

Defense Security Service

Risk Management Framework (RMF)





What is Risk Management Framework (RMF)

- It is a unified information security framework for the entire federal government that replaces legacy Certification and Accreditation (C&A) Processes applied to information systems
- RMF is a key component of an organization's information security program used in the overall management of organizational risk





RMF Policy References

NIST

- SP 800-30
- SP 800-37
- SP 800-39
- SP 800-53
- SP 800-53A
- 800-137)

CNSS

- CNSSP 22
- CNNSI 1253
- CNSSI 1253A
- CNSSI 4009

NISP

- DoD 5220.22-M
- Industrial Security Letters
- DSS Assessment and Authorization Process Manual





RMF Process Stakeholders: New Terminology

Many RMF stakeholder titles have been revised in the transition from C&A. The following table outlines former terms in the C&A process as well as the corresponding **new terms in the RMF process**. You may continue hearing both sets of terms during the transition to RMF.

Old Term in the C&A Process	New Term in the RMF Process
Designated Approving Authority (DAA)	Authorizing Official (AO)
Regional Designated Approving Authority (RDAA)	Regional Authorizing Official (RAO)
Office of the Designated Approving Authority (ODAA)	NISP Authorization Office
Information System Security Professional (ISSP)	Security Control Assessor (SCA)
Host "Node"	Common Control Provider (CCP)
Customer, Government Contracting Activity (GCA)	Information Owner (IO)
Contractor	Information System Owner (ISO)
Information System Security Manager (ISSM)*	ISSM
Information System Security Officer (ISSO)*	ISSO

**Titles will remain the same in RMF.*





Connecting the Dots Old and New

Process	C&A	RMF
ODAA Business Management System (OBMS)	same	same
SSP Template	same	same
Categorization	Basic, Med, High PLs	Low, Mod, High Accessibility
Certification Statement	same	same
Risk Acknowledgement/Tailoring-out	Risk Acknowledged	Tailored-Out
MOU/Enhancements	MOU	ISA
Standing-Up Like System	Self- Certification	Type Authorization
Controls	NISPOM Refs	NIST Controls
Approval to Process	Accreditation	Authorization



Connecting the Dots Cont.



Process	C&A	RMF
Submission Validation within OBMS	SSP Certification Statement Profile	SSP Certification Statement POAM Risk Assessment Report
Assessment Comments on issues	Comments Form	Security Assessment Report (SAR)





Key Factors Driving the Transition to RMF

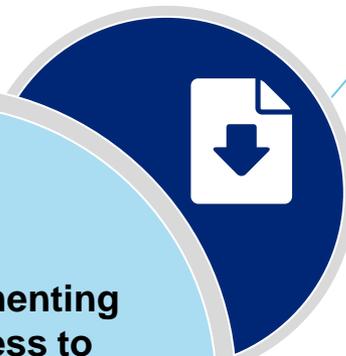
Effective and Efficient Risk Management

Shift from a static, “check-the-box” mentality to a flexible, dynamic approach to assess and manage risk more effectively and efficiently.



Common Foundation for Information Security

Implement a common foundation for information security that aligns to federal government standards for DSS and cleared contractors for a more uniform and consistent approach to manage risk associated with the operation of a classified IS.



DSS is implementing the RMF process to assess and authorize Information Systems (IS).

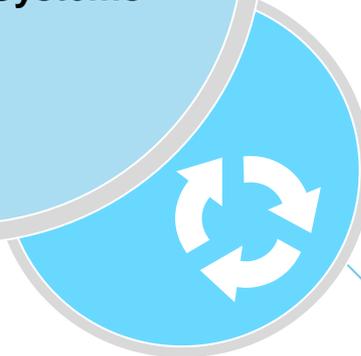
Trust Across the Federal Government

Build reciprocity with other federal agencies to develop trust across the federal government through a more holistic, flexible, and strategic process for the risk management of IT systems.



Streamline DSS processes

Streamline DSS processes to support the authorization of a cleared contractor’s IS processing classified information as part of the NISP.





