

- **Primary Responsibility:** AO or AODR
- **Output:** Risk determination

R-3 Risk Response: Identify and implement a preferred course of action in response to the risk determined.

- **Primary Responsibility:** AO or AODR
- **Output:** Risk responses for determined risks

R-4 Authorization Decision: Determine if the risk from the operation or use of the IS or the provision or use of common controls is acceptable.

- with security and privacy risk management.
- **Primary Responsibility:** AO
- **Output:** Authorization decision document (ATO, DATO, or IATT)

R-5 Authorization Reporting: Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.

- **Primary Responsibility:** AO or AODR
- **Output:** A report indicating the authorization decision for a system or set of common controls

Monitor Step

Purpose: Maintain ongoing situational awareness of IS security and privacy.

If ATO is granted, the IS undergoes continuous monitoring, or ConMon, to assess control effectiveness, to document and analyze changes to the system or environment of operation, and to report the security state of the system.

Monitor Roles

The roles engaged in the Monitor step include:

- ISO
- SCA
- ISSO / ISSM

Monitor Tasks

Within the Monitor step, there are 7 tasks.

M-1 System and Environment Changes: Monitor the IS and its environment of operation for changes that impact the security and privacy posture of the system.

- **Primary Responsibility:**
  - ISO or CCP
  - ISSO / ISSM
  - Senior Agency Official for Privacy Head of Agency
- **Outputs:**
  - Updated security and privacy plan / SSP
  - POA&M
  - Security and privacy assessment reports

M-2 Ongoing Assessments: Assess the controls implemented within and inherited by the system in accordance with the ConMon strategy.

- **Primary Responsibility:**
  - SCA
  - ISSO / ISSM
- **Output:** Updated security and privacy assessment reports

M-3 Ongoing Risk Response: Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.

- **Primary Responsibility:**
  - ISO or CCP
  - ISSO / ISSM
- **Output:** Documented evidence of correction

M-4 Authorization Package Updates: Update plans, assessment reports, and plans of action and milestones based on the results of the ConMon process.

- with security and privacy risk management.
- **Primary Responsibility:** Security Officer (SO) or CCP
- **Outputs:**
  - Updated security and privacy report
  - SSP
  - SAR
  - RAR
  - POA&M

M-5 Security and Privacy Reporting: Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational ConMon strategy.

- **Primary Responsibility:**
  - ISO
  - CCP
  - Senior Agency Official for Privacy

- **Output:** Security and privacy posture reports

M-6 Ongoing Authorization: Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.

- **Primary Responsibility:** AO
- **Outputs:**
  - Risk determination
  - Ongoing authorization or denial

M-7 System Disposal: Implement a system disposal strategy and execute required actions when a system is removed from operation.

- **Primary Responsibility:** SO
- **Output:**
  - Disposal strategy
  - Updated system component inventory
  - Updated security and privacy plans / SSP

Review Activity

Match each step with its summarized purpose.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

1. **Purpose:** Determine if selected controls have been implemented correctly, are operating as intended, and are producing the desired outcome.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

2. **Purpose:** Employ and document the controls in the security and privacy plans / SSP for the system and organization.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

3. **Purpose:** Maintain ongoing situational awareness of the security and privacy posture of the IS and organization.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

4. **Purpose:** Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk is acceptable.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement

- ○ Assess
- ○ Authorize
- ○ Monitor

5. **Purpose:** Inform organizational risk management processes and tasks by determining the adverse impact.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor
6. **Purpose:** Carry out essential activities to help the organization manage security and privacy risks using the RMF.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor
7. **Purpose:** Determine, tailor, and document the controls necessary to protect the IS and organization commensurate with risk.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

Conclusion

Congratulations on completing the Introduction to the RMF for SAPs Short.

In this Short, you learned about the purpose of each step of the RMF for SAP ISs.

Access the Introduction to the RMF for SAPs Job Aid from the Resources for related terminology, detailed role descriptions, and supporting tasks.

Appendix A: Answer Key

Review Activity

Match each step with its summarized purpose.

1. **Purpose:** Determine if selected controls have been implemented correctly, are operating as intended, and are producing the desired outcome.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ◉ Assess (correct response)
   - ○ Authorize
   - ○ Monitor

   ***Feedback**: The purpose of the Assess step is to determine if selected controls have been implemented correctly, are operating as intended, and are producing the desired outcome.*

2. **Purpose:** Employ and document the controls in the security and privacy plans / SSP for the system and organization.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ◉ Implement (correct response)
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

   ***Feedback**: The purpose of the Implement step is to employ and document the controls in the security and privacy plans / SSP for the system and organization.*

3. **Purpose:** Maintain ongoing situational awareness of the security and privacy posture of the IS and organization.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize

- ⦿ Monitor (correct response)

Feedback*: The purpose of the Monitor step is to maintain ongoing situational awareness of the security and privacy posture of the IS and organization.*

4. **Purpose:** Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk is acceptable.
   - ○ Prepare
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ⦿ Authorize (correct response)
   - ○ Monitor

Feedback*: The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk is acceptable.*

5. **Purpose:** Inform organizational risk management processes and tasks by determining the adverse impact.
   - ○ Prepare
   - ⦿ Categorize (correct response)
   - ○ Select
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

Feedback*: The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact.*

6. **Purpose:** Carry out essential activities to help the organization manage security and privacy risks using the RMF.
   - ⦿ Prepare (correct response)
   - ○ Categorize
   - ○ Select
   - ○ Implement
   - ○ Assess

- ○ Authorize
- ○ Monitor

***Feedback**: The purpose of the Prepare step is to carry out essential activities to help the organization manage security and privacy risks using the RMF.*

7. **Purpose:** Determine, tailor, and document the controls necessary to protect the IS and organization commensurate with risk.
   - ○ Prepare
   - ○ Categorize
   - ◉ Select (correct response)
   - ○ Implement
   - ○ Assess
   - ○ Authorize
   - ○ Monitor

***Feedback**: The purpose of the Select step is to determine, tailor, and document the controls necessary to protect the IS and organization commensurate with risk.*