

2016 Defense Health Information Technology Symposium

Navigating the Risk Management Framework Process



“A joint, integrated, premier system of health, supporting those who serve in the defense of our country.”



“Medically Ready Force...Ready Medical Force”

Learning Objectives

- Explain what happens during each of the six steps in the Risk Management Framework
- Describe the use of Privacy Overlay to address and augment privacy-centric security controls for information (i.e., PII/PHI) within an information system
- Discuss collaborative efforts between DHA Privacy and DHA HIT CSD on effective system design to ensure privacy and security of medical information and information systems
- Identify and understand RMF readiness and preparation resources

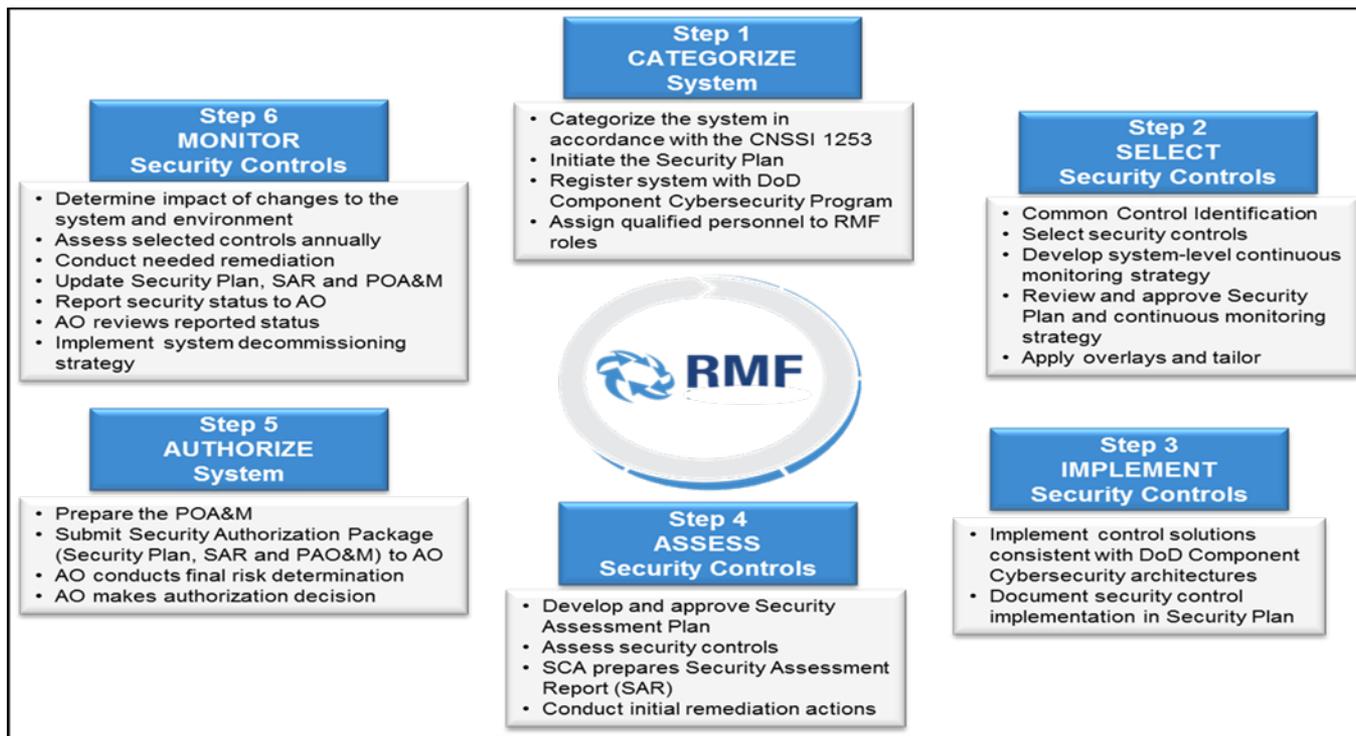
Agenda

- RMF Workflow
 - Categorization
 - Selection
 - Overlays Benefits
 - Implementation
 - Assess
 - Authorize
 - Monitor
- Benefits of implementing the Privacy Overlay
- RMF Readiness
- Resources

The End to DIACAP

- Completed packages must be submitted to the AO for signature NLT October 1, 2016 to receive a valid DIACAP Accreditation (maximum 1.5 year ATD)
- All packages submitted to the AO for signature post October 1, 2016 must receive an RMF Authorization.

