Introduction to the RMF for SAPs Short

Student Guide

July 2017

Center for Development of Security Excellence

Contents

Introduction to the RMF for SAPs Short

Introduction

We hear every day about attacks on our information systems and networks. Protecting information system 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 win the war against criminal hackers and other adversaries that wish to harm us, cybersecurity specialists use the Risk Management Framework, or RMF, along with the key concepts of authentication and non-repudiation, to protect information systems and networks, and the information residing on those systems. The RMF helps ensure that information remains not only confidential, but also that it retains its integrity and is available to access when needed.

Welcome to the Introduction to the RMF for SAPs Short.

Impact Levels

It's not enough for information stored on information systems, or IS's and networks to simply remain confidential. 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 by authorized users, in the appropriate place and form, and at the appropriate time.

The RMF process considers and addresses all of these elements: confidentiality, integrity, and availability—or C-I-A—and utilizes impact levels, which reflect the importance of the information and/or the SAP IS. Impact level ratings of low, moderate, or high are assigned for each of these elements.

Confidentiality

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

Confidentiality 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.

Integrity 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, in fact, who or what it is declared to be. It utilizes something you know, such as a password, combined with something you have, such as a CAC, to authenticate the user's identity.

Non-repudiation establishes the "proof concept," and provides the recipient of data with evidence that proves its origin, such as a digital signature.

Roles

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

General support and oversight roles include the Program Security Officer, or PSO; the Government SAP Security Officer, or GSSO; and the Contractor Program Security Officer, or CPSO. These oversight roles facilitate several control families: areas of information security that are essential to securing information systems.

Control Families include (but are not limited to):

- Access Control (AC)

- Awareness and Training (AT)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)

Note: A complete list of the Control Families can be found in the DoD Joint Special Access Program (SAP) Implementation Guide (JSIG).

Application of the RMF process, specifically, requires the participation of several individuals and organizations, in a variety of roles. RMF decision authorities make authorization and risk management decisions. RMF decision authorities include: the element head or service/agency SAP Central Office, or SAPCO; the Authorizing Official, or AO, and the Delegated Authorizing Official, or DAO.

RMF assessors and owners have oversight responsibilities and conduct assessments of information systems. These roles include: the Security Control Assessor, or SCA, and the information owner or steward.

Finally, RMF implementers are those individuals responsible for the development and maintenance of information system security, including: the Information System Owner, or ISO, who is most often the government or contractor Program Manager, or PM; the Information System Security Manager, or ISSM, or the Information System Security Officer, or ISSO; and the Information System Security Engineer, or ISSE. Note that some organizations also refer to an ISSE as an Information Security Architect or Information Assurance Systems Architect and Engineer, or IASAE.

Please refer to the Introduction to the RMF for SAPs Job Aid for more information, including detailed descriptions of each of these roles.

Risk Management Framework

As discussed, the RMF is a fundamental part of the protection of information systems. The RMF is a 6-step process during which information systems and networks are assessed, appropriate control measures are identified and implemented, and the system or network is authorized.

During the first step, RMF decision authorities categorize the IS – and the information processed, stored, and transmitted by the system – in order to determine which security controls must be implemented.

Next, RMF implementers select an initial set of baseline security controls for the IS based on the security categorization of the system and tailor them as needed.

During the third step, RMF implementers implement the security controls and describe how they are employed within the IS and its environment of operation.

In step 4, RMF assessors assess the security controls to determine whether they are implemented correctly, operate as intended, and produce the desired outcome.

In step 5, RMF implementers seek official Authorization to Operate, or ATO. They submit the Security Authorization Package, which documents the organization's risk, along with other supporting documentation.

Finally, provided the RMF decision authorities grant ATO, the IS undergoes continuous monitoring to ensure the controls remain effective and that the impacts of any changes are assessed.

Note that the steps in the RMF process align with the five phases of the System Development Life Cycle, or SDLC, identified by the National Institute of Standards and Technology, or NIST.

