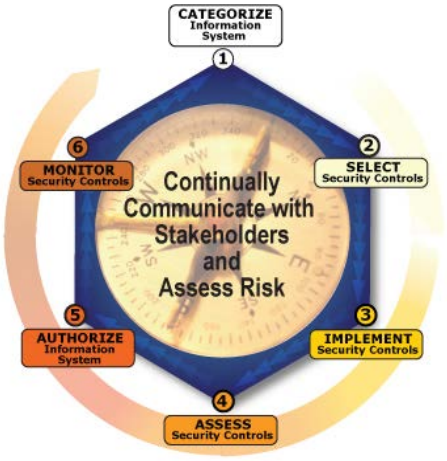
DOD SPECIAL ACCESS PROGRAM (SAP) PROGRAM MANAGER'S (PM) HANDBOOK TO THE JOINT SPECIAL ACCESS PROGRAM (SAP) IMPLEMENTATION GUIDE (JSIG) AND THE RISK MANAGEMENT FRAMEWORK (RMF)



AUGUST 11, 2015

PREPARED BY:

DOD JOINT SAP CYBERSECURITY (JSCS) WORKING GROUP

EXECUTIVE SUMMARY

This *DoD Special Access Program (SAP) Program Manager's (PM) Handbook to the Joint Special Access Program (SAP) Implementation Guide (JSIG) and the Risk Management Framework (RMF)* serves as a guide for Program Managers (PM), Program Directors (PD), Information System Owners (ISO), and Commanders[1] who are responsible for achieving an Authorization to Operate (ATO) for an Information System (IS) within the DoD SAP Community. Obtaining an ATO is required under the Federal Information Security Management Act (FISMA) of 2002 and regulated by Federal Government and DoD SAP Community guidance that specifies the minimum security requirements necessary to protect Information Technology (IT) assets. Identifying security controls at the beginning of the System Development Life Cycle (SDLC) and integrating throughout the SDLC optimizes efficiency and cost-effectiveness. Through this new approach, PM/ISOs may avoid surprises during the security assessment process and help to ensure timely achievement of ATOs. By following DoD Manual (DoDM) 5205.07 SAP Security Manual, JSIG, and the RMF methodology, the DoD SAP Community will implement technologically-sound systems with the necessary capabilities to defend against threats, protect IT and information assets, and achieve its vital, national-security missions.

 Text boxes are provided throughout this document to emphasize key points important to the role of Information System Owner (ISO) under RMF.

The Joint SAP Cybersecurity Working Group (JSCS WG) is co-chaired by Jeffrey Spinnanger/OSD and Robert Nitzenberger/Navy CSD. The purpose of the JSCS WG is to provide organizations within the DoD SAP Community a forum to address all aspects of cybersecurity. JSCS WG functions and activities related to RMF include:

- Promote DoD SAP Community coordination in methodologies for assessing and authorizing SAP information systems and related areas (e.g., documentation, tools, assessment methods, processes, etc.) to provide for consistency in methodologies, approaches, templates, and organization-defined values across the DoD SAP Community
- Develop, maintain, and periodically update the policies and procedures related to RMF to include, as needed, JSIG, RMF training, templates, and other supporting documentation
- Promote, review, and update training and awareness objectives, material, and availability for all service, agency, and industry partners on cybersecurity, emphasizing insider threat, community best practices, and RMF

Current organizations and primary POCs represented in the JSCS WG:

- AF – Michael Christmas; Amir Guy
- Army – Dr. Julie Mehan; Ruben Rios
- CSSWG/Industry – Matthew Lang; Doug Walls
- DARPA – Marshall Hawkins; Lisa Smith

[1] The term Program Manager/Information System Owner (PM/ISO) will be used throughout this document to include Program Managers (PM), Program Directors (PD), Information System Owners (ISO), and Commanders. The ISO role is described in Section 3.1.11.

- DSS – Jonathan Cofer
- MDA – Shelly Briggs
- Navy – Tom Kraft
- OSD – Jon Henderson
- SOCOM – Stephen Smith

Questions, comments, and feedback on documents related to the JSCS WG should be vetted through your working group representative. Contact Windy Benigno, JSCS WG facilitator, at 402-315-0815 if you need your representative's contact information. Jeffrey Spinnanger and Robert Nitzenberger are also available to address any questions or comments: Jeffrey.p.spinnanger.civ@mail.mil; robert.nitzenberger@navy.mil.

Approval:

Jeff Spinnanger
Chief of Security
DoD Special Access Programs Central Office

Robert Nitzenberger
Director, Cybersecurity Directorate (CSD)
DoNSAP DAA/AO

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

In December 2013, the DoD Special Access Program Central Office (SAPCO) issued a mandate requiring the DoD Special Access Program (SAP) Community to transition to the Risk Management Framework (RMF) and to use the Joint SAP Implementation Guide (JSIG), which provides essential guidance to implementing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls within the DoD SAP Community effective January 2014. Further, the DoDM 5205.07, *SAP Security Manual*, Volume 1, *General Procedures (DRAFT)*, provides policy, guidance, and standards for the application of RMF for the authorization of information systems (IS) within DoD SAPs and institutes the use of the JSIG as the replacement for the Joint Air Force – Army – Navy (JAFAN) 6/3 Manual, *Protecting Special Access Program Information within Information Systems.* The DoD and the Intelligence Community (IC) have adopted common guidelines to streamline and build reciprocity into the assessment and authorization (formerly certification and accreditation (C&A)) process under the RMF methodology.

This *DoD SAP PM Handbook* provides a high-level summary of the RMF[2] and JSIG for program managers as well as other individuals involved in the RMF process.

 A Program Manager with a budget line for an information system is an Information System Owner (ISO) under RMF. ISO responsibilities are included in this Handbook.

One of the principal goals of the transformation initiative was to consider the entire mission and apply a balanced risk management process to reach an authorization decision. Information assurance through implementation of the RMF provides organizations with a disciplined, structured, flexible, and repeatable process for managing risk related to the operation and use of information systems.

To further facilitate information sharing within the Federal Government, DoD, and the IC; the Committee on National Security Systems (CNSS) established standards applicable to DoD and the IC for information system security categorization, security controls selection and organization-defined parameter values, and security controls assessment and monitoring for consistency and reciprocity. The DoD SAP Community is ensuring that its policies and procedures comply with the CNSS standards (e.g., CNSS Instruction (CNSSI) 1253) allowing the DoD SAP Community to align with the IC's approach to support reciprocity.

The RMF process addresses risk holistically and emphasizes the development and use of common standards and processes. The Program Manager/Information System Owner (PM/ISO0 must now address security and risk earlier in the System Development Life Cycle (SDLC), beginning during concept development and continuing throughout the entire life cycle from Initiation through Disposal.

[2] The RMF is described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. February 2010.

 Identifying security controls at the beginning and integrating them throughout the entire SDLC is more efficient and cost-effective than addressing security controls at the end of the SDLC.

This PM Handbook will explain the steps required to integrate security requirements throughout the SDLC and identify the key steps required for a system to obtain an Authorization to Operate (ATO). Preparing for and obtaining an ATO is required before deployment and operation of an IS. This Handbook will explain what to expect. Early up-front planning and integration of functional and security specifications, cost, schedule, resources, skill sets, and deliverables help PM/ISOs proactively manage their programs and minimize the unexpected cost of tacking on security requirements late in the SDLC.

 Think Program Objective Memorandum (POM), budgeting for the right information assurance (IA) equipment, personnel with the requisite skill set (e.g., information system security engineer (ISSE), network administrators, etc.), hardware, software, training; incorporating security controls with functional requirements during a system build, starting at system concept; and scheduling realistic timelines to include security assessments and to correct findings. IA has always been a part of owning an IS, RMF provides the framework to clearly identify and address the risk. This will likely require an increased IA budget, plan accordingly.

Security risk management is an essential management function for protecting a DoD SAP element's ability to perform its mission, not just protect its information assets. Policy and legislation mandate specific minimum security requirements to protect mission, information, and IT assets. Unique mission and technology requirements may drive additional security requirements. Computer systems and networks are constantly under attack – putting missions at risk. Within the DoD SAP Community, balancing security of an IS with the need to accomplish the mission is a critical task. The goal of this transformative effort is to achieve greater interoperability and trust across the DoD SAP Community and with the IC.