Risk Management Framework Workflow



“Medically Ready Force...Ready Medical Force”

DHA RMF A&A Timeline

- DHA RMF Assessment Authorization (A&A) effort based on 4-month timeline
- Bi-weekly meetings scheduled to track progress and milestones

Note: All Security Authorization Packages associated with circuit connections to the Defense Information System Network (DISN) must be signed 35 days prior to expiration.

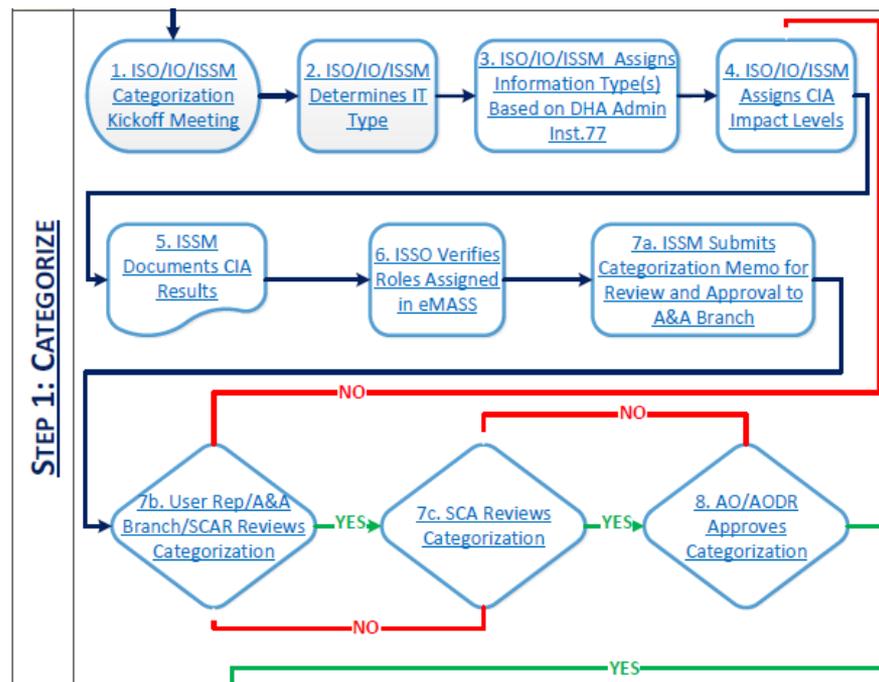
Phase	Activity	Timeline
Phase I	Preparation for Independent Verification & Validation (IV&V) (Steps 2 & 3)	(up to) 45 Days
Phase II	Execute IV&V Onsite Assessment (Step 4)	(up to) 15 Days
Phase III	Post IV&V Plan of Action & Milestones (POA&M) and Security Assessment Report (SAR) Development and Mitigation (Step 4 continues)	(up to) 35 days
Phase IV	Submit Package for Approval (Step 5)	(up to) 30 Days
Phase V	A&A Process Closeout	(up to) 7 Days

A&A Effort Major Milestones

- Submit System Security Plan with Boundary documents
- Completion of Control Correlation Identifiers (CCIs) in Enterprise Mission Assurance Support Service (eMASS)
- Provide Self Assessment Scans (>30 days old) and Manual Checklists
- Submit Policies and Procedures documentation
- Provide Readiness Review Checklist
- IV&V kickoff
- IV&V Team onsite
- Security Authorization Package submission
- Authorizing Official (AO) signature date

