BAI Information Security Consulting & Training

Risk Management Framework (RMF) Resource Center

1-800-RMF-1903 (763-1903)

www.rmf.org

RMF for DoD IT
Training Program Overview & Outline

Training Overview

The RMF for DoD IT training program is suitable for DoD employees and contractors. This training program emphasizes the transition now taking place at DoD from DIACAP to RMF. The full program consists of a one-day *RMF for DoD IT Fundamentals* class, followed by a three-day *RMF for DoD IT In Depth* class.

- *RMF for DoD IT Fundamentals* (One Day) provides an overview of information security and risk management and proceeds to a high-level view of RMF for DoD IT. Discussion is centered on RMF for DoD IT policies, roles and responsibilities, along with key publications from the National Institute of Standards and Technology (NIST) and the Committee on National Security Systems (CNSS). The class includes high-level discussion of the RMF for DoD IT "life cycle", including security authorization (aka. certification and accreditation), along with the RMF documentation package and NIST security controls.

- *RMF for DoD IT In-Depth* (Three Days) expands on these topics at a level of detail that enables practitioners to immediately apply the training to their daily work. Each student will gain an in depth knowledge of the relevant DoD, NIST and CNSS publications along with the practical guidance needed to implement them in the work environment. Each life cycle activity in the DoD Instruction 8510.01 (RMF for DoD IT) is covered in detail, as is each component of the corresponding documentation package. NIST Special Publication (SP) 800-53 Security Controls, along with corresponding assessment procedures, are covered in detail, as are CNSS Instruction 1253 "enhancements". Specific attention is paid to the process of transition from DIACAP to RMF, as well as the application of the eMASS tool to various aspects of the RMF life cycle. "Class participation" exercises and collaboration reinforce key concepts. *RMF for DoD IT Fundamentals* is recommended as a "prerequisite" to *RMF for DoD IT In-Depth.*

Who should attend?

The RMF for DoD IT training program is suitable for DoD employees and contractors, as well as their supporting vendors and service providers. Managers and others who wish to gain high-level knowledge of RMF should attend RMF for DoD IT Fundamentals (one day). Those who wish to gain detailed implementation knowledge of RMF and NIST Security Controls should attend both RMF for DoD IT Fundamentals and RMF for DoD IT In Depth (total of four days).

BAI Information Security Consulting & Training

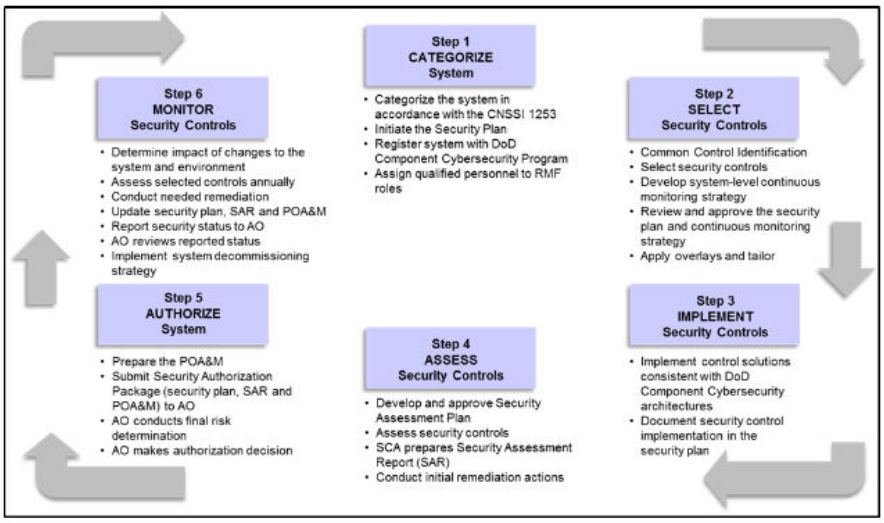
Risk Management Framework (RMF) Resource Center

1-800-RMF-1903 (763-1903)

www.rmf.org

RMF for DoD IT
Training Program Overview & Outline

RMF for DoD IT – Fundamentals (One-Day Course)



- Getting Started
- Policy Background: FISMA, OMB A-130, NIST Publications (FIPS and SP), DoDI 8500.01, 8510.01
- Introduction to RMF
- Roles and Responsibilities
- RMF Life Cycle: Categorize, Select, Implement, Assess, Authorize, Monitor
- RMF Documentation
- Security Controls and Assessment Procedures
- RMF and DIACAP
- RMF Resources

RMF for DoD IT – In Depth (Three-Day Course)

INSTRUCTIONAL UNITS*

Information on DIACAP-to-RMF transition and application of eMASS are included throughout these instructional units

- Getting Started
  - Course Information
  - DoD Primary Resources
- Step 1: Categorize
  - Categorize the System
  - Describe the System and Boundary
  - Conduct a Basic Risk Assessment
  - Register the System
- Step 2: Select
  - RMF Security Control Overview
  - Analyze Security Controls
  - Select the Control Baseline
  - Tailor the Control Baseline
  - Planning for Continuous Monitoring
- Step 3: Implement
  - Implement Control Solutions
  - Document Security Control Implementation
  - STIGs and Automated Tools
- Step 4: Assess
  - Identify Security Control Assessment Team
  - Prepare for the Security Assessment
  - Security Control Assessment Procedures
- Step 5: Authorize
  - Types of Authorizations
  - Authorization Decisions
  - Security Authorization Package
  - Documentation
- Step 6: Monitor
  - ISCM Strategy Considerations
  - Automated Tools
  - System Decommissioning and Removal
- Project Planning
  - Preparing for Success
  - System Acquisition
  - Knowledge Service

CLASS ACTIVITY HIGHLIGHTS*

- Informal Risk Assessment
- Propose a Boundary
- Categorize the System
- Identify Security Control Requirements
- Allocate Security Controls
- Identify Applicable Overlays
- Write Justification Statements for Non-applicable Controls
- Propose Criteria and Frequencies for Continuous Monitoring
- Write Control Implementation Statements
- Identify Security Control Assessment Methods
- Transition Plan
  - Identify Stakeholders
  - Prepare for Project Kick-off Meeting
  - Prepare for Project Activities, Timelines and Participants

---

* RMF publications covered in this training program include: DoDI 8500.01, 8510.01; CNSSI 1253, FIPS 199, 200; NIST SP 800-18, 800-30, 800-37, 800-39, 800-53, 800-53A, 800-59, 800-60, 800-137 and more.