Job Aid: Introduction to the RMF for Special Access Programs (SAPs)

Contents

Terminology

This section covers:

- *General Terminology*
- *Documents and Deliverables*
- *Changes and Updates in Terminology*

General Terminology

Authentication: The process of verifying a user's identity or verifying the source and integrity of the data. Examples: something you have to identify who you are (e.g., token, CAC).

Common Controls: Inheritable security controls. Example: physical/environmental security or network boundary controls that would likely be provided at a host data center/common control provider.

Non-repudiation: Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. You are establishing the "proof concept" via a method of something you know (e.g., PIN, digital signature).

Risk Assessment: Identifies risks and assesses residual risk level for the system.

System Development Life Cycle (SDLC): Federal information systems, including operational systems, those under development, and systems undergoing modification or upgrade, are in some phase of a SDLC. National Institute of Standards and Technology (NIST) identifies five phases of a general SDLC:

- Initiation
- Acquisition/Development
- Implementation/Assessment
- Operations/Maintenance
- Disposition/Sunset

Documents and Deliverables

Continuous Monitoring (ConMon) Plan/Strategy: Maintains a current security status for the Information System.

Information Assurance Standard Operating Procedures (IA SOP): Provides guidance for the management, use, protection, dissemination, and transmission of program data as it relates to an information system within a Special Access Program Facility (SAPF).

Plan of Action & Milestones (POA&M): Outlines the measures planned to identify weaknesses or deficiencies and mitigate actions. Defines the resources and timelines for corrective actions to reduce or eliminate known vulnerabilities.

Security Assessment Report (SAR): Contains security control assessment results and recommended corrective actions for control of weaknesses or deficiencies.

System Security Plan (SSP): Best practices in systems and security engineering. Documents the segmentation of the information system in the SSP. Overview of security requirements, description of agreed upon controls, & other supporting security-related documents.

Changes in Terminology

The old terminology is previously associated with the information assurance process formerly referred to as certification and accreditation. This new terminology is adopted under the Risk Management Framework (RMF).

Key Concepts:

Old Terminology	*New Terminology*
Accreditation	Authorization
Certification	Assessment or Security Control Assessment
Certification and Accreditation (C&A) Process	Risk Management Framework (RMF)
Certification Test and Evaluation (CT&E)/Security Test and Evaluation (ST&E) Report	Security Assessment Report (SAR)
Government Contracting Authority (GCA), Customer, etc.	Information System Owner (ISO)
Guest Systems	External Information System
Interim Approval to Operate (IATO)	Authorization to Operate (ATO) with a Plan of Actions and Milestones (POA&M)
Level of Concern	Impact Level
Master SSP (MSSP)	Information Assurance Standard Operating Procedures (IA SOP)
Protection Levels (PL) • PL1/PL2 • PL3/PL4/PL5	Accessibility • Baseline • Baseline + Appropriate Overlay (e.g., Cross Domain Solution (CDS) Overlay)
Requirements	Controls
Security Requirements Traceability Matrix (SRTM)	Security Controls Traceability Matrix (SCTM)
System Security Authorization Agreement (SSAA) / System Security Plan (SSP)	System Security Plan (SSP)
	Overlay
	Risk Executive (Function) (REF)
	Common Control Provider (CCP)
	Overlay (e.g., Accessibility, CDS, Standalone)

Roles:

Old Terminology	*New Terminology*
Certifier, Certification Authority, Service Certifying Organization (SCO)	Security Control Assessor (SCA)
Chief Information Assurance Officer (CIAO)	Chief Information Security Officer (CISO)/Senior Information Security Officer (SISO)
Designated Accrediting Authority (DAA)	Authorizing Official (AO)
Information Assurance Manager (IAM)	Information System Security Manager (ISSM)
Information Assurance Officer (IAO)	Information System Security Officer (ISSO)
	Information System Security Engineer (ISSE)/Information Assurance Systems Architect and Engineer (IASAE)
	Authorizing Official (AO)/Delegated AO (DAO)
Program Manager	Information System Owner (ISO) *PM and ISO terms may be used interchangeably.

Cybersecurity for SAPs: Roles

This section covers:

- *Support/Oversight Roles*
- *RMF Decision Authorities*
- *RMF Assessors and Owners*
- *RMF Implementers*

Note: For more detail about these roles refer to the Joint SAP Implementation Guide (JSIG).