RMF Step 1 – Categorize (1 of 7)

- DHA IV&V Pre-Kickoff Activities



RMF Step 1 – Categorize (2 of 7)

- DHA IV&V Pre-Kickoff Activities
 - DHA Administrative Instruction 77, Security Categorization and Control Selection for Information Technology, is used during Categorization
 - Located on the DHA RMF Portal in the DHA RMF Guidance folder
 - ([DHA RMF Portal
https://info.health.mil/hit/infosec/assessor/rmfipt/SitePages/home.aspx](https://info.health.mil/hit/infosec/assessor/rmfipt/SitePages/home.aspx))
 - Categorization is completed and submitted for SCAR review
 - System Categorization is AODR or AO approved
 - Signed Categorization Memo is uploaded to eMASS
 - System registered in eMASS/DoD Information Technology Portfolio Repository (DITPR) with identical naming convention

RMF Step 1 – Categorize (3 of 7)

- Security category = Potential impact to organization or individuals if there is a loss of control of the information or information systems needed to accomplish the organization’s mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, or protect individuals
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories (Provides categorization guidance for Non-NSS)
- CNSSI Instruction No. 1253, Security Categorization and Controls Selection for National Security Systems (NSS)(Provides categorization guidance for NSS)

Security Category PII = {(confidentiality, impact), (integrity, impact), (availability, impact)}

RMF Step 1 – Categorize (4 of 7)

- RMF Categorization of PII
 - NIST SP 800-122, Guide to Protecting the Confidentiality of PII, provides guidance to identify PII, categorize PII and determine the PII confidentiality impact level using:
 - Federal Information Processes Standard (FIPS) 199 Potential Impact Values
 - Six additional factors: Identifiability, Quantity of PII, Data Field Sensitivity, Obligation to Protect Confidentiality, Access to and Location of PII, and Context of Use
 - PII confidentiality impact level:
 - Indicates the potential harm that could result to the subject individuals or the organization if PII were inappropriately accessed, used, or disclosed

RMF Step 1 – Categorize (5 of 7)

FIPS 199 Potential Impact Values as incorporated in NIST SP 800-122

Impact Value	Type of Adverse Effect	Expected adverse effect of the loss of confidentiality, integrity, or availability
Low	Limited	(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals

RMF Step 1 – Categorize (6 of 7)

FIPS 199 Potential Impact Values as incorporated in NIST SP 800-122 (continued)

Impact Value	Type of Adverse Effect	Expected adverse effect of the loss of confidentiality, integrity, or availability
Moderate	Serious	(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries

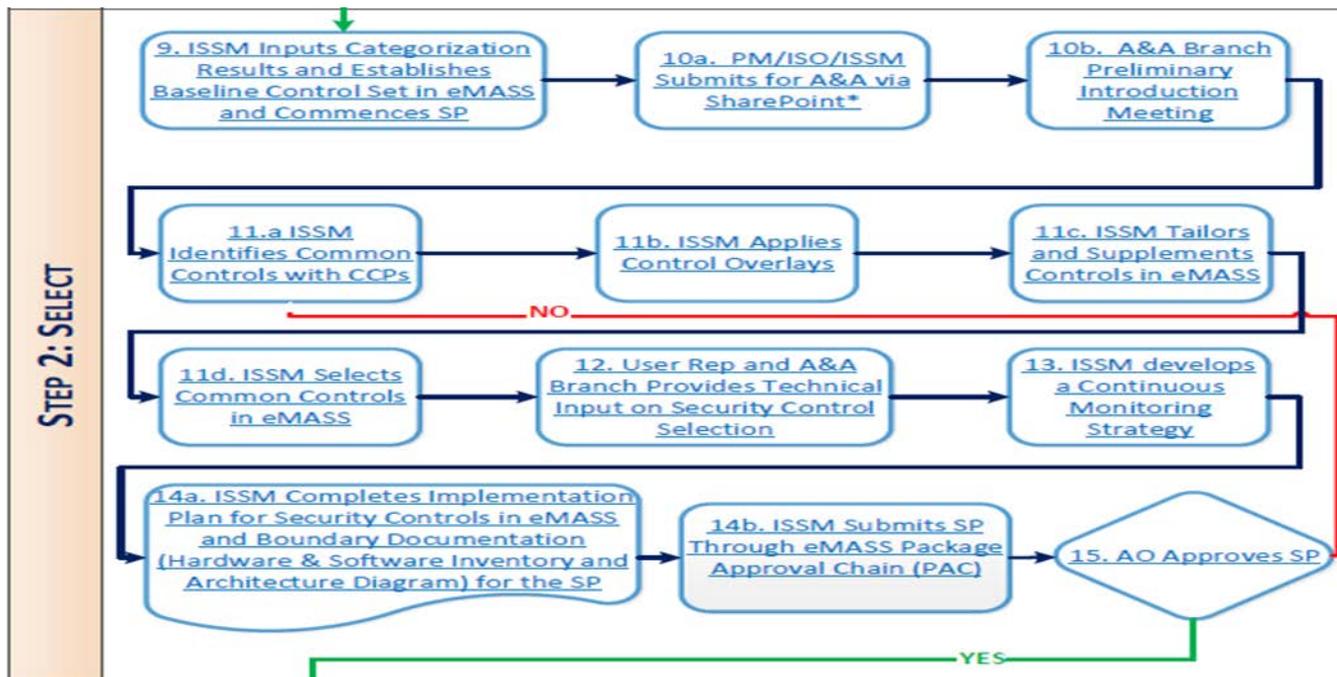
RMF Step 1 – Categorize (7 of 7)

FIPS 199 Potential Impact Values as incorporated in NIST SP 800-122 (continued)

Impact Value	Type of Adverse Effect	Expected adverse effect of the loss of confidentiality, integrity, or availability
High	Severe or catastrophic	(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

RMF Step 2 – Select (1 of 5)

- DHA IV&V Pre-Kickoff Activities



RMF Step 2 – Select (2 of 5)

- DHA IV&V Pre-Kickoff Activities
 - Develop Systems' Baseline in eMASS
 - Apply overlay(s) and identify Common Controls
 - Establish inheritance relationships
 - Complete Security Plan (SP) and Implementation Plan
 - Final Detail Architecture Diagram, Hardware, Software, and Ports, Protocols and Services (PPS) documents must be submitted with SP
 - Security Assessment Plan (SAP) cannot be completed by the DHA IV&V Team without these documents
 - Information System Security Manager (ISSM)/Program Manager (PM) initiate SP Approval

RMF Step 2 – Select (3 of 5)

The overlay provides the following for each control it contains:

- Justification for inclusion in overlay
- Applicable control specifications:
 - Selection indicator (+, --, or blank with other specifications)
 - Supplemental Guidance (G)
 - Parameter Value (V)
 - Control Extensions (E)
- Reference to the applicable requirement(s) (R)
- Table 3 provides summary of all four overlays

Table 3: Privacy Overlays Security and Privacy Controls

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			PHI
	LOW	MODERATE	HIGH	
AC-1	+GR	+GR	+GR	+ER
AC-2	+EGVR	+EGVR	+EGVR	+EGR
AC-2(8)		--R	--R	
AC-2(9)	GVR	GVR	GVR	R
AC-2(13)	+R	+R	+R	+R
AC-3	+EGR	+EGR	+EGR	+GR
AC-3(9)		+EVR	+EVR	+R
AC-3(10)	GVR	GVR	GVR	
AC-4		+GR	+GR	+R
AC-4(8)			+VR	
AC-4(12)				+GR
AC-4(15)		+GR	+GR	+R
AC-4(17)		+GVR	+GVR	
AC-4(18)		+GR	+GR	+R
AC-5		+GR	+GR	+GR

