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).

C-I-A: The security objectives of Confidentiality, Integrity, and Availability.

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.

IS: Information System

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 SLDC.

- 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 (PM)	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 aSSP
- 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 or Oversight Authority / (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; 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) and Authorizing Official Designated Representative (AODR)

- 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) / IS Architect or Information Assurance Systems Architect and Engineer (IASAE)

- 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:

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

Prepare Step

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

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

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

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

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

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

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