1.1 PURPOSE AND SCOPE

The purpose of this PM Handbook is to explain the RMF steps required to integrate security requirements throughout the SDLC and identify the key steps required for a system to obtain and maintain an ATO. This Handbook is intended primarily for IS PMs. It provides the following information about JSIG and the RMF:

- High-level process overview
- The relationship between SDLC and the RMF
- Roles and responsibilities
- Information on the steps in the RMF process
- Key deliverables

1.2 CHANGES IN TERMINOLOGY

Table 1 provides a mapping between terminologies previously associated with information assurance (IA) activities related to security certification and accreditation and new terminology adopted under RMF.

Table 1: Changes in Terminology

Old Term	New Term
Certification and Accreditation (C&A) Process	Risk Management Framework (RMF) Process
Certification	Assessment or Security Control Assessment
Accreditation	Authorization
Requirements	Controls
Protection Level (PL) - PL1/PL2 - PL3 - PL4/PL5	Accessibility (met through the following control selections) - Baseline - Baseline + Accessibility Overlay - Baseline + CDS Overlay
Level of Concern	Impact Level
Security Requirements Traceability Matrix (SRTM)	Security Controls Traceability Matrix (SCTM)
System Security Authorization Agreement (SSAA) / System Security Plan (SSP)	System Security Plan (SSP)
Certification Test and Evaluation (CT&E)/ Security Test and Evaluation (ST&E) Report	Security Assessment Report (SAR)
Designated Accrediting Authority (DAA)	Authorizing Official (AO)
Chief Information Assurance Officer (CIAO)	Chief Information Security Officer (CISO)/ Senior Information Security Officer (SISO)
Certifier, Certification Authority, Service Certifying Organization (SCO), Information System Security Professional (ISSP)	Security Control Assessor (SCA)
DAA Representative	Varies depending on service/ agency implementation, e.g. certifier
No equivalent	Delegated Authorizing Official (DAO)
No equivalent	Risk Executive (function) (REf)
No equivalent	Common Control Provider (CCP)
No equivalent	Overlay (e.g. Accessibility, Cross Domain Solution (CDS), Privacy, Standalone, etc.)
Information Assurance Manager (IAM)	Information System Security Manager (ISSM)
Information Assurance Officer (IAO)	Information System Security Officer (ISSO)
Program Manager/Program Director/Commander	Information System Owner (ISO)*

Old Term	New Term
Information System Security Engineer (ISSE)	ISSE/Information Assurance Systems Architect and Engineer (IASAE)
Master SSP (MSSP)	Information Assurance Standard Operating Procedures (IA SOP)
Guest System	External Information System
*PM and ISO terms may be used interchangeably.	

The ISO is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The ISO is responsible for all aspects of taking an information system from concept through authorization to operate (ATO) and the continuous monitoring requirements that follow through system end-of-life. Success hinges on understanding the changing risk associated with your system and a sound working relationship with the Authorizing Official (AO) and Security Control Assessor (SCA), as well as appointing an ISSM, ISSO, and potentially ISSE, with the right skill set to build/manage/monitor your system.

1.3 HANDBOOK MAINTENANCE

The DoD Joint SAP Cybersecurity (JSCS) Working Group (WG) will review and evaluate this PM Handbook annually and update as appropriate.

2 RMF OVERVIEW

In 2007, the IC Chief Information Officer (CIO), the DoD CIO, CNSS, and NIST formed the Joint Task Force (JTF) Transformation Initiative Working Group. This interagency working group's effort was designed to produce a holistic, common process for security risk management, as documented in NIST Special Publications (SP).

Some of the key changes highlighted in these publications include:

- The traditional compliance-focused C&A model, with periodic reaccreditations, has been replaced with a risk management approach with continuous monitoring of security controls and periodic reauthorization.
- The RMF (including monitoring) has been adopted across the IC, DoD, and Federal Government civilian agencies.
- All Federal Government agencies use common security controls derived from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (Revision 3) or its follow-on, *Security and Privacy Controls for Federal Information Systems and Organizations* (Revision 4).
- The IC, DoD, and the DoD SAP Community use additional security-control guidance from CNSSI 1253, *Security Categorization and Control Selection for National Security Systems.*

NIST SP 800-53 and CNSSI 1253 are further augmented by the JSIG, which designates which NIST or CNSS publications shall be used by the DoD SAP Community. The JSIG also provides DoD SAP-specific values, identified as 'organization-defined parameter values' by NIST, for security controls, as appropriate to define at the DoD SAP Community level. Organization-defined parameter values not identified at the DoD SAP Community level, will need to be defined at the organization or system level.

The following documents have a key role in the assessment and authorization of SAP information systems:

- DODM 5205.07 SAP Security Manual :
  - Volume 1 (V1) *General Procedures, Draft,* Reference Enclosure 6, *Cyber Security*
  - Volume 2 (V2) *Personnel Security, Draft*
  - Volume 3 (V3) *Physical Security, Draft*
  - Volume 4 (V4) *Marking, October 10, 2013*
- NIST Publications:
  - NIST SP 800-53, Revision 3[3], *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*

[3] NIST SP 800-53, Revision 4, and CNSSI 1253, dated March 2014, have been issued; but as of the publication of this PM Handbook, the JSIG has not been updated to reflect NIST SP 800-53 Rev4 changes.

  - NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
  - NIST SP 800-30, *Guide for Conducting Risk Assessments*
- CNSSI 1253, *Security Categorization and Control Selection for National Security Systems,* March 2012
- Joint SAP Implementation Guide (JSIG), October 9, 2013 for NIST SP 800-53, Revision 3

Additional NIST publications provide guidance on various aspects of cybersecurity and the RMF methodology including, but not limited to:

- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*
- NIST SP 800-60 Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-60 Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal information Systems and Organizations*
- NISTIR 7298, Glossary of Key Information Security Terms

In the near future, the DoD SAP Community will transition from implementing security controls based on NIST SP 800-53 Revision 3 to implementing controls in Revision 4. Ensure your personnel and individuals you interact with during joint authorization and reciprocity use documents that map to each other. **Do not transition to NIST SP 800-53 Rev4 until authorized by the AO.** Documents align as follows:

NIST SP 800-53 Rev3	NIST SP 800-53 Rev4
CNSSI 1253, March 2012	CNSSI 1253, March 2014
JSIG, October 9, 2013	JSIG, TBD 2015
JSIG, October 9, 2013 Errata Sheet, March 2, 2015	

The diagram in Figure 1[4] below illustrates the six steps of the RMF as applied in the DoD SAP process for information system security and risk management, also known as the assessment and authorization process. Information system security is defined as the secure design, implementation, configuration, operation, and continuous monitoring of security controls. System security also depends on ongoing risk management, which requires active situational awareness of external and internal threats and attacks, as well as a process for identifying issues, assessing impact, and taking action.