RMF Step 2 – Select (4 of 5)

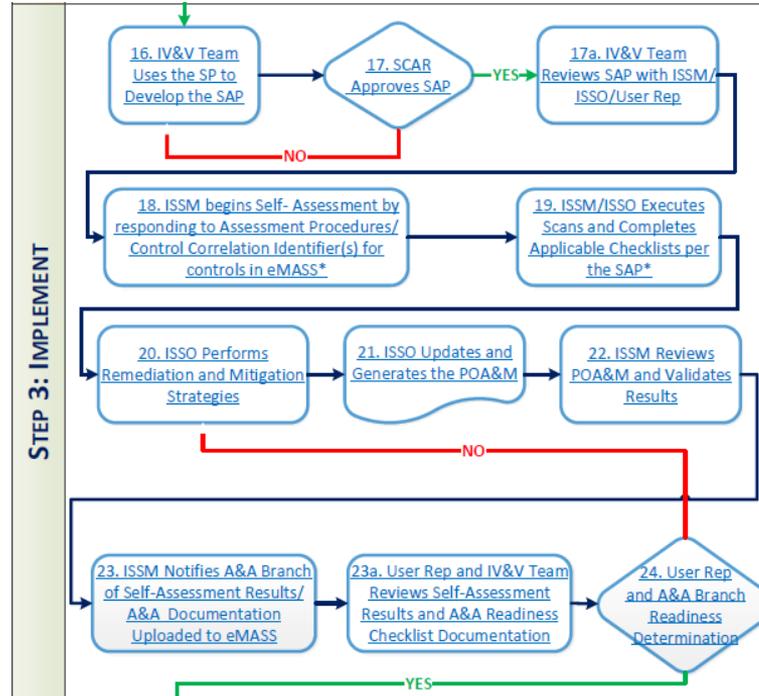
- Benefits of implementing the privacy overlays
 - Enterprise level benefits
 - Informed leadership decision-making based on organization’s privacy risk and sensitivity of PII
 - Efficient allocation of resources (e.g., human capital, budget, etc.)
 - Determination of when a system is ready to “go live”
 - Defined, constant, and repeatable business process to provide consistent protections for PII throughout an organization based on sensitivity
 - Technical implementation of broad or vague privacy requirements (e.g., “establish appropriate administrative, technical, and physical safeguards ...” 5 U.S.C. 552a(e)(10))
 - System level benefits
 - Effective communication between privacy and security professionals supports tangible implementation of privacy policies at the system level
 - Proportionate relationship between sensitivity of PII and system-level privacy protection

RMF Step 2 – Select (5 of 5)

- Inheritance
 - eMASS Systems of Records (SOR)
 - Common Controls provided by an overarching entity
 - Tier 1 SOR – Provided by DoD (Mandatory)
 - Tier 2 SOR – Provided by DHA (Mandatory for DHA)
 - MEDCOM SOR – Provided by MEDCOM (Mandatory for Army)
 - Tier 3 SOR – Provided by Program Office
 - Inheritance is requested within eMASS
 - System Management > Associations (Inheritance)
 - Know exactly what you are inheriting
 - May not inherit all CCIs for a control
 - Establish Inheritance as soon as possible
 - External Inheritance requires Service Level Agreement (SLA)/Memorandum of Agreement (MOA)
 - Vulnerabilities will be Inherited along with Controls
 - Inherited Vulnerabilities will be included on POA&M

RMF Step 3 – Implement (1 of 2)

- DHA IV&V Pre-Kickoff Activities



RMF Step 3 – Implement (2 of 2)

- DHA IV&V Pre-Kickoff Activities
 - Security Assessment Plan (SAP) is developed by IV&V Team
 - Detailed roadmap on how to conduct the assessment
 - Initiate Self-Assessment scans (automated and manual checklists)
 - Upload scans to the Trend Analysis Database (TAD) ([TAD https://iaportal.health.mil](https://iaportal.health.mil)) and evaluate results
 - Remediate and develop mitigation strategies for N/C controls
 - Export final results to eMASS
 - Update/upload additional documents and evidence
 - Enter findings and proposed strategies in Risk Assessment Tab
- Completed A&A Readiness Checklist, submit 5 days prior to IV&V Kickoff
 - Several items listed on the checklist have already been submitted
 - This is a final sanity check to ensure system/application is ready
NOTE: At this point, all findings, mitigations and/or fixes should be in place. Next step is IV&V.