Roles and Responsibilities in the RMF Process

Role	Responsibilities
 <p>Authorizing Official (AO) (formerly the DAA) and Designated Authorizing Official (DAO) (formerly the RDAA)</p>	<ul style="list-style-type: none">• Formally assumes responsibility for operating an IS at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and national security
 <p>Security Control Assessor (SCA) (formerly the ISSP)</p>	<ul style="list-style-type: none">• Performs oversight of a contractor's IS processing classified information• Conducts 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• Provides an assessment of the severity of weaknesses or deficiencies discovered in the IS and its environment of operation and recommends corrective actions• Provides an authorization decision recommendation to the DAO
 <p>Common Control Provider (CCP) (formerly the Host "Node")</p>	<ul style="list-style-type: none">• Assumes responsibility for the development, implementation, assessment, and monitoring of common security controls
 <p>Information Owner (IO)/Government Contracting Activity (GCA) (a.k.a. the Customer)</p>	<ul style="list-style-type: none">• Holds statutory, management, or operational authority for specific information to establish the policies and procedures governing its generation, collection, processing, dissemination, and disposal• Establishes the rules for appropriate use and protection of the subject information and retains that responsibility when the information is shared with or provided to other organizations• Provides input to the Information System Owners (ISOs) regarding data





Roles and Responsibilities in the RMF Process

Role	Responsibilities
 <p>Information System Owner (ISO) (a.k.a. GCA for government systems and ISSM for contractor-owned systems)</p>	<ul style="list-style-type: none">• Holds responsibility for the procurement, development, integration, modification, operation, maintenance, and disposal of an IS• Addresses the operational interests of the user community and ensures compliance with information security requirements
 <p>Information System Security Manager (ISSM)</p>	<ul style="list-style-type: none">• Serves as a principal advisor on all matters, technical and otherwise, involving the security of an IS under her/his purview• Ensures physical and environmental protection, personnel security, incident handling, and security training and awareness• Monitors a system and its environment of operation to include developing and updating the System Security Plan (SSP), managing and controlling changes to the system, and assessing the security impact of those changes• Must be trained to the level commensurate with the complexity of the contractor's IS or have a local ISSO who is trained.
 <p>Facility Security Officer</p>	<ul style="list-style-type: none">• Supports the ISSM in their efforts to implement security requirements for classified information systems• Ensures physical and environmental protection, personnel security, incident handling, and security training and awareness
<p>Information System Security Officer (ISSO)</p>	<ul style="list-style-type: none">• If appointed, supports the ISSM in their efforts to implement security requirements as mandated by NISPOM and DAAPM.• Configures and manage the IS configuration





RMF Process Walk Through: Introduction

RMF is a six step process designed to build information security capabilities into Information Systems (IS) throughout the NISP through the application of community best practices for IS management, operational, and technical security controls. The RMF process is explained in further detail in the ISOM and the DAAPM.





RMF Process Walk Through

Step 1: Categorize the IS

- ✓ The ISSM/ISSO categorizes the IS based on the impact due to a loss of confidentiality (moderate/high), integrity (low/moderate/high), and availability (low/moderate/high) of the information or IS according to information provided by the IO.
- ✓ Industry should perform a Risk/Threat Assessment for specific concerns for their Facility/Program.
- ✓ Absent any other requirements Industry may use the DSS baseline of moderate/low/low.
- ✓ The ISSM then documents the description, including the system/authorization boundary in the System Security Plan (SSP)
- ✓ ISSM assign qualified personnel to RMF roles and document team member assignments in the Security Plan

This step will result in the following:

- **Artifact(s):** Risk Assessment and start initial SSP describing the IS. [Risk Assessment Report - Template.docx](#)
- See NIST SP 800-30 (Risk Assessment) for additional guidance.





RMF Process Walk Through

Step 2: Select Security Controls

- ✓ The ISSM (and ISSO, as appropriate) selects the security control baseline applicable to the IS based upon the results of the categorization and tailors the controls as needed by supplementing, modifying, or tailoring out controls to effectively manage risk for any unique system conditions.
- ✓ The ISSM (and ISSO, as appropriate) develops a strategy for continuous monitoring of security control effectiveness.
- ✓ The ISSM then documents the results of selecting the security controls in the SSP via the OBMS.
- ✓ The assigned ISSP/SCA reviews the SSP to ensure it meets the necessary security requirements and effectively identifies potential risks to the IS. The ISSP/SCA also reviews the ISSM-recommended deltas from the standard baseline.
- ✓ The ISSP/SCA then notifies the ISSM of concurrence with selected security controls.

This step will result in the following:

- **Outcome:** Agreed upon security control set.
- **Artifact(s):** Continuous monitoring strategy and updated SSP with controls identified. [DSS RMF SSP Template M-I-I with Controls Overlays_9 May 16 v5.docx](#) [Categorization Concurrence Implementation Form.docx](#)





RMF Process Walk Through

Step 3: Implement Security Controls

- ✓ The ISSM and ISSO implement security controls for the IS and may conduct an initial assessment to facilitate early identification of weaknesses and deficiencies.
- ✓ The ISSM then documents the security control implementation in the Security Controls Traceability Matrix (SCTM) portion of the SSP via the OBMS.