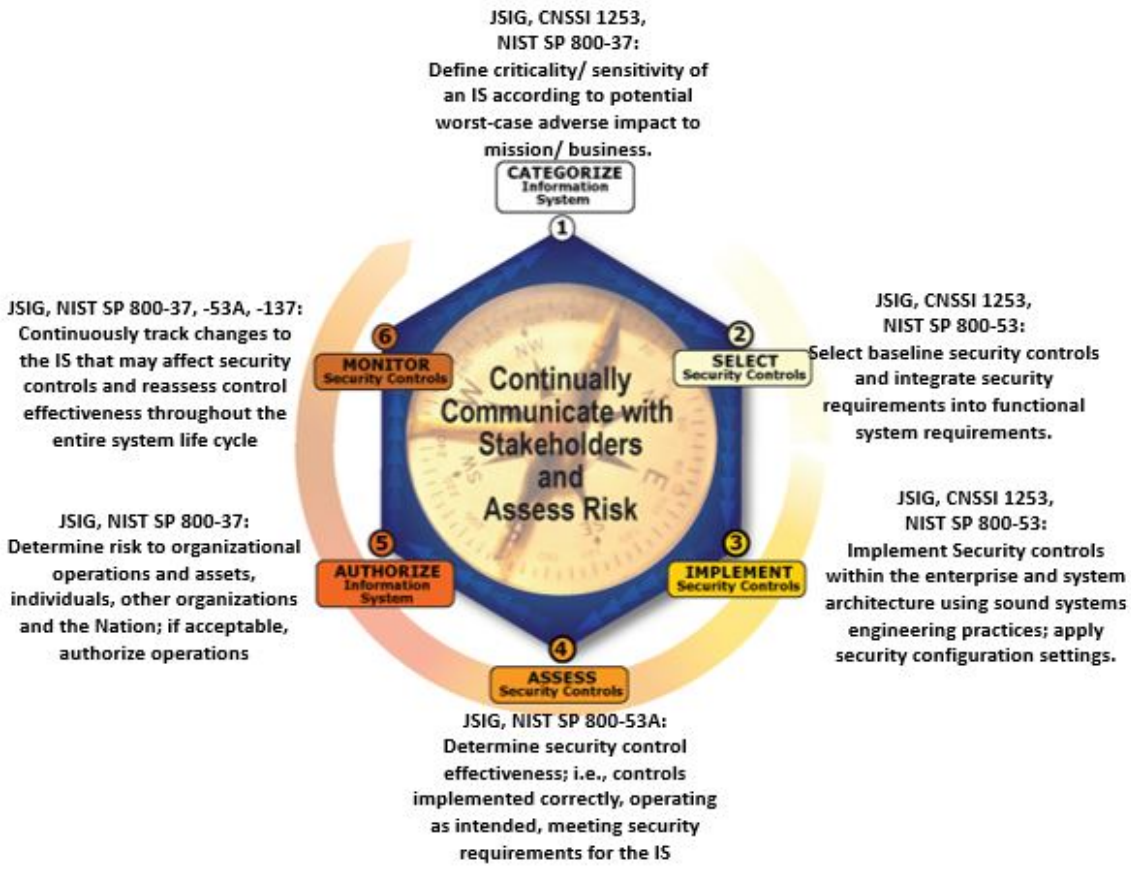


Figure 1: The Six Steps of the RMF

[4] Note: Figure 1 maps the RMF Steps to publications that provide additional details about each phase of the process.

3 RMF PROCESS

This section describes the RMF's six (6) Steps and the security authorization artifacts (section 3.2.5.1), which the Authorizing Official (AO)[5] uses to make an informed risk–based decision whether to grant an ATO for an IS.

NIST SP 800-37 is designed to provide consistent guidelines for applying the RMF to Federal[6] IT systems. The 6 steps of the RMF process are:

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

The output of the RMF process includes an understanding of the risk associated with the system and the security authorization artifacts, also known as the Body of Evidence (BoE), submitted as part of the Security Authorization Package for the IS. The AO will use the Security Authorization Package to determine whether deployment of the IS presents or continues to present an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Security artifacts include, but are not limited to: System Security Plan (SSP), Risk Assessment Report (RAR), Information Security Continuous Monitoring (ISCM) Plan (commonly referred to as the Continuous Monitoring (ConMon) Plan), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M). Additional information on the security authorization artifacts is given in Section 3.5.

Although the PM/ISO will likely delegate the development and update of documents in the Security Authorization Package, the PM/ISO will sign off on the Security Authorization Package before forwarding it to the SCA/AO, indicating that the documentation accurately reflects the configuration and security state of the information system and the environment in which it operates.

[5] Previously referred to as the "Designated Accrediting Authority (DAA)."

[6] The term 'Federal IT systems' includes all Federal civilian agencies, DoD and the IC.

The RMF emphasizes the need to consider security throughout the system life cycle. As illustrated in Figure 2 below, the RMF, the SDLC, and Acquisition processes are closely aligned.

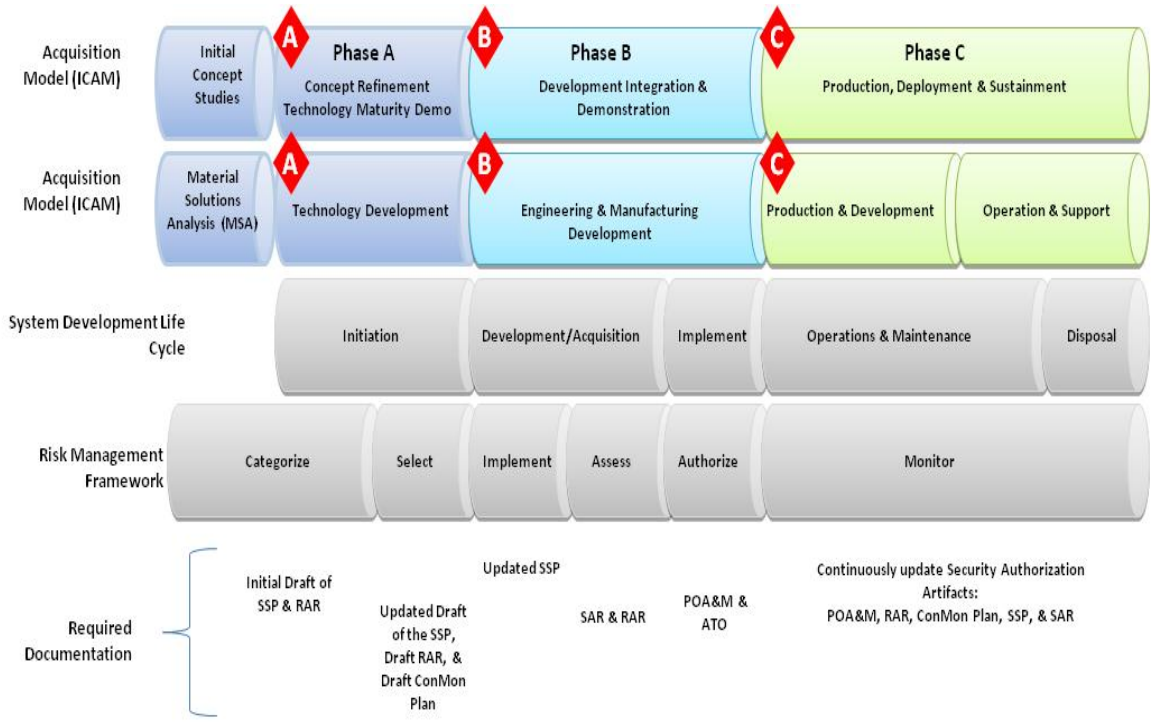


Figure 2: DoD Acquisition, SDLC and RMF Processes

3.1 Roles and Responsibilities for the RMF Process

For a PM/ISO to successfully navigate an IS through the risk management process and obtain an ATO, the following participants/stakeholders are critical. In addition to the traditional design and development team, resources may include participants/stakeholders described in the following subsections. Roles and responsibilities are also defined in DoDM 5205.07 and the JSIG. As indicated in the JSIG, not all roles are required for all systems, e.g. there may not be a Chief Information Security Officer (CISO), Delegated AO (DAO), or Information System Security Engineer (ISSE) and some roles may collapse with AO approval.

Primary and supporting roles for each step in the RMF are depicted in Figure 3. In some situations a role may float from supporting to primary or vice versa depending on the system, environment, and

mission, e.g. not all systems will have an ISSE assigned. Roles and responsibilities are further defined in the remainder of this section.