Review the supporting tasks for each step, including primary roles and key deliverables.

Step 1: Categorize System

In step 1, the IS is categorized based on an analysis of the impact due to a loss of confidentiality, integrity, and availability. This analysis leads to a defined impact level of low, moderate, or high, and these impact levels determine which security controls must be implemented. Recall that all SAP Systems have confidentiality impact levels of moderate or high.

A risk assessment is conducted before or during this step and documented in a Risk Assessment Report, or RAR.

Step 1 Primary Roles:

- Authorizing Official (AO)
- Information System Owner (ISO)
- Security Control Assessor (SCA)
- Information System Security Manager (ISSM)/ Information System Security Officer (ISSO)
- Information System Security Engineer (ISSE)

There are three supporting tasks in step 1.

Supporting Task 1.1

- **Supporting Task:** Categorize the information system and document the results in the System Security Plan (SSP)

- **Primary Responsibility:** ISO or information owner/steward
- **Output(s):** Draft SSP with system Categorization filled in

Supporting Task 1.2

- **Supporting Task:** Describe the information system (including system boundary) and document the description in the SSP
- **Primary Responsibility:** ISO
- **Output(s):** Updated SSP to include a description of the IS

Supporting Task 1.3

- **Supporting Tasks:** Register the IS with the appropriate organizational program management offices
- **Primary Responsibility:** ISO
- **Output(s):** Document or entry in the IT registry with the official system name, system owner, and categorization.

Step 2: Select Security Controls

In step 2, RMF implementers select the initial set of baseline security controls for the IS, based on the security categorization, and apply overlays and tailor the 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 considered part of the System Security Plan, or SSP.

Step 2 Primary Roles:

- Authorizing Official (AO)
- Information System Owner (ISO)
- Security Control Assessor (SCA)
- Information System Security Manager (ISSM)/ Information System Security Officer (ISSO)
- Information System Security Engineer (ISSE)

There are four supporting tasks in step 2.

Supporting Task 2.1

- **Supporting Task:** Identify the security controls that are provided by the organization as common controls for organizational IS and document the controls in the SSP
- **Primary Responsibility:** Common Control Provider (CCP), ISO, ISSM/ISSO, ISSE, SCA

- **Output(s):** Document the common controls in the SSP/SCTM

Supporting Task 2.2

- **Supporting Task:** Select the security controls for the IS (i.e., baseline, overlays, tailoring) and document the controls in the SSP
- **Primary Responsibility:** ISO, ISSE
- **Output(s):** Document the selected controls in the SSP/SCTM

Supporting Task 2.3

- **Supporting Task:** Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the IS and its environment of operation
- **Primary Responsibility:** ISO or CCP
- **Output(s):** Documented and approved Continuous Monitoring (ConMon) Plan/Strategy that includes frequency of monitoring for each control

Supporting Task 2.4

- **Supporting Task:** Review and approval of the draft SSP by the AO or DAO
- **Primary Responsibility:** AO or DAO, ISSM/ISSO
- **Output(s):** Documented and approved draft SSP/SCTM

Step 3: Implement Security Controls

In step 3, RMF implementers implement the security controls and document this implementation in the SSP.

Step 3 Primary Roles:

- Information System Owner (ISO)
- Information System Security Manager (ISSM)/ Information System Security Officer (ISSO)
- Information System Security Engineer (ISSE)

There are two supporting tasks in step 3.

Supporting Task 3.1

- **Supporting Task:** Implement the security controls specified in the SSP
- **Primary Responsibility:** ISO or CCP
- **Output(s):** Documented and approved Continuous Monitoring (ConMon) Plan/Strategy that includes frequency of monitoring for each control

Supporting Task 3.2

- **Supporting Task:** Document the security control implementation, as appropriate in the SSP, providing a functional description of the control implementation
- **Primary Responsibility:** ISO or CCP; ISSM/ISSO; ISSE
- **Output(s):** Update SSP with information describing how security controls are implemented

Step 4: Assess Security Controls

In this step, the RMF assessors assess the controls to determine whether they are implemented correctly, operating as intended, and producing the desired outcome. Based on findings from this assessment, RMF implementers conduct any required remediation actions. Finally, in this step RMF implementers develop the Security Assessment Report, or SAR.

