BAI Information Security Consulting & Training

Risk Management Framework (RMF) Resource Center

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

www.rmf.org

# RMF for Federal Agencies
## Training Program Overview

## Training Overview

The **Risk Management Framework (RMF) for Federal Agencies** training program is suitable for federal employees and contractors in Federal "Civil" departments/agencies and the intelligence community. This training program provides a comprehensive working knowledge of RMF, including government policies and procedures, along with the practical guidance needed to successfully implement them. The full four-day program consists of **RMF for Federal Agencies Fundamentals** (one day), followed by **RMF for Federal Agencies In Depth** *(*three days*).*

- **RMF for Federal Agencies Fundamentals** (Day 1) provides an overview of information security and risk management and proceeds to a high-level view of FISMA regulations, roles, and responsibilities, and NIST RMF process steps, including security authorization (aka. certification and accreditation). It also includes an introduction to the NIST RMF documentation package and the NIST security controls.

- **RMF for Federal Agencies In Depth** (Days 2-4) 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 NIST publications along with the practical guidance needed to implement them in his/her environment. Each activity in the NIST SP 800-37 Rev 2 Risk Management Framework is covered in detail, as is each component of the documentation package. NIST SP 800-53 (Rev 4 and Rev 5) Security Controls and NIST 800-53a Assessment Procedures are covered in detail, as are CNSSI 1253 "enhancements" applicable to National Security Systems (NSS) and the intelligence community. "Class participation" exercises and collaboration reinforce key concepts.

## Who should attend?

The **RMF for Federal Agencies** training program is suitable for employees and contractors of federal "civil" departments/agencies and the intelligence community, as well as their supporting vendors and service providers. The full four-day program is recommended for most students. Managers and others who need only high-level knowledge of RMF have the option of attending just the **RMF for Federal Agencies Fundamentals** (one day).

## How to register

**RMF for Federal Agencies** is offered on a regularly-scheduled basis in online, instructor-led classes, using our Online Personal Classroom™ technology. For class schedule, registration and payment options, please visit register.rmf.org.

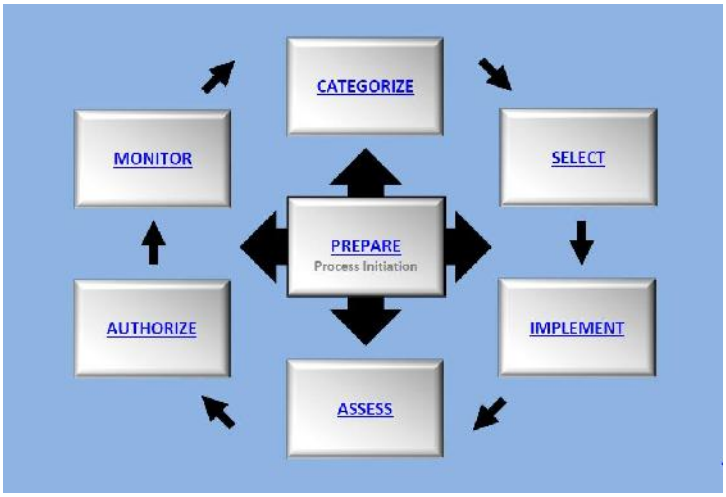
## Group classes

If you have a group of 8 or more students, we can arrange a private group class, either at your site or through our Online Personal Classroom™, with substantial savings over "per student" registration. Please contact BAI at 1-800-RMF-1903 or e-mail rmf@rmf.org.

BAI Information Security Consulting & Training
Risk Management Framework (RMF) Resource Center
1-800-RMF-1903 (763-1903)
www.rmf.org

# RMF for Federal Agencies
Training Program Outline

## RMF for Federal Agencies Fundamentals (Day 1)




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

## RMF for Federal Agencies In Depth (Days 2-4)

### INSTRUCTIONAL UNITS

- Getting Started
  - Course Information
  - 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: FIPS 199, 200; CNSSI 1253; NIST SP 800-18, 800-30, 800-37, 800-39, 800-53, 800-53A, 800-59, 800-60, 800-137 and more.