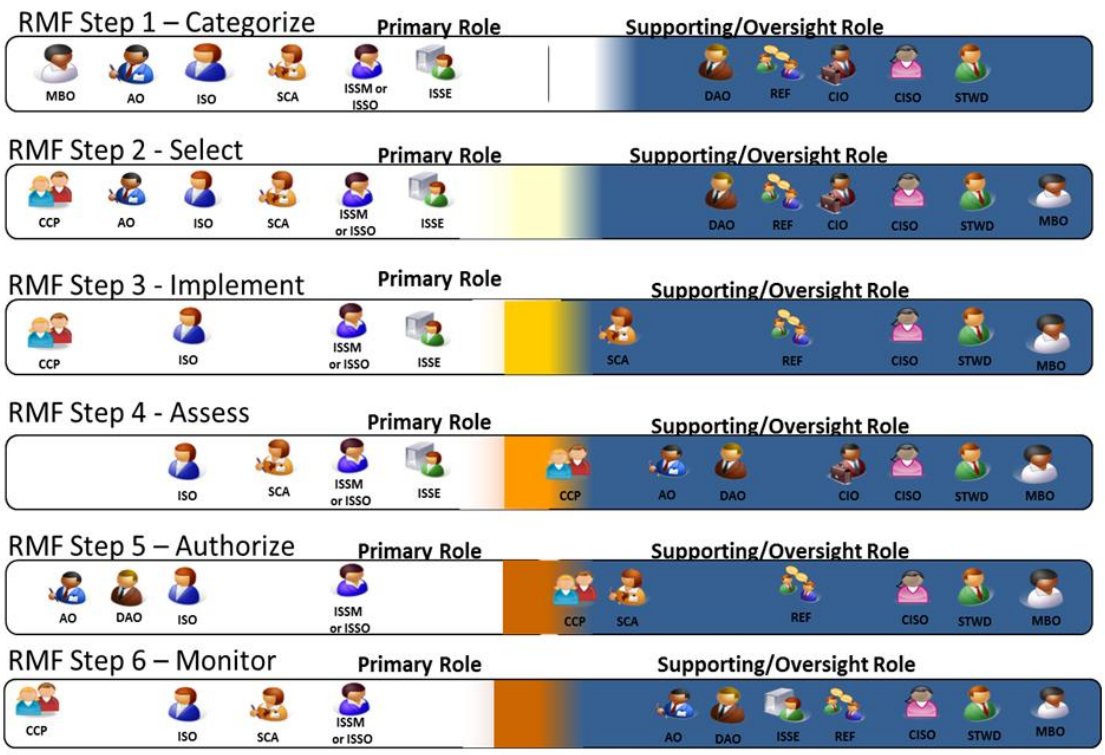


Figure 3: RMF Primary and Supporting Roles

3.1.1 AGENCY/ELEMENT HEAD (GOVERNMENT)

Each DoD SAP Element Head bears ultimate responsibility for mission accomplishment and execution of business functions, and hence for adequately mitigating risks to the element, its individuals, and the Nation. The Element Head defines priorities to ensure collaboration and information-sharing sufficient to ensure both element and DoD SAP Community-wide mission accomplishment As stated in NIST SP 800-37, the Element Heads are responsible for ensuring that: (i) information security management processes are integrated with strategic and operational planning processes; (ii) senior officials within the organization provide information security for the information and information systems that support the operations and assets under their control; and (iii) the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines.

3.1.2 RISK EXECUTIVE (FUNCTION) GOVERNMENT

The Risk Executive function (REf) may be fulfilled by an individual, a group, or an assigned function within an organization. The REf directly supports the Authorizing Official (AO) and ensures: (i) that risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective (with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions) and (ii) that

managing information-system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.

3.1.3 CHIEF INFORMATION OFFICER (CIO) (GOVERNMENT)

The CIO[7], along with the Element Head and other senior officials, ensures that information systems are acquired and information resources are managed in a manner consistent with laws, Executive Orders, directives, policies, regulations, as well as priorities established by the Element Head. The CIO develops, maintains, and ensures the implementation of sound, secure, integrated, IS architectures and promotes the effective, efficient design, development, and operations of all major information and resource management processes.

3.1.4 CHIEF INFORMATION SECURITY OFFICER (CISO)/SENIOR INFORMATION SECURITY OFFICER (SISO)

A CISO or SISO executes the CIO's responsibilities under the Federal Information Security Management Act (FISMA) of 2002 and serves as the CIO's liaison to the DoD SAP organization's AOs, ISO, Common Control Providers (CCP), and Information System Security Officers/Managers (ISSO/ISSM).

3.1.5 AUTHORIZING OFFICIAL (AO) (GOVERNMENT)

An AO is a senior official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security. Across the Federal Community, AOs may have budgetary oversight for an IS or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, AOs are accountable for the security risks associated with information system operations. Accordingly, AOs are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks.

An AO may appoint one or more Delegated Authorizing Officials (DAO) in writing to expedite authorizations of designated systems, and provide mission support.


Within the DoD SAP Community, the AO determines the acceptable level of risk associated with a given information system and the collective risk to the organization from information systems operating across the organization. Continued operation of your information system is dependent on the AO's determination that the PM/ISO is maintaining the information system at an acceptable level of risk. The AO takes under advisement observations and concerns from members of the REf including the Director of Security, CIO, CISO, et.al, when making an acceptable risk determination.

[7] Not all DoD SAP organizations include a Chief Information Officer and/or a Chief Information Security Officer/Senior Information Security Officer.

3.1.6 DELEGATED AUTHORIZING OFFICIAL (DAO) (GOVERNMENT)

A DAO is delegated authority by an AO to carry out specific activities for specific systems as identified by the AO (e.g., authorizations to operate).

3.1.7 SECURITY CONTROL ASSESSOR (SCA)

A SCA is an individual appointed in writing by the AO to act on his or her behalf to conduct a security assessment. The SCA is 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 (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). SCAs also provide an assessment of the severity of weaknesses or deficiencies discovered in the IS and its environment of operation and recommend corrective actions to address identified vulnerabilities.

Although the PM/ISO is responsible for all aspects of the information system, from concept to disposal, the ISSM/ISSO role, described below, is responsible for the day-to-day security posture and continuous monitoring of the system and reporting any issues/concerns to the PM/ISO. In addition, the SCA, as described above, is appointed by the AO to assess the system and address issues with the ISSM/ISSO that arise between assessments. The SCA's 'loyalty' is to the AO, but the SCA (or AO) will inform the PM/ISO whether an assessment is satisfactory or not and whether the system is being maintained at an acceptable level of risk. This provides the PM/ISO with daily views of the system (ISSM) and a periodic view (SCA assessment) and assurance they are on target.

3.1.8 COMMON CONTROL PROVIDER (CCP)

A CCP is responsible for the development, implementation, assessment, and monitoring of common controls. Organizations can have multiple CCPs depending upon how information security responsibilities are allocated organization-wide, e.g., a Navy or Air Force CCP; or a site/campus CCP (commonly the ISSM) who establishes implementation, assessment, and monitoring procedures for specific controls across the site/campus.

3.1.9 INFORMATION OWNER/STEWARD (GOVERNMENT)

An Information Owner/Steward is an organization official with statutory, management, or operational authority for specific information and is responsible for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.

The information system owner is responsible for the information system; the information owner is responsible for the data.

3.1.10 Mission/Business Owner (MBO) (Government)

An individual with MBO responsibilities has operational responsibility for the mission or business process supported by the mission/business segment or the information system. The MBO is a key participant/stakeholder regarding system life-cycle decisions.

3.1.11 Information System Owner (ISO)

An ISO is responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of an information system (as well as the system components), to include development and provision of the SSP and every other document required for security ATO. The ISO is responsible for ensuring that the program ISSM and ISSE are identified. As the focal point for the IS, the ISSM and ISSE support the ISO and serve as a central point of contact regarding the authorization process. ***Some organizations may refer to ISOs as PMs/PDs or Commanders.***

With the description of the ISSE and ISSM/ISSO roles below, the PM/ISO should be aware at this point of the many roles under RMF and where each fit into the process of continuously assessing and managing risk. An IS at-risk ripples beyond the system itself, affecting the mission, the organization, and ultimately national security. Stating that risk to your system could ultimately affect national security is not a line. We develop technology in this community and we build widgets. Those products may not be fully functional for several years, but we need to protect that development today.

While you as the PM focus on the mission at hand, keep in mind that an IS is required to support that mission. So you, as the ISO, are in partnership with IA professionals from the AO to the SCA, to the ISSE and ISSM/ISSO, right down to that system administrator. It is imperative that the PM/ISO work side by side with the IA professionals to continually address and mitigate risk. Budget accordingly, POM for the out-years, learn what skill set your IA personnel need, the training they need to maintain and improve their skills, learn to ask the right questions of your ISSM/ISSOs. "What is the risk?" is a great place to start!

It is not a matter of just the risk on just your system; it is the collective risk introduced by every system in the DoD SAP Community. Understanding that collective risk is the responsibility of the AO. Understanding and addressing the risk associate with your system is the responsibility of the PM/ISO.

3.1.12 Information System Security Engineer (ISSE)/Information Assurance Systems Architect and Engineer (IASAE)

An ISSE/IASAE ensures that information-security requirements are effectively implemented throughout the security architecting, design, development, configuration, and implementation processes. The ISSE coordinates his/her security-related activities with ISOs, ISSOs/ISSMs, and CCPs. ***Some organizations also refer to an ISSE as an Information Security Architect.***

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

An ISSM or ISSO is appointed in writing by the ISO and is responsible for maintaining the day-to-day security posture and continuous monitoring of a system. The ISSM or ISSO is responsible for the overall IA of a program, organization, system, or enclave.