Step 4 Primary Roles:

- Information System Owner (ISO)
- Security Control Assessor (SCA)
- Information System Security Manager (ISSM)/ Information System Security Officer (ISSO)
- Information System Security Engineer (ISSE)

There are four supporting tasks in step 4.

Supporting Task 4.1

- **Supporting Task:** Develop, review, and approve a plan to assess the security controls
- **Primary Responsibility:** ISSM/ISSO, ISSE, SCA
- **Output(s):** Security Assessment Plan

Supporting Task 4.2

- **Supporting Task:** Assess the security controls in accordance with the assessment procedures defined in the Security Assessment Plan
- **Primary Responsibility:** SCA
- **Output(s):** Individual test results for each test or matrix for all tests

Supporting Task 4.3

- **Supporting Task:** Prepare the SAR, documenting the issues, findings, and recommendations from the security control assessment
- **Primary Responsibility:** SCA
- **Output(s):** Security Assessment Report (SAR)

Supporting Task 4.4

- **Supporting Tasks:** Conduct initial remedial actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate
- **Primary Responsibility:** AO, ISO or CCP, SCA, ISSM/ISSO
- **Output(s):** Updated Security Assessment Plan (SAR), Updated Risk Assessment Report (RAR), Updated System Security Plan (SSP)

Step 5: Authorize System

In this step, RMF decision authorities authorize IS operation based on their review of the Security Authorization Package, which documents the organization's risk, and any additional supporting documentation. This authorization decision will result in authorization to operate, or ATO, interim authority to test, or IATT, or denial of authorization to operate, or DATO.

Step 5 Primary Roles:

- Authorizing Official (AO)
- Delegated Authorizing Official (DAO)
- Information System Owner (ISO)
- Information System Security Manager (ISSM)/ Information System Security Officer (ISSO)

There are four supporting tasks in step 5.

Supporting Task 5.1

- **Supporting Task:** Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations of the SAR, including any remediation actions taken
- **Primary Responsibility:** SCA (documents initial findings); ISO (completes POA&M; adds additional items; includes CCP, if findings are against a common control)
- **Output(s):** POA&M

Supporting Task 5.2

- **Supporting Task:** Assemble the Security Authorization Package to include artifacts and submit the package to the AO for authorization decision.
- **Primary Responsibility:** ISO, ISSO, SCA
- **Output(s):** Security Authorization Package; artifacts include: SSP/SCTM, SAR, POA&M, RAR, and Continuous Monitoring (ConMon) Strategy Plan

Supporting Task 5.3

- **Supporting Task:** Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
- **Primary Responsibility:** AO or DAO
- **Output(s):** Documented and approved Continuous Monitoring (ConMon) Plan/Strategy that includes frequency of monitoring for each control

Supporting Task 5.4

- **Supporting Task:** Determine if risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable
- **Primary Responsibility:** AO
- **Output(s):** Authorization decision document (ATO, DATO, or IATT)

Step 6: Monitor Security Controls

After a system is authorized, it must continue to operate at an acceptable level of risk to maintain its authorization. Ongoing monitoring requires RMF implementers to assess control effectiveness, document changes to the system or its environment of operation and conduct an impact analysis of those changes, and report the security state of the system to designated organizational officials.

Step 6 Primary Roles:

- Information System Owner (ISO)
- Security Control Assessor (SCA)
- Information System Security Manager (ISSM)/ Information System Security Officer (ISSO)

There are seven supporting tasks in step 6.