This step will result in the following:

- **Outcome:** Implemented security requirements.
- **Artifact(s):** Updated SSP with a functional description of security control implementation.





RMF Process Walk Through

Step 4: Assess Security Controls - *Part One*

- ✓ The ISSM, with the ISSO, develops a Security Assessment Plan (SAP) that addresses objectives for the assessment, methods for verifying security control compliance, the schedule for the initial control assessment, and actual assessment procedures. (*Cleared Industry can leverage assessment procedures in the DAAPM*).
- ✓ The ISSM then conducts the initial assessment of the effectiveness of the security controls and documents the issues, findings, and recommendations in a Security Assessment Report (SAR).
- ✓ The ISSM, after the initial assessment, conducts remediation actions based on the findings and recommendations in the Plan of Action and Milestones (POA&M), signs a Certification Statement, and submits the SSP (using the OBMS) to DSS.

[RMF POAM.xlsx](#)

[DSS RMF IS Security Package Submission and Certification Statement v1 April 26 2016.rtf](#)





RMF Process Walk Through

Step 4: Assess Security Controls - *Part Two*

- ✓ The ISSP/SCA receives the SSP, performs an SSP review, and conducts an on-site validation/assessment.
- ✓ The ISSP/SCA informs the ISSM of any additional deficiencies or weaknesses discovered and identifies necessary remediation actions in a POA&M.
- ✓ The ISSP/SCA schedules a revalidation visit if necessary and makes final updates to the SAR.

This step will result in the following:

- **Outcome:** Tested, evaluated, and remediated security controls.
- **Artifact(s):** SAR, and final SSP.

[DSS SAR Template april 2016.docx](#)

Additional guidance for assessing controls: NIST SP 800-53A





RMF Process Walk Through

Step 5: Authorize the IS

- ✓ The ISSP/SCA reviews and submits the security authorization package to the DAO.
- ✓ The DAO assesses the security authorization package and issues an authorization decision for the IS—either Authorization to Operate (ATO) or Denied Authorization to Operate (DATO)—which includes any terms and conditions of operation as well as the authorization termination date (ATD).

This step will result in the following:

- **Outcome:** Risk determination and acceptance decision by the DAO.
- **Artifact(s):** Complete security authorization package to include the POA&M.

[DSS SAR Template april 2016.docx](#)

[RMF ATO Rev 7.docx](#)





RMF Process Walk Through

Step 6: Monitor the IS

- ✓ The ISSM determines the security impact of proposed or actual changes to the IS and its operating environment and informs the ISSP/SCA as necessary.
- ✓ The ISSM assesses a selected subset of the security controls, based on the approved continuous monitoring strategy, and informs the ISSP/SCA of the results.
- ✓ The ISSM updates SSP documentation and works to satisfy POA&M requirements, and provides regular status reports to their ISSP/SCA per the continuous monitoring strategy.
- ✓ The ISSM conducts any necessary remediation actions based on findings discovered during continuous monitoring.
- ✓ The ISSM ensures IS security documentation is updated and maintained and reviews the reported security status of the IS.
- ✓ As necessary, the ISSM develops and implements an IS decommissioning strategy.

This step will result in the following:

- **Outcome:** Continued evaluation and remediation of the authorized IS.
- **Artifact(s):** Updated POA&M, updated SSP, and decommissioning strategy (as necessary).





Security Controls and Continuous Monitoring

The RMF process will manage risk more effectively through the introduction of security controls and continuous monitoring of those controls.

