800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Risk Management Framework (RMF) Training

Applied Technology Academy

Federal agencies and contractors face increasing pressure to secure systems while staying compliant with evolving cybersecurity standards. This training offers a hands-on introduction to the latest updates to the Risk Management Framework (