As the PM/ISO you likely have reach-back to a contracts person who understands all the nuances of contracting, a PSO who understands the rules and regulations on physical and personnel security; as an ISO you have an ISSM and/or ISSO (along with one or more system administers) who know your system inside and out. Encourage the ISSM/ISSO to keep you informed on the status of the IS and any issues or potential issues they can foresee. You don't have to know all that they know, but understand the concepts related to the IS and any risks that are identified, and their potential impact to the Confidentiality, Integrity, and Availability of your system.

The PM/ISO frequently delegates document development (e.g. SSP, SCTM, RAR, ConMon Plan, Security Assessment Plans, et.al.) to the ISSM/ISSO (or ISSE if your system has one). The responsibility of ensuring the documents are completed, accurately reflecting the system and environment, and in a timely manner to allow for assessment and authorization to operate to meet mission needs, remains with the PM/ISO. Ask questions…of your ISSM/ISSO or ISSE, your SCA, and/or the AO. As the PM/ISO, the IS is your responsibility, but there are a number of IA professionals available to educate and assist you.

3.2 Steps in the RMF Process

The following sections provide an overview of each RMF Step, including its associated SDLC phase(s), roles and responsibilities, tasks, and deliverables. For additional information about the RMF, reference JSIG or NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. A Risk assessment Report (RAR) is addressed in RMF Step 2 (Task 2-2), but is frequently initiated before RMF Step 1 to identify potential risk. Identifying risk up front is helpful in determining impact levels in RMF Step 1.

3.2.1 *RMF STEP 1—Categorize Information System (IS)*

Purpose: Categorize an IS, by first categorizing the information on the system, according to the potential impact of a loss of Confidentiality, Integrity, and Availability (C-I-A).

SDLC Phase: Initiation

In Step 1, information (or information types) and IS are categorized according to the potential impact of a loss of C-I-A. Information and subsequently the IS must be placed in one of three defined categories (Low, Moderate, or High) to determine which security controls must be implemented. This step, known has categorization, is described in JSIG, Section 2.3.1 and CNSSI 1253, Chapter 2.

Figure 4 below provides the definitions for C-I-A.

Figure 4: C-I-A Triad and Definitions

Table 2 below lists supporting tasks, the primary roles associated with each task, and the task deliverables. As defined in NIST SP 800-53, the ISO (aka PM) is the official responsible for the overall procurement, development, integration, modification, and operation and maintenance of an information system. Although certain tasks may be delegated, **you** as the PM or ISO are responsible for all ISO tasks in the RMF.

Table 2: RMF Step 1 - Categorize IS

Supporting Tasks	Primary Responsibility	Deliverable(s)
Task 1-1—Categorize the Information System and document the results in the SSP.	ISO or Information Owner/Steward	Draft SSP with System Categorization filled in
Task 1-2—Describe the information system (including system boundary) and document the description in the SSP.	ISO	Updated SSP to include a description of the IS
Task 1-3—Register the IS with the appropriate organizational program management offices.	ISO	Document or entry in the IT registry with the official system name, system owner, and categorization

3.2.1.1 Determine Potential Impact Levels[8]

[8] The terms 'impact level' and 'impact value' are used interchangeably in RMF discussions. NIST RMF documents were developed based on concepts in FIPS-199, which uses the term impact value, and FIPS-200, which uses the term impact level.

Information is categorized based on three security objectives—Confidentiality, Integrity, and Availability (C-I-A)—and is assigned a potential impact level of Low (L), Moderate (M), or High (H) for information and is based on the potential impact of a security breach on organizations and/or individuals. **For the purposes of the DoD SAP Community, the minimum baseline impact level assigned to a DoD SAP IS has been determined to be Moderate Confidentiality, Low Integrity, and Low Availability (MLL).**

In RMF Step 1, identify the potential impact level (L, M, H) for the three security objectives (i.e., C-I-A) for each identified information type.

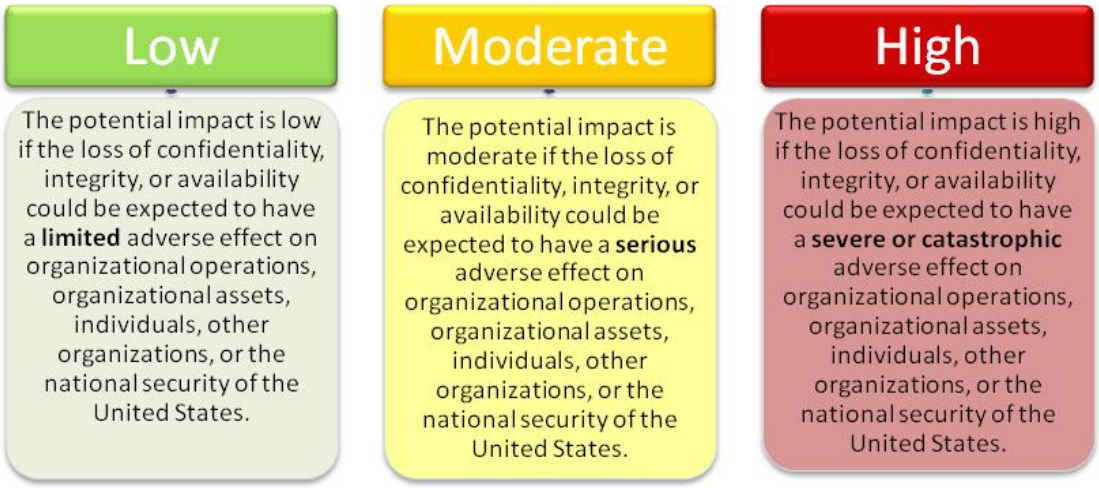


Figure 5: Low-Moderate-High Impact Definitions

Identifying information types, even within program-level data, provides insight into which information types are more critical and therefore require more protection, such as limiting access to fewer users, which may mitigate insider threat to the more critical information.

3.2.1.2 Determine Confidentiality Categorization

The Confidentiality categorization is derived from the potential impact level (as determined by using the guidance given in Figure 5) and additional factors, which are:

- Aggregation of information
- Information system environment
- Attributes of users

The highest potential impact level determined for any of the information types processed, stored or transmitted by the system serves as a point of reference for the Confidentiality value of the information system. However, the additional factors listed above may result in the need for the

information system's Confidentiality value to be lower or higher than the information's Confidentiality value.

All classified National Security Systems (NSS)[9] must be categorized as Moderate or High for Confidentiality.[10] All SAP systems are NSS.

Table 3: Confidentiality Impact Level

Classification	Confidentiality Impact Level	Adjustments to Impact Level
TS//SAR OR S//SAR	Moderate	Adjust to the High Confidentiality Impact Level if: - Any user lacks either the required security clearance or the required citizenship (address with overlay)

Within the DoD SAP Community the nominal Confidentiality impact level for information is as illustrated in Table 3 above. For Integrity and Availability, each information type accessed and processed by the system is considered, and the highest impact level for each of those objectives is selected as the system impact level for that objective as illustrated in Table 4 below.

Table 4: System Integrity and Availability Categorization Example

Information Type	Integrity	Availability
Information Type A	L	L
Information Type B	**H**	**M**
Information Type C	M	**M**
Overall System Categorization per Objective	**H**	**M**

For information systems with information having a Confidentiality level of High, if the below additional factors permit, the information system categorization for Confidentiality may be designated as Moderate.

For information systems with information having a Confidentiality impact level of Moderate, if at least one of the additional factors identified below requires, the information system categorization for Confidentiality may be designated as High.

[9] Systems are categorized as National Security Systems (NSS) as established in FISMA, Title II, Public Law 107-347, December 17, 2002 (Section 3542, Paragraph (2)(A)(ii)), and further described in NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

[10] For classified information and DoD SAP information systems, the Confidentiality categorization impact level must be at least Moderate.

Aggregation of information – If the information system contains information that, when aggregated, increases the risk to the organization, the system's Confidentiality impact level may need to be designated at a level higher than the information Confidentiality impact level.

