

Getting Started Guide for Classified Systems under the Risk Management Framework (RMF)

1. TRAINING- CDSE/STEPP (www.cdse.edu)

- a. Introduction to RMF (CS124.16)
- b. Categorization of the System (CS102.16)
- c. Selecting Security Controls (CS103.16)
- d. Implementing Security Controls (CS104.16)
- e. Assessing Security Controls (CS105.16)
- f. Authorizing Systems (CS106.16)
- g. Monitoring Security Controls (CS107.16)
- h. Continuous Monitoring (CS200.16)
- i. RMF Overview - Recorded Webinar



(<http://www.cdse.edu/catalog/webinars/webinar-archives.html>)

2. DEENSE SECURITY SERVICE (DSS) HOMEPAGE (www.dss.mil)

- Check for RMF latest updates under “News”.

3. RMF INFORMATION AND RESOURCES (www.dss.mil/rmf)

a. Policy and Guidance

- DSS Assessment and Authorization Process Manual (DAAPM) DSS RMF Implementation Guidance
- NISPOM, Change 2 (National Industrial Security Operating Manual)
- CNSS 1253 (RMF Guidance for National Security System)
- NIST 800-53 (RMF Guidance for Federal Systems)

b. Resources/Templates

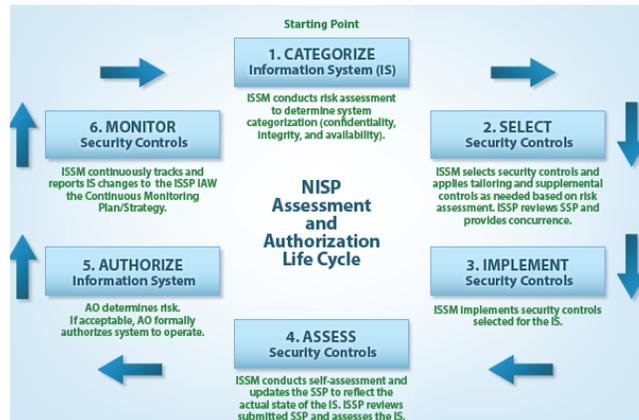
- RMF SSP Template
- RMF SSP Template Appendices
- Technical Assessment Guide Windows 7
- Technical Assessment Guide Windows 10
- Technical Assessment Guide Windows Server 2012
- Technical Assessment Guide RHEL 6
- DISA STIG Viewer
- SCAP Compliance Checker

Getting Started Guide for Classified Systems under the Risk Management Framework (RMF)

4. RMF (Six Step Process)

a. Step 1 – Categorization

- Read contract, DD254, classification guidance etc. for system requirements.
- Perform Risk Assessment (Stakeholders ISSM, FSO, Program Manager, Program CI Representative, and appropriate Business/Mission Owners).
- Define System type, boundary, environment, special requirements.
- Determine if DSS baseline Moderate-Low-Low is acceptable or if the baseline needs to be increased due to contractual requirements or outcome for the Risk Assessment. The customer/information owner is not required.



b. Step 2 – Select Security Controls

- The ISSM selects the security controls according to system type, program specific requirements, environment, boundary and continuous monitoring strategy.
- The ISSM can tailor controls as needed and/or utilize DSS provided overlays.
- The ISSM is required to show selected, tailored and/or modified controls within the initial SSP with an appropriate justification.
- Initial SSP and Risk Assessment should be forwarded via the OBMS.

c. Step 3 – Implement Controls

- The ISSM implements security controls for the IS and may conduct an initial assessment to facilitate early identification of weaknesses and deficiencies.
- ISSM then documents the security control implementation in the Security and update POAM as applicable.

**Getting Started Guide for Classified Systems under the
Risk Management Framework (RMF)**

d. Step 4 - Assess Controls

- The ISSM will conduct initial assessment of the security controls in accordance with defined implementation within the SSP.
- The ISSM may use the Security Content Automation Protocol (SCAP) Compliance Checker (SCC) Tool with automated SCAP content, DISA's Security Technical Implementation Guidelines (STIGs), STIG Viewer, and the DSS Technical Assessment Job Aids to support the initial assessment.
- 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.
- ISSP/SCA receives the SSP, performs review and coordinates with requirements with appropriate DSS member if needed.
- Implementation responses must provide sufficient data to describe how the security control is met.

e. Step 5 – Authorization

- The ISSP/SCA reviews and submits the security authorization package to the AO.
- The AO 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).

f. STEP 6 – MONITORING

- 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 in coordination with appropriate leadership, 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.

**Getting Started Guide for Classified Systems under the
Risk Management Framework (RMF)**

- 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.

PLEASE CONTACT YOUR LOCAL ISSP IF YOU HAVE ANY QUESTIONS OR CONCERNS.