RMF Readiness (1 or 2)

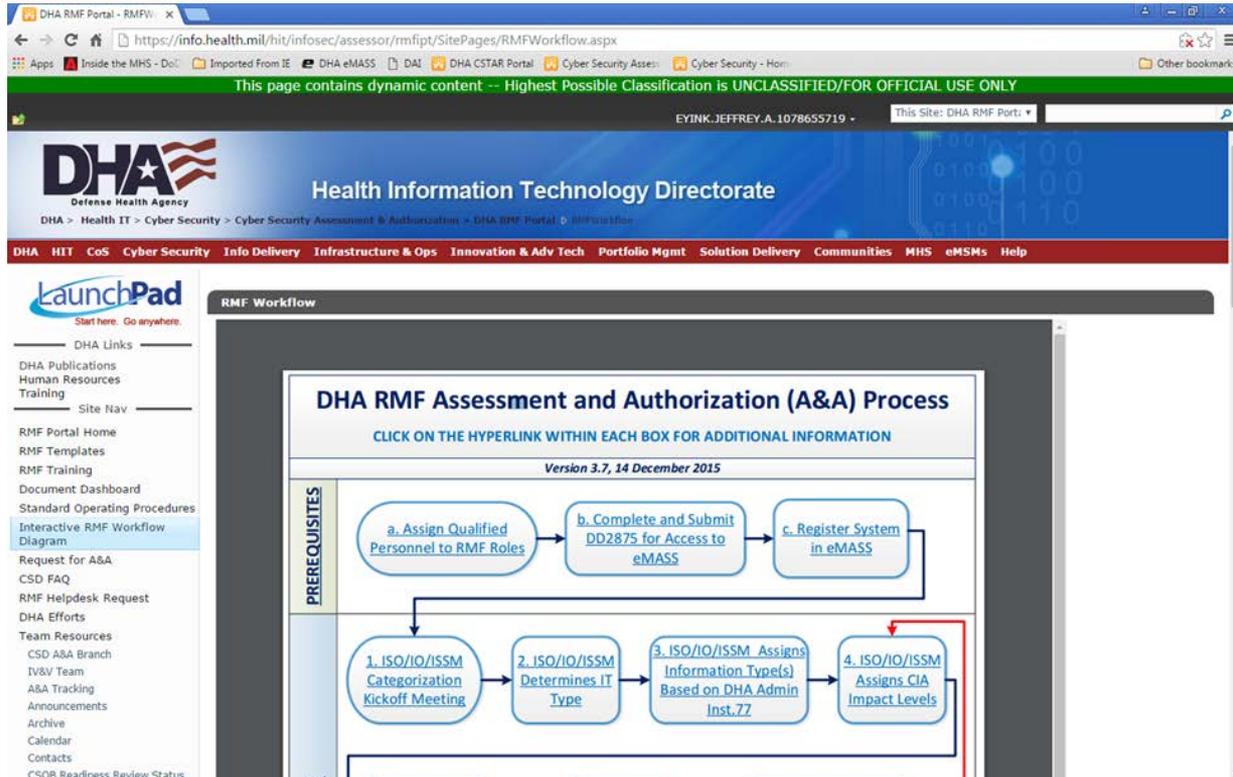
- Get DHA RMF and DISA eMASS Training
 - Schedule available on DHA RMF Portal or DISA IASE site
- Documents that need to be completed:
 - Hardware/Software Listings
 - Architecture Diagram
 - Ports, Protocols and Services Management
 - Privacy Impact Assessment
 - Continuous Monitoring Strategy
 - Security Plan
 - Contingency Plan
 - Configuration Management Plan
 - Incident Response Plan
 - System Interconnection Agreements (i.e., SLA, MOU)