Information system environment – If the information system is physically located in an environment that is authorized for the processing or open storage of the information processed by the system (e.g., an accredited Special Access Program Facility [SAPF] for SAP information), the system's Confidentiality impact level may be a lower value than the Confidentiality impact level of its information (but not lower than moderate for classified NSS). If the information system is not located in such an environment, the system's Confidentiality impact level may need to be designated at a level higher than the information Confidentiality value.

Attributes of users – If the information system must provide capabilities to mitigate the risk of users having access to classified information for which they lack the required security clearance, or the required citizenship; then the system's Confidentiality impact level should be designated as High[11]. If the information system is not required to mitigate these types of risks, then the system's Confidentiality impact level may be designated at a value of Moderate.

3.2.1.3 Determine Integrity and Availability Categorization

Systems commonly contain information types that may have different potential impacts. In that case, the information type with the highest potential impact for each security objective (Integrity and Availability) defines the value assigned to that security objective. For example, a system might contain administrative data that is assessed to have a Low Availability potential impact level. The same system may also contain mission data that is assessed to have a Moderate Availability potential impact level. In such an instance, the system's Availability impact level would be designated as Moderate because this is the highest Availability potential impact level of information processed by the system. A similar determination is made for the Integrity security objective.

The generalized format for expressing the security category (SC) of a NSS is —

SC NSS = {(Confidentiality, *value*), (Integrity, *value*), (Availability, *value*)}, where the acceptable values are Low, Moderate, or High (except classified NSS where the **only** acceptable values for Confidentiality are Moderate or High).

By the end of RMF Step 1, documents to include the Draft SSP and potentially a Draft RAR.

3.2.2 RMF STEP 2—SELECT SECURITY CONTROLS

Purpose: Select security controls using appropriate baseline and overlay(s), then tailor as required to prevent security breaches of an IS.

SDLC Phase: Initiation

Security controls are the safeguards and countermeasures employed within an organizational IS to protect the C-I-A of the system and its information and to properly manage mission, business, and system risks. Security controls are documented in the Security Controls Traceability Matrix (SCTM),

[11] Appropriate security control overlays must also be applied.

which is considered part of the SSP. More information on this step may be found in CNSSI 1253 Chapter 3, JSIG Chapter 2, and NIST SP 800-53. Table 5 below lists supporting tasks, the roles associated with each task, and the task deliverables for Step 2—Select Security Controls.

Table 5: RMF Step 2 - Select Security Controls

Supporting Tasks	Primary Responsibility	Deliverable(s)
Task 2-1—Identify the security controls that are provided by the organization as common controls for organizational IS and document the controls in the SSP.	CCP; ISO, ISSM/ISSO, ISSE, SCA	Document the common controls in the SSP/SCTM
Task 2-2—Select the security controls for the IS (i.e. baseline, overlays, tailored) and document the controls in the SSP.[12]	ISO; ISSE	Document the selected security controls in the SSP/SCTM, Draft RAR
Task 2-3—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.	ISO or CCP	Documented and approved Continuous Monitoring (ConMon) Plan/Strategy including frequency of monitoring for each control
Task 2-4—Review and approve the draft SSP by the AO or DAO.	AO or DAO; ISSM/ISSO	Documented and approved Draft SSP/SCTM

Although Table 5 reflects the Step 2 tasks as outlined by NIST, in reality Task 2-1 is not always completed first and as explained in CNSSI 1253, Task 2-2 becomes a four-step process:

Step 1: Select the initial baseline set of security controls specifying type: common, system-specific, or hybrid.

Step 2: Select and apply security control overlays.

Step 3: Tailor (in or out) the set of security controls.

Step 4: Supplement the tailored set of security controls.

The Security Control Traceability Matrix (SCTM) is part of the SSP, usually as an attachment or appendix. The SCTM lists all of the controls selected for the system as well as additional details on each control, e.g. implementation status, monitoring frequency, etc.

3.2.2.1 Selecting the Initial Set of Security Controls

Selecting the initial control set, or baseline, is the process of grouping the appropriate column of controls corresponding to the security categorization of the system as identified in RMF Step 1 (e.g.,

[12] Security Controls are selected based on a formal or informal risk assessment.

Moderate, Low, Low (MLL)). Baseline controls are identified in the JSIG as derived from CNSSI 1253, Appendix D. CNSS identified the initial control sets to capture the needs of the majority of NSS with the intent of minimizing the efforts required for tailoring control selections. Table 6 provides an excerpt from CNSSI 1253, Appendix D Security Control Baselines.

An 'X' in the table signifies that the control in that row is allocated to the respective security objective (Confidentiality, Integrity or Availability) and at the value (Low, Moderate or High) specified in the header rows above that column. A blank, e.g., there is neither a letter, + or -, signifies the control is not allocated for that objective or at that impact level. A dash '-' signifies the control was in an earlier revision of NIST SP 800-53, but has been withdrawn[13]. In CNSSI 1253, March 2012, Table D-1 includes an additional column titled 'Suggested Common' to identify controls that are potentially common controls. In the JSIG, October 9, 2013, each 'X' was replaced with 'C,' 'H,' or 'S' to provide tentative designation for the control enforcement:

- 'C' – the security control is likely a Common control, i.e., inherited by the system and enforcement/responsibility is at the CCP level (e.g. organization, ISSM level)
- 'S' – the control is a System Specific control and the responsibility of the PM/ISO and enforced at the system level
- 'H' – indicates a Hybrid control and a portion of the control is Common and a portion is System Specific

Some security controls listed are not allocated to any baseline because even though they represent capabilities that may be required by some organizations under some circumstances, they are not considered necessary for all NSS based on any impact level for Confidentiality, Integrity or Availability. Controls not allocated can be allocated through the application of overlays, or during the tailoring or supplementing steps of the selection process.

Table 6: Security Control Baseline Examples

ID	Title	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy And Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)[14]	Account Management	X	X	X	X	X	X			
AC-2(2)	Account Management		X	X		X	X			

[13] When the DoD SAP Community moves to NIST SP 800-53 Revision 4 and CNSSI 1253 dated March 2014, the chart in Appendix D of CNSSI 1253 changes slightly in that the 'X' indicates it is in the NIST baseline and a '+' reflects it is an additional specification CNSS requires for all NSS for the specified objective (C-I-A) and impact level (L-M-H).

[14] AC-2(1) is read as security control AC-2 enhancement (1). Descriptions of the security controls and enhancements are found in NIST SP-800-53.

ID	Title	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-2(3)	Account Management		X	X		X	X			
AC-2(4)	Account Management	+	X	X	+	X	X			
AC-2(5)	Account Management									
AC-2(6)	Account Management									
AC-2(7)	Account Management	+	+	+	+	+	+			
AC-2(8)	Account Management									
AC-2(9)	Account Management	+	+	+	+	+	+			
AC-2(10)	Account Management	+	+	+	+	+	+			
AC-2(11)	Account Management									
AC-2(12)	Account Management	+	+	X	+	+	X			
AC-2(13)	Account Management	+	+	X	+	+	X			
AC-3	Access Enforcement	X	X	X	X	X	X			
AC-3(1)	Access Enforcement	-	-	-	-	-	-	-	-	-
AC-3(2)	Access Enforcement									
AC-3(3)	Access Enforcement									
AC-3(4)	Access Enforcement	+	+	+	+	+	+			

3.2.2.2 Selecting and Applying Security Control Overlays

Security control overlays are specifications of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI 1253 and to complement the supplemental guidance in NIST SP 800-53. Organizations select and apply security control overlays by using the guidance in each of the standardized CNSS or DoD SAP approved overlays.

Applying one or more required overlays provides a structured form of tailoring (section 3.2.2.3), e.g. based on data, environment, system type, etc., and supplementing (section 3.2.2.4) the initially selected set of security controls. Applying one or more overlays can reduce the need for additional tailoring and supplementing of controls.

If the use of multiple overlays results in conflicts between the application or removal of security controls, the AO (or designee), in coordination with the information owner/steward, will resolve the

conflict. If a control is added or removed by the application of an overlay, the SSP should reflect the change with the justification being the application of the specific overlay(s) directing the change.

Further guidance on overlays is provided in Appendix E of CNSSI 1253 and the JSIG.