Purpose of Security Controls and Continuous Monitoring

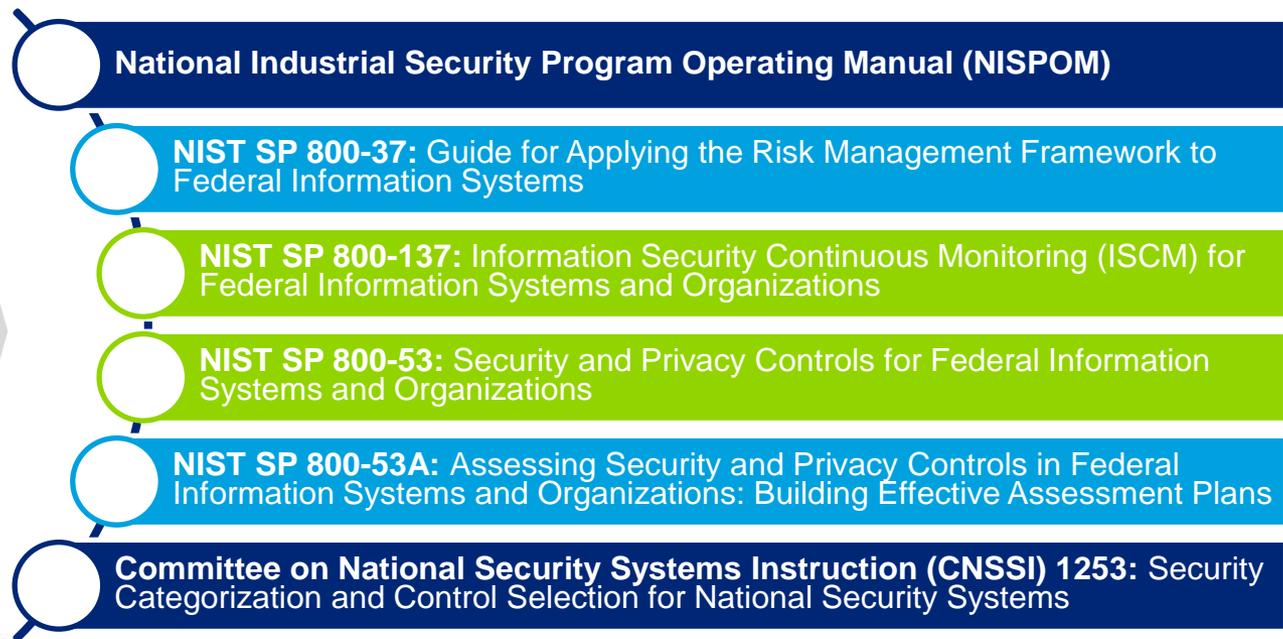
- ✓ Assess security control effectiveness for an IS
- ✓ Document changes to the IS or its environment of operation
- ✓ Conduct security impact analyses of associated changes
- ✓ Report the security status of an IS

Benefits of Security Controls and Continuous Monitoring

- ✓ Facilitate more efficient enterprise management of cybersecurity
- ✓ Increase security in the system development and acquisition processes
- ✓ Ensure compliance with national standards and reporting requirements

Resources to assist in the RMF Process

Many additional resources can be found on the NIST website (www.nist.gov)



Security Authorization Package Submissions to AO



The RMF process will require the inclusion of additional artifacts when Industry submits a security authorization package to DSS.



Artifacts Required in Security Authorization Packages

- Requirements Documents (e.g. DD Form 254)
- Risk Assessment Report (RAR)
- System Security Plan (SSP)
- Security Assessment Report (SAR)
- ISSM Certification Statement
- Plan of Action and Milestones (POA&M)
- Authorization Decision Letter for Signature



Resources to Assist with RMF Process

- RMF SharePoint Site
- Frequently Asked Questions (FAQs) on the DSS website
- DSS Authorization and Assessment Process Manual (DAAPM)
- RMF job aids and validation artifacts for ISSPs/SCAs
- Industrial Security Operating Manual (ISOM) (once update is complete)



Transition Timeline



System Accreditation Status	Transition Timeline / Instructions
SSP submitted prior to 1 August 2016	Cleared contractors continue using current Certification & Accreditation process with the latest version of the ODAA Process Manual. ATO will be no greater than 18 months starting August 1, 2016. Within 6 months of authorization, develop a POA&M for transition to RMF.
Stand-Alone Systems after 1 August 2016	Execute RMF Assessment and Authorization through the use of the DSS Assessment and Authorization Process Manual (DAAPM).

Transition Timeline Cont.

