DSS Risk Management Framework (RMF) Process – Step 1 (Categorize)

Start

Collect Key Documents (Contract, DD 254, RAR, SCG, etc.)

Determine System’s Authorization Boundary

Current RAR On Record?

Yes

Prepare Risk Assessment Report (RAR)

No

Coordinate with Company’s Assigned DSS ISR/CISA

Higher Impact Levels Justified?

Yes

Obtain GCA / Stakeholder Approval (SSP Artifact)

No

Determine Final Categorization of IS & Information There-in (Default=M-L-L)

Update SSP (Description, Auth Boundary, System Type, etc.)

Higher Impact Levels Justified?

Yes

Goto RMF Step-2

No

Prepare Risk Assessment Report (RAR)

GCA / Stakeholder Approval Memo

Provide Program Risk Assessment/Threat Data Information

Current RAR On Record?

Yes

Goto RMF Step-2

No

Goto RMF Step-2
DSS Risk Management Framework (RMF) Process – Step 2 (Select Security Controls)

From RMF Step-1
- Identify Baseline Security Controls For IS Categorization
  - DAAPM
  - DSS Overlay

Update SSP with Baseline Security Controls
- Update SSP with Tailored Security Controls & Justification
  - tailoring as needed
  - NIST SP 800-53v4
  - CNSI 1253 Overlay(s)
  - DSS Overlay

Develop CONMON Strategy
- Tailored-Out SecCtrls? Yes
  - Tailored SecCtrl Approval (DD 254, SOW, RAL)
  - Submit SSP, RAR, CONMON Strategy, & Artifacts into OBMS
  - Email ISSP of DSS RMF Step 1/2 OBMS Submission
- Tailored-Out SecCtrls? No
  - UNCLAS Docs Only
  - Coordinate Tailored-Out SecCtrls with ISSP-TL / AO

Tailored-Out SecCtrls? Yes
- Complete Categorization & Implementation Concurrence Form
  - Complete Categorization & Implementation Concurrence Form
  - Concur w/Cat & SecCtrl Selection?
    - To Step 4 Part (B)
    - Proceed w/DATO Action
    - Validate Tailored-Out SecCtrls Justification (DD 254, SOW)
- SecCtrl Justification Included? Yes
  - Notify ISSM of RAL Requirement
  - Notify ISSM of RAL Requirement
  - AO Requires RAL?
    - Yes
      - Coordinate Tailored SecCtrls with ISSP-TL / AO
    - No
  - No

Tailored-Out SecCtrls? No
- Email ISSM of DSS RMF Step 1/2 OBMS Submission
- Return OBMS Record back to Submitter (ISSM)
- Upload Categorization & Implementation Concurrence Form into OBMS
- Complete Categorization & Implementation Concurrence Form
- Concur w/Cat & SecCtrl Selection?
  - Yes
  - Proceed w/DATO Action
  - Severe Issues w/RMF Pkg
    - Yes
      - Review RMF Pkg Submission
    - No
      - Proceed w/DATO Action
DSS Risk Management Framework (RMF) Process – Step 3 (Implement Security Controls)

- **Implementation Tools**
  - DAAPM
  - STIG Viewer
  - Tailored SSP
  - NAO Group Policy Config Tool
  - SCAP Compliance Checker (SCC) Tool
  - Manual Configuration

- **Steps**
  1. Implement Technical Security Controls on System(s)
  2. Develop Applicable Non-Technical Documentation
  3. Update SSP with Security Control Implementation Status
  4. Start POA&M As Applicable

- **Artifacts**
  - Updated SSP (UNCLASS Docs Only)
  - Disaster Recovery Plan (DRP)
  - Configuration Management (CM) Plan
  - Incident Response Plan (IRP)
  - Security Awareness Training Plan
  - MOU/MOAs
  - Other Applicable Artifacts

- **Related Documents**
  - NAO Group Policy Config Tool
  - SCAP Compliance Checker (SCC) Tool
  - Manual Configuration
  - SCAP Compliance
  - NIST 800-53
  - NIST 800-53A

Source: DAAPM Ver. 1.1
Author: A.E. Carbone/IOFSA Revised: 2017/05/18
Conduct "Initial" Assessment to Ensure Security Controls Operating as Intended → Update SSP with "Actual" Security Control State Information → Develop/Update POA&M with "Residual" Vulnerabilities → Download Validation Tools and Install on System for SCA OSV (STIG Viewer, SCC, etc.) → Submit Final RMF Authorization Package via OBMS (UNCLAS Docs Only) → Email ISSP of OBMS Submission

Assessment Tools:
- DAAPM
- Updated SSP
- POA&M
- Certification Statement (Required)
- ISSM Appointment Letter (Required)
- SSP (Required)
- POA&M (Required)
- RAR (Required)
- COOP, DRP, etc.
- CM Plan CCB Charter
- Contract Info (DD 254, SOW, RFP)
- MOU/MOA/ISA
- IRP
- Security Awareness & Training Plan
- RAL(s)
- All Other Relevant Artifacts (Policy)

Tailored SSP Parameters
NIST Security Controls
SCAP Compliance Checker (SCC)
STIG Viewer Tool

From RMF Step-3
To RMF Step-4B

Source: DAAPM Ver. 1.1
Author: A.E. Carbone/IOFS Revised: 2017/05/18
DSS Risk Management Framework (RMF) Process – Step 6 (Monitor Security Controls)

Source: DAAPM Ver. 1.1
Author: A.E. Carbone/IOFSA Revised: 2017/05/18

From Step 5:
- Implement COMMON Strategy
- Assess Security Control Subset IAW COMMON Strategy
- Mitigate Risk Based on COMMON Results
- Update SSP & POA&M with COMMON Results
- Submit Status Reports to ISSP IAW COMMON Strategy

IS Decommissioned?

Yes
- Submit IS Decommission Action in OBMS

No
- Stop
- Implement Decommission Strategy

Implement A0-Approved Mitigation Strategy

Review ISSM’s Status Report

Acceptable Risk?

Yes
- File Status Report
- Create ISFD Entry
- Review/Update Risk Mitigation Strategy
- Upload Decom Ltr in OBMS & Closeout Record
- Email Decommission Ltr to ISSM/DSS Staff
- Sign Decommission Letter

No
- Develop Risk Mitigation Strategy with ISSM
- Immediately Contact ISSP-TL/AO

Prepare Decommission Letter

Email Decommission Letter to ISSP/Tl

Sign Decommission Letter

ISSP/Tl

ISPM/SCA

ISSM

AO