RMF Readiness (2 of 2)

- Below are additional policies/procedures that are required, if not already included in the current requested documents. Templates are available.
- These could be Tier three System of Record Common Controls:
 - Information Assurance Vulnerability Management (IAVM) Program Plan
 - Cyber Security Training Plan
 - Audit Policy (AP)
 - Quality Assurance (QA)
 - Rules of Behavior (RoB)
 - Rules of Engagement (RoE)
 - Business Impact Analysis (BIA)

Links to Resources

- [RMF Knowledge Service \(https://rmfks.osd.mil\)](https://rmfks.osd.mil)
- [DHA Enterprise Mission Assurance Support Service \(https://emass-dha.csd.disa.mil\)](https://emass-dha.csd.disa.mil)
- [DHA RMF Portal \(https://info.health.mil/hit/infosec/assessor/rmfipt/SitePages/home.aspx\)](https://info.health.mil/hit/infosec/assessor/rmfipt/SitePages/home.aspx)
- [DISA Information Assurance Support Environment \(http://iase.disa.mil/Pages/index.aspx\)](http://iase.disa.mil/Pages/index.aspx)



The screenshot displays the DHA RMF Portal interface. At the top, a navigation bar includes the DHA logo and the text "Health Information Technology Directorate". Below this is a secondary navigation menu with categories like HIT, CoS, Cyber Security, and Info Delivery. The main content area features a "LaunchPad" sidebar on the left with various links. The central focus is the "RMF Workflow" section, which contains a flowchart titled "DHA RMF Assessment and Authorization (A&A) Process".

DHA RMF Assessment and Authorization (A&A) Process
CLICK ON THE HYPERLINK WITHIN EACH BOX FOR ADDITIONAL INFORMATION
Version 3.7, 14 December 2015

PREREQUISITES

- a. [Assign Qualified Personnel to RMF Roles](#)
- b. [Complete and Submit DD2875 for Access to eMASS](#)
- c. [Register System in eMASS](#)

Main Process Steps:

1. [ISO/IO/ISSM Categorization Kickoff Meeting](#)
2. [ISO/IO/ISSM Determines IT Type](#)
3. [ISO/IO/ISSM Assigns Information Type\(s\) Based on DHA Admin Inst.77](#)
4. [ISO/IO/ISSM Assigns CIA Impact Levels](#)

The flowchart shows a sequence of steps starting from the prerequisites, moving through the four main process steps, and then looping back to the prerequisites. A red arrow highlights the transition from step 4 back to the prerequisites.

SRG/STIG Applicability Guide and Collection Tool



Defense Health Agency

2016 Defense Health Information Technology Symposium

- Assist the user community in determining what SRGs and/or STIGs apply to a particular situation or Information System (IS) and to create a fully formatted document containing a “Collection” of SRGs and STIGs applicable to the situation being addressed
- [SRG/STIG Applicability Guide and Collection Tool \(http://iase.disa.mil/stigs/agct/Pages/index.aspx\)](http://iase.disa.mil/stigs/agct/Pages/index.aspx)

References

- CNSSI 1253, “Security Categorization and Control Selection for National Security Systems”, March 27, 2014
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, April 2013
- NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”, April 2010
- DoDI 8500.01, “Cybersecurity”, March 14, 2014
- DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT)”, March 12, 2014

Lessons Learned (1 of 2)