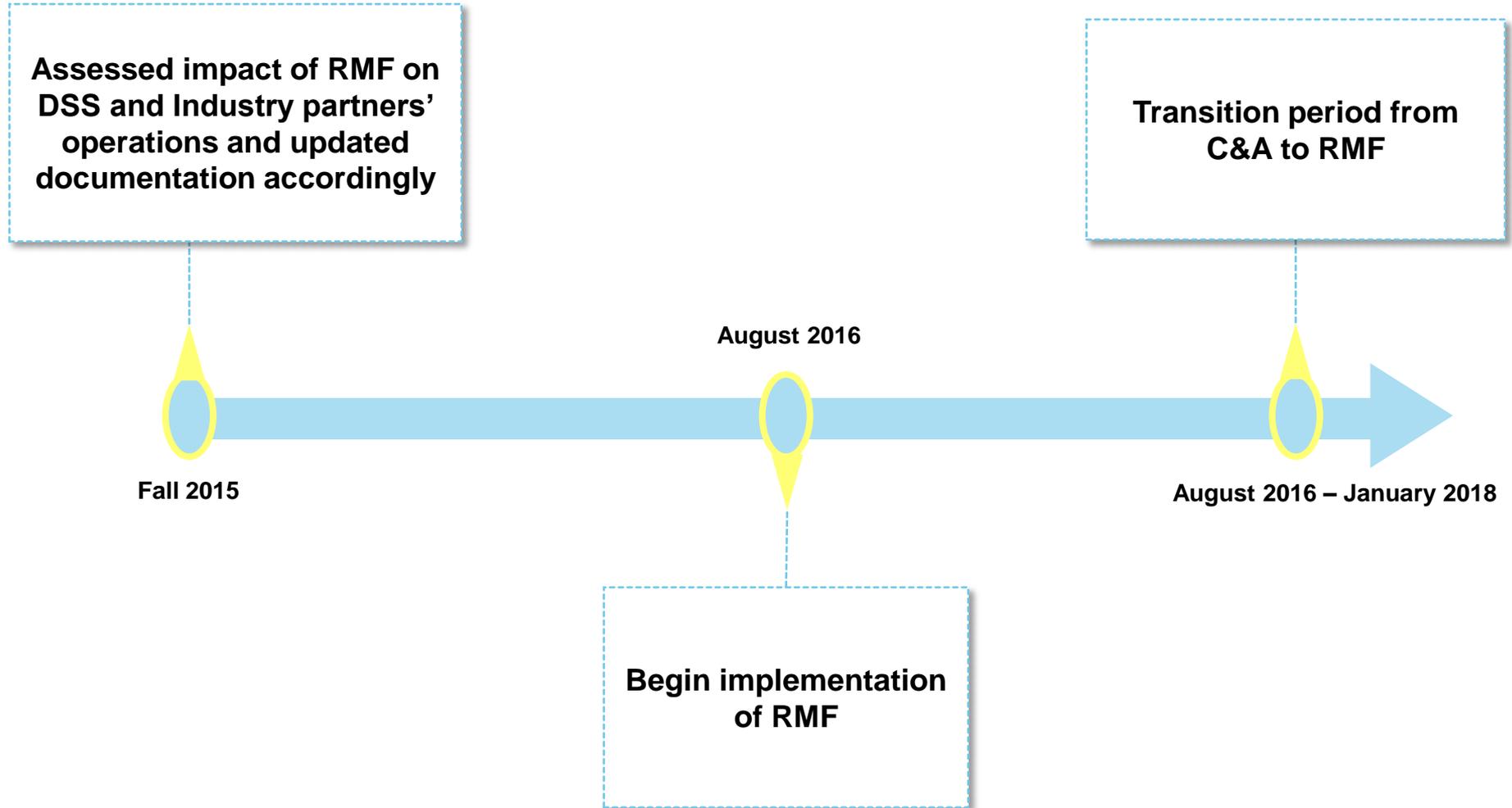


System Accreditation Status	Transition Timeline / Instructions
<p data-bbox="9 396 879 606">Local Area Network, Wide Area Network or Interconnected System between August 1, 2016 – 28 February 2017</p>	<p data-bbox="966 396 1912 778">Cleared contractors continue using the current Certification & Accreditation process with the latest version of the ODAA Process Manual. ATO will be no greater than 18 months starting August 1, 2016. Within 6 months of authorization, develop a POA&M for transition to RMF.</p>
<p data-bbox="9 959 743 1092">Local Area Network, Wide Area Network or Interconnected System after 1 March 2017.</p>	<p data-bbox="966 959 1835 1149">Execute RMF Assessment and Authorization process through the use of the DSS Assessment and Authorization Process Manual (DAAPM).</p>





RMF Implementation Schedule





CDSE Training courses

- Introduction to RMF (CS124.16)
- Continuous Monitoring (CS200.16)
- Categorization of the System (CS102.16)
- Selecting Security Controls (CS103.16)
- Implementing Security Controls (CS104.16)
- Assessing Security Controls (CS105.16)
- Authorizing Systems (CS106.16)
- Monitoring Security Controls (CS107.16)

- www.dss.mil/rmf





Questions ?