3.2.2.3 Tailoring the Set of Security Controls

The AO, REf, and other decision-makers may find it necessary to tailor (modify) a control set. The resultant set of security controls derived from tailoring is referred to as the final (or tailored) control set.

After selecting the initial set of baseline security controls, organizations initiate the tailoring process to modify and align the controls more closely with the specific conditions within the organization. Refer to and use JSIG, Chapter 3 or CNSSI 1253, Chapter 3 for initial guidance on tailoring controls.

Tailoring decisions must be aligned with operational considerations and the environment of the information system. For example, in command and control systems in which lives may be in the balance, adoption of security controls must be balanced against operational necessity. In the case of an air traffic control console, the need to access the console at all times outweighs the security need for screen or session lock capability.

Organizations should remove or "tailor out" security controls only as a function of specified, risk-based determinations. Tailoring decisions, including the specific rationale (i.e., mapping to risk tolerance) for those decisions, are documented in the SSP for the information system.

Every selected control must be accounted for either by the organization or the information system owner. If a selected control is not implemented, then the rationale for not implementing the control must be documented in the SSP.

 When an ISSM/ISSO or ISSE identifies a cost or other impact associated with a specific control, it's worth asking: Can we tailor the control? If we tailor the control, what's the risk?

3.2.2.4 Supplementing the Tailored Set of Security Controls

Supplementation addresses residual risks not adequately mitigated by the tailored control set, but may not eliminate all residual risk. In many cases, additional security controls or control enhancements will be needed to address specific threats to or vulnerabilities in a system or to satisfy the requirements of public laws, Executive Orders, directives, policies, standards, or regulations. Risk assessment at this stage in the security control selection process provides important inputs for determining the sufficiency of the tailored set of security controls. The inclusion of each control is based on the need to reduce risk to an established tolerance level.

The final set of tailored and/or supplemented security controls must be submitted for approval to the respective AO prior to finalizing implementation.

By the end of RMF Step 2, documents include the Draft SSP/SCTM, RAR (updated or initial draft), and a Draft ConMon Plan.

3.2.3 RMF STEP 3—IMPLEMENT SECURITY CONTROLS

Purpose: Security controls are implemented on the information system.

SDLC Phase: Development/Acquisition, Implementation

Implementing these controls consistent with the enterprise architectures, IA architectures, laws, policies, and configuration standards is critical to achieving an acceptable level of risk and an ATO. More information on this step may be found in JSIG, CNSSI 1253, NIST SP 800-37, and NIST SP 800-53A.

Table 7 lists supporting tasks, the roles with primary responsibility for each task, and the task deliverables for Step 3—Implementing Security Controls.

Table 7: RMF Step 3 - Implement Security Controls

Supporting Tasks	Primary Responsibility	Deliverable(s)
Task 3-1—Implement the security controls specified in the SSP.	ISO or CCP	
Task 3-2—Document the security control implementation, as appropriate in the SSP, providing a functional description of the control implementation.	ISO or CCP; ISSM/ISSO; ISSE	Updated SSP with information describing how security controls are implemented.

By the end of RMF Step 3, documents include the SSP with updated SCTM, Draft RAR and Draft ConMon Plan.

3.2.4 RMF STEP 4—ASSESS SECURITY CONTROLS

Purpose: Determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements.

SDLC Phase: Development/Acquisition; Implementation

After security controls are implemented, they must be evaluated. This is when the security control assessment occurs. This step determines the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements. NIST SP 800-53A is often used as guidance for these assessments.

Table 8 lists supporting tasks, the roles associated with each task, and the task deliverables associated for Step 4—Assess Security Controls.

Table 8: RMF Step 4 - Assess Security Controls

Supporting Tasks	Primary Responsibility	Deliverable(s)
Task 4-1—Develop, review, and approve a plan to assess the security controls.	ISSM/ISSO; ISSE; SCA	Security Assessment Plan
Task 4-2—Assess the security controls in accordance with the assessment procedures defined in the Security Assessment Plan.	SCA	Individual test results for each test or matrix for all tests
Task 4-3—Prepare the SAR documenting the issues, findings, and recommendations from the security control assessment.	SCA	Security Assessment Report (SAR)
Task 4-4—Conduct initial remedial actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate.	ISO or CCP; SCA; ISSM/ISSO	Updated Risk Assessment Report (RAR)

The Security Assessment determines the risk to agency operations, agency assets and individuals and, if deemed acceptable by the AO/DAO, the Security Authorization in RMF Step 5 will formalize the SCA's assessment with the AO/DAO's acceptance to authorize operation of the IS.

By the end of RMF Step 4, documents include the SSP/SCTM, RAR, ConMon Plan, and SAR. The AO/SCA may request that the Security Assessment Plan be included in the Security Authorization Package.

3.2.5 RMF STEP 5—AUTHORIZE INFORMATION SYSTEM

Purpose: Identify weaknesses or deficiencies to be corrected and any residual vulnerabilities and submit a security authorization package to the AO (via the SCA) for adjudication. The Security Authorization will formalize the AO's/DAO's acceptance (or not) to authorize operation of the IS. Authorization decisions include: ATO, denied authorization to operate (DATO), or interim authorization to test (IATT).

SDLC Phase: Implementation

Table 9 lists supporting tasks, the roles associated with each task, and the task deliverables for RMF Step 5—Authorize Information System. Task 5-1 addresses preparation of the POA&M. The SCA may initiate the POA&M based on the findings in the SAR, but in reality not all SCAs initiate a POA&M. The PM/ISO is responsible for completing the POA&M fields, updating, and resolving POA&M items.

Table 9: RMF Step 5 - Authorize Information System

Supporting Tasks	Primary Responsibility	Deliverable(s)
Task 5-1—Prepare the POA&M based on the findings and recommendations of the SAR, excluding any remediation actions taken.	SCA (document initial findings); ISO (completes POA&M; adds additional items; includes CCP, if finding is against a common control)	POA&M
Task 5-2—Assemble the Security Authorization Package to include artifacts and submit the package to the AO for adjudication.	ISO; ISSM/ISSO; SCA	Security Authorization Package; artifacts include: SSP/SCTM, SAR, POA&M, RAR, and ConMon Plan.
Task 5-3—Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	AO or DAO	
Task 5-4—Determine if risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.	AO	Authorization decision document (e.g. ATO, DATO, IATT)

Generally, if a Security Authorization Package is submitted with a request for ATO and the package is incomplete or unsatisfactory, the AO will not (normally) issue a DATO; the AO will more likely send the package back to the PM/ISO with instructions on why it was returned.

A DATO is most frequently issued when a system is granted an ATO and the conditions under which the ATO was granted have deteriorated. A DATO may also be issued if the PM/ISO did not ensure the Security Authorization Package was submitted in a timely manner to allow the AO/SCA to review the package. If a Security Authorization Package is submitted in a timely manner, but the AO/SCA is not able to review the package before the ATO expires, the AO will likely extend the existing ATO, e.g., for three (3) months, either via memo or verbally. (Send a follow-up email to the AO reiterating the extension for your

records or request a memo.)

It is extremely rare that a DATO is issued without the PM/ISO being aware that conditions related to the system or its environment have deteriorated to an unacceptable level and that a DATO may result. Be aware that the AO/SCA recognize that the risk level associated with your system can fluctuate, human error is inevitable, that data spills happen. Keep them apprised of incidents and the actions being taken. Reporting goes a long way in building a trust relationship between the AO/SCA and the PM/ISO and their ISSM/ISSO.

3.2.5.1 Security Authorization Package

By the end of RMF Step 5, documents submitted in the Security Authorization Package, at a minimum, included:

- System Security Plan (SSP)/Security Controls Traceability Matrix (SCTM)

  Provides an overview of security requirements, description of agreed-upon controls and other supporting security-related information.

- Risk Assessment Report (RAR)

  Defines the organizationally established level of acceptable risk associated with the operation of an IT system at a specific level; identifies risks; and provides an assessed residual-risk-level for the system.

- Continuous Monitoring (ConMon) Plan

  Provides the strategy to routinely evaluate selected IA controls/metrics. Reference NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*.

- Security Assessment Report (SAR)

  Contains security control assessment results and recommended corrective actions for security-control weaknesses and deficiencies.

- Plan of Action and Milestones (POA&M)

  Defines plans of action and milestones related to correcting weaknesses or deficiencies, as well as reducing or eliminating known vulnerabilities and identifies completion dates.