Supporting Task 6.1

- **Supporting Task:** Determine the security impact of proposed or actual changes to the IS and its environment of operation
- **Primary Responsibility:** ISO or CCP; ISSO/ISSM
- **Output(s):** Change Request

Supporting Task 6.2

- **Supporting Task:** Assess a selected subset of security controls employed within and inherited by the IS in accordance with the organization-defined monitoring strategy
- **Primary Responsibility:** SCA, ISSO/ISSM

- **Output(s):** Periodic Continuous Monitoring Report

Supporting Task 6.3

- **Supporting Task:** Conduct remediation actions based on the results of ongoing monitoring activities, assessment or risk, and outstanding items in the POA&M
- **Primary Responsibility:** ISO or CCP, ISSM/ISSO
- **Output(s):** Documented evidence of correction such as scan results, registry "dumps," etc.

Supporting Task 6.4

- **Supporting Task:** Update SSP, SAR, and POA&M based on the results of the continuous monitoring process
- **Primary Responsibility:** ISO or CCP
- **Output(s):** SSP, SAR, RAR, and POA&M

Supporting Task 6.5

- **Supporting Task:** Report the security status of the IS (including the effectiveness of security controls employed within and inherited by the IS) to the AO and other appropriate organizational officials on an ongoing basis, in accordance with the continuous monitoring strategy
- **Primary Responsibility:** ISO or CCP
- **Output(s):** Periodic Continuous Monitoring Report

Supporting Task 6.6

- **Supporting Task:** Review the reported security status of the IS (including the effectiveness of security controls employed within and inherited by the IS) on an ongoing basis in accordance with the continuous monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable
- **Primary Responsibility:** AO
- **Output(s):** ATO

Supporting Task 6.7

- **Supporting Task:** Implement an IS Decommissioning Strategy, when needed, which executes required actions when a system is removed from service
- **Primary Responsibility:** ISO
- **Output(s):** Updated tracking, management, and inventory system. The AO shall formally decommission the IS by issuing a Decommission letter.

Conclusion

Congratulations! You have completed the Introduction to the RMF for SAPs Short.

You should now be aware of: the importance of the RMF in protecting information systems and networks; impact level ratings for confidentiality, integrity, and availability of information stored on information systems; key roles in SAP cybersecurity; and the steps of the RMF process.

For more detailed information, refer to the attached Introduction to the RMF for SAPs Job Aid.

Review Activity

Determine the order of the steps in the RMF process.
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

What is the **first** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

What is the **second** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

What is the **third** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

What is the **fourth** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

What is the **fifth** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

What is the **sixth** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

Appendix A: Answer Key

Review Activity

Determine the order of the steps in the RMF process.

What is the **first** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ⦿ Categorize System (correct response)
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

***Feedback**: During the first step, RMF decision authorities categorize the IS to determine which security controls must be implemented.*

What is the **second** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ⦿ Select Security Controls (correct response)
- ○ Assess Security Controls

***Feedback**: During the second step, RMF implementers select and tailor an initial set of baseline security controls.*

What is the **third** step in the RMF process?

- ⦿ Implement Security Controls (correct response)
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

***Feedback**: During the third step, RMF implementers implement the security controls and describe how they are employed within the IS.*

What is the **fourth** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ⦿ Assess Security Controls (correct response)

***Feedback**: During the fourth step, the RMF implementers assess the security controls to determine whether they are implemented correctly, operate as intended, and produce the desired outcome.*

What is the **fifth** step in the RMF process?

- ○ Implement Security Controls
- ○ Monitor Security Controls
- ○ Categorize System
- ⦿ Authorize System (correct response)
- ○ Select Security Controls
- ○ Assess Security Controls

***Feedback**: During the fifth step, RMF implementers submit the Security Authorization Package, which documents the organization's risk, and decision authorities decide whether or not to authorize the system..*

What is the **sixth** step in the RMF process?

- ○ Implement Security Controls
- ⦿ Monitor Security Controls (correct response)
- ○ Categorize System
- ○ Authorize System
- ○ Select Security Controls
- ○ Assess Security Controls

***Feedback**: Provided the RMF decision authorities granted ATO, in the sixth step the IS undergoes continuous monitoring to ensure the controls remain effective and that the impacts of any changes are assessed*