- Type Authorization must list locations in supporting document
- Re-evaluate Privacy Impact Analysis (PIA) with new or re-authorization
- PKI vulnerabilities determine if PKI/ASP extension is needed
- POA&M N/A controls must include explanation for N/A
- All Implementation Plan fields must be completed
 - Estimate completion date, future date system will become Compliant
 - Status of N/A must include explanation for N/A
- Each Control/CCI in System Main Tab must have responses
- Review Assessment Procedure (AP) list and document detailed responses for:
 - AP status: Compliant/Non-Compliant/Not Applicable
 - Include Test Results and Artifacts
 - Add/link Artifact to CCI

Lessons Learned (2 of 2)

- Develop POA&M Mitigation Strategies from Self-Assessment
- Gather False Positive evidence early (screenshots)
- Documentation review and comments (address each comment)
- Review SLA and update to RMF if applicable
- External Inheritance is selected when System of Record (SOR) has not been established for inheritance; SLA/MOA must be provided as evidence
- When PHI/PII is stored on system without encryption (SC-28)
- Information Owner must be notified through the Memo
 - Information Owner Memo Template is available on the DHA RMF Portal in the DHA RMF Templates folder
 - POA&M must also document risk/mitigation/milestones
 - When template is not used, add SCA and AO signature blocks to memo
 - [DHA RMF Templates folder](https://info.health.mil/hit/infosec/assessor/rmfip/ SitePages/home.aspx)
<https://info.health.mil/hit/infosec/assessor/rmfip/ SitePages/home.aspx>

Summary

- RMF Workflow
 - Categorization
 - Selection
 - Overlays Benefits
 - Implementation
 - Assess
 - Authorize
 - Monitor
- Benefits of implementing the Privacy Overlay
- RMF Readiness
- Resources

Key Takeaways

- Six steps to RMF are integrated in to the DHA Assessment and Authorization workflow
- Organizations need to be prepared for the Assessment of the Application/System/Enclave
- Use the DHA RMF Portal for resources to help with the A&A process

Questions?



“Medically Ready Force...Ready Medical Force”

RMF Role Acronyms

- Authorizing Official (AO)
- Authorizing Official Designated Representative (AODR)
- Chief Information Officer (CIO)
- Common Control Provider (CCP)
- Designated Approval Authority (DAA)
- Information Owner (IO)
- Information System Owner (ISO)
- Information System Security Manager (ISSM)
- Information System Security Officers (ISSO)
- Mission Owner (MO)
- Program Manager/System Manager (PM/SM)
- Security Control Assessor (SCA)
- Security Control Assessor Representative (SCAR)
- Component Senior Information Security Officer (SISO)

RMF Acronyms

- Assessment & Authorization (A&A)
- Assured Compliance Assessment Solution (ACAS)
- Authorization Decision Document (ADD)
- Authorization Termination Date (ATD)
- Authorization to Operate (ATO)
- Control Correlation Identifier (CCI)
- Committee on National Security Systems Instruction (CNSSI)
- Continuous Monitoring Risk Strategy (CMRS)
- Enterprise Mission Assurance Support Service (eMASS)
- Independent Verification and Validation (IV&V)
- Host Based System Security (HBSS)
- Memorandum of Understanding (MOU)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Platform Information Technology (PIT)
- Plan of Action and Milestones (POA&M)
- Risk Assessment Report (RAR)
- Risk Management Framework (RMF)
- Security Authorization Package (SAP)
- Security Assessment Report (SAR)
- Security Control Assessments (SCA)
- Service Level Agreement (SLA)
- Security Plan (SP)

Other Acronyms

- Defense Enterprise Computing Center (DECC)
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Defense Information Systems Agency (DISA)
- Information Assurance Support Environment (IASE)
- National Institute of Standards and Technology (NIST)
- Privacy Impact Assessment (PIA)
- Public Key Infrastructure/Authentication Security Plan (PKI/ASP)
- Security Content Automation Protocol (SCAP)
- Security Technical Implementation Guide (STIG)
- Special Publication (SP)

Evaluations

Please complete your evaluations

Contact Information

Jeffrey Eyink
Chief, Assessment and Authorization
Branch/Cybersecurity Division
jeffrey.a.eyink.civ@mail.mil