Support/Oversight Roles

Program Security Officer (PSO)

- Verifies configuration management policies and procedures for hardware and software on an IS
- With ISSM/ISSO coordination, provides written approval for entry of IS into the SAPF, as appropriate
- Has authority to appoint the ISSM and ISSO
- Reports data spillage incidents to Director of Security and/or Cognizant Authority Special Access Program Coordinating Office (CA SAPCO)
- Authorizes all digital media and the use of such media
- Reviews and approves media sanitization procedures and equipment
- Issues specific guidance regarding TEMPEST requirements

Government SAP Security Officer (GSSO)/Contractor Program Security Officer (CPSO)

- Creates a secure environment for development and execution of a SAP
- With ISSM/ISSO coordination, provides written approval for entry and removal of IS into the SAPF, as appropriate
- Facilitates several control families essential to securing IS
- Reports incidents regarding SAP information spillage to the PSO via secure communications
- Coordinate on the Incident Response Plan
- Develop media sanitization and removal procedures for PSO/AO approval

Common Control Provider (CCP)

- Develops, implements, assesses, and monitors common security controls (i.e., security controls inherited by information systems)
- Documents the organization-identified common controls in a SSP
- Ensures that required assessments of common controls are carried out by qualified assessors
- Documents assessment findings in a SAR
- Produces and maintain a POA&M for all common security controls having weaknesses or deficiencies
- Ensures SSPs, SARs, and POA&Ms for common controls are made available to ISOs inheriting those controls
- Note that the CCP may be an individual, group, or organization

RMF Decision Authorities

Element Head/ (Service/Agency SAPCO) (must be Government)

- Bears ultimate responsibility for mission accomplishment and execution of business functions and all decisions made on his/her behalf
- Responsible for adequately mitigating risks to the organization, individuals, and the Nation
- Designates an authorizing official to make authorization decisions on behalf of the Element Head

Authorizing Official (AO)
(Designated in writing by Service/Agency SAPCO; must be Government)

- Has a broad and strategic understanding of the SAP Community, his/her organization, and its place/role in the overall SAP community
- Accountable to the Element Head for system authorization and associated risk management decision
- Senior official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk

Delegated Authorizing Official (DAO)
(Appointed in writing by Service/Agency AO; must be Government)

- Acts on behalf of the authorizing official
- Carries out and coordinates the required activities associated with security authorization
- Cannot authorize high impact level systems

RMF Assessors and Owners

Security Control Assessor (SCA) (Appointed in writing by Service/Agency AO)

- Designated by AO
- Acts on his or her behalf to conduct security assessment
- Responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IS to determine the overall effectiveness of the controls
- Responsible for determining the degree to which it meets its security requirements

Information Owner/Steward (STWD) (Service/Agency SAPCO; must be Government)

- Has statutory or operational authority for specified information and responsibility for establishing controls for its generation, classification, collection, processing, dissemination, and disposal
- Typically, in the case of Stewards of classified information, this role is also the appointed Original Classification Authority (OCA) for that particular information
- Development and maintenance of security plan in accordance with security controls
- Appoints the ISSM/ISSO

RMF Implementers

Information System Owner (ISO) (Government or Contract PM)

- Responsible for overall procurement, development, integration, modification, or operation, maintenance, and disposal of an IS
- Responsible for the development and maintenance of the System Security Plan (SSP) and every other document required for security ATO.
- Ensures that the system is deployed and operated in accordance with the agreed-upon security controls
- Appoints the program ISSM/ISSO and ISSE (may be the same person)

Information System Security Manager (ISSM)/Information System Security Officer (ISSO)

- Principal advisor on all matters, technical and otherwise, involving the security of information systems under his/her purview
- Responsible for the day-to-day security posture and continuous monitoring for a SAP IS
- Responsible for the overall information assurance of a program, organization, system, or enclave
- Responsibilities also include physical and environmental protection, personnel security, incident handling, and security training and awareness
- May be identified and appointed in writing to fulfill the role of ISSE
- ISSM responsibilities should not be assigned as collateral duties

Information System Security Engineer (ISSE)

- An individual or group responsible for conducting information system security engineering activities
- An integral part of the development team designing and developing organizational information systems or upgrading legacy systems
- Ensures the information system is designed, developed, and implemented with required security features and safeguards
- Appointed in writing by the ISO

RMF: Supporting Tasks

This section details the supporting tasks for each step of the RMF Process:

- *Step 1: Categorize System*
- *Step 2: Select Security Controls*
- *Step 3: Implement Security Controls*
- *Step 4: Assess Security Controls*
- *Step 5: Authorize System*
- *Step 6: Monitor Security Controls*

Step 1: Categorize System

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

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 commoncontrols 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

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

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

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

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.