3.2.5.2 Reciprocity

The Body of Evidence (BOE) for reciprocity include the documents above and frequently the following documents:

- Security Assessment Plan

  Provides a roadmap for how the assessment will be conducted, the type of assessment; it may also be updated during the process to include assessment procedures, and an explanation of how the assessment results were achieved. This Plan is also referred to as the Security Assessment Plan and Procedures.

- Authorization Decision Document

  Conveys the final security authorization decision (i.e., ATO, DATO, IATT) from the authorizing official, any terms and conditions for authorization, and the authorization termination date if appropriate. If the authorization decision document is classified, a memo may be provided in lieu of the decision document.

Reciprocity is defined in CNSSI 4009, IA Glossary, as a "mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information." The AOs will negotiate and agree upon the final documentation set and roles and responsibilities for reciprocity.

Body of Evidence (BOE) is the term commonly used by the IC to describe the artifacts from the assessment and authorization process that support reciprocity. The SSP/SCTM, RAR, ConMon Plan SAR, and POA&M are completed/updated during RMF Step 5 and may be referred to as the security authorization artifacts. Reciprocity within the DoD SAP Community, as well as with the IC, generally requires the documents in the security authorization package (i.e., artifacts) as well as the security assessment plan and the authorization decision document.

For more information on reciprocity with the IC, reference the IC's *Program Manager's Pocket Guide to ICD 503 and the Risk Management Framework*, found on the Intelligence Community Directive (ICD) 503 wiki at:
https://intellipedia.intelink.gov/wiki/Implementing_Intelligence_Community_Directive_503.


At this point the system likely was granted an ATO. The ATO is not just a piece of paper granting authorization to operate; it is, in essence, a contract with the AO. The PM/ISO submitted the Security Authorization Package reflecting the security of the system, how it operates, the environment it operates in, and the risk associated with that system. The AO signed the ATO agreeing that as long as the system is maintained at an acceptable level of risk, the AO will allow it to operate. To ensure that the system stays within an acceptable level of risk, continuous monitoring (ConMon) tasks are performed as outlined in RMF Step 6 - Monitor Security Controls, below.

3.2.6 RMF STEP 6—MONITOR SECURITY CONTROLS

Purpose: Assess and track the security state of an information system and its operational environment.

SDLC Phase: Operational/Maintenance/Disposal

Once an IS has been granted an ATO by an AO/DAO, the system's security state must be monitored. The security control Monitoring step tracks changes to the IS that may affect security controls, ensures no unauthorized changes were made, and assesses security-control effectiveness. DoD SAP elements may use a number of sources including NIST SP 800-37, NIST SP 800-137, and NIST SP 800-53A to develop rigorous and comprehensive, ongoing monitoring programs.

In order to be considered compliant with the continuous monitoring requirements for the DoD SAP Community, each Program must "test" at least one-third of the security controls annually and verify the continued compliance of the remaining controls. By the end of the three-year authorization period, every control will have been tested at least once. However, using a one-third, one-third, one-third approach to assessing controls over the course of three years was determined to be an ineffective method in meeting the intent of continuous monitoring. Critical or more volatile controls should be assessed more frequently, e.g. quarterly, semi-annually; where more static controls may be assessed once every three years. Contact the SCA for additional guidance on recommended frequencies for monitoring controls. Continuous monitoring compliance will be reported at least annually to the respective AO as part of the requirement to maintain the system ATO.

Table 10 lists supporting tasks, person responsible for each task and the deliverables associated with those tasks for Step 6—Monitor Security Controls.

Table 10: RMF Step 6 - Monitor Security Controls

Supporting Tasks	Primary Responsibility	Deliverable(s)
Task 6-1—Determine the security impact of proposed or actual changes to the IS and its environment of operation.	ISO or CCP; ISSO/ ISSM	Change Request
Task 6-2—Assess a selected subset of security controls employed within and inherited by the IS in accordance with the organization-defined monitoring strategy.	SCA; ISSO/ ISSM	Periodic Continuous Monitoring Report
Task 6-3—Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.	ISO or CCP; ISSM/ISSO	Documented evidence of correction such as scan results, registry "dumps," etc.
Task 6-4—Update the SSP, SAR, and POA&M based on the results of the continuous monitoring process.	ISO or CCP	SSP, SAR, RAR, and POA&M
Task 6-5—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 Monitoring Strategy.	ISO or CCP	Periodic Continuous Monitoring Report
Task 6-6—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 monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation	AO	ATO

Supporting Tasks	Primary Responsibility	Deliverable(s)
remains acceptable.		
Task 6-7—Implement an IS Decommissioning Strategy, when needed, which executes required actions when a system is removed from service.	ISO	Updated system inventory

Throughout RMF Step 6, all of the documents created earlier, as well as the system inventory, are updated as needed (at least annually) as part configuration management and monitoring activities. A ConMon Report is submitted to the AO/SCA at least annually.

REFERENCES

DoDM 5205.07, *SAP Security Manual*, Draft, comprised of four volumes, currently only Volume 4: Marking is published, October 10, 2013.

JSIG, *Joint SAP Implementation Guide*, October 9, 2013.

CNSSI 1253, *Security Categorization and Control Selection for National Security Systems,* March 2012.

NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments, September 2012.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* February 2010.

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* March 2011.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009 (includes updates from May 01, 2010).

NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans,* June 2010.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System,* April 2003.

NIST SP 800-60 Volume I, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* August 2008.

NIST SP 800-60 Volume II, Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories,* August 2008.

NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle,* October 2008.

NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

FIPS-199, *Standards for security Categorization of Federal Information and Information Systems*, February 2004.

FIPS-200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

ICD 503, *Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation*, September 15, 2008.

NISTIR 7298, Revision 2, *Glossary of Key Information Security Terms,* May 2013.

ACRONYMS

Acronym	Definition
AO	Authorizing Official
ATO	Authorization To Operate
BoE	Body of Evidence
C&A	Certification and Accreditation
CCP	Common Control Provider
CDS	Cross Domain Solution
C-I-A	Confidentiality, Integrity, and Availability
CIAO	Chief Information Assurance Officer (See new term: CISO)
CIO	Chief Information Officer
CISO	Chief Information Security Officer, See also SISO
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
ConMon	Continuous Monitoring, see also ISCM
CT&E	Certification Test and Evaluation
DAA	Designated Accrediting Authority (See new term: AO)
DAO	Delegated Authorizing Official
DATO	Denied Authorization to Operate
DoD	Department of Defense
DoDM	Department of Defense Manual

FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Management Act of 2002
IA	Information Assurance
IA SOP	Information Assurance Standard Operating Procedures
IAM	Information Assurance Manager (See new term: ISSM)
IAO	Information Assurance Officer (See new term: ISSO)
IASAE	Information Assurance System Architecture Engineer, see also ISSE
IATT	Interim Authorization to Operate
IC	Intelligence Community
ICD	Intelligence Community Directive
IS	Information System
ISCM	Information Security Continuous Monitoring (NIST term, see also ConMon)
ISO	Information System Owner
ISSE	Information Systems Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSP	Information System Security Professional (See new term: SCA)
IT	Information Technology
JAFAN	Joint Air Force – Army – Navy
JSCS	Joint SAP Cybersecurity
JSIG	Joint SAP Implementation Guide
JTF	Joint Task Force

MBO	Mission/Business Owner
MSSP	Master System Security Plan (See new term: IA SOP)
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NSS	National Security Systems
PD	Program Director
PL	Protection Level
PM	Program Manager
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
RAR	Risk Assessment Report
REf	Risk Executive (function)
RMF	Risk Management Framework
SAP	Special Access Program
SAPCO	Special Access Program Central Office
SAPF	Special Access Program Facility
SAR	Security Assessment Report
SC	Security category (i.e. impact level)
SCA	Security Control Assessor
SCO	Service Certifying Organization (See new term: SCA)
SCTM	Security Control Traceability Matrix
SDLC	System Development Life Cycle

SISO	Senior Information Security Officer
SP	Special Publication
SRTM	Security Requirements Traceability Matrix (See new term: SCTM)
SSAA	System Security Authorization Agreement (See new term: SSP)
SSP	System Security Plan
ST&E	Security Test and Evaluation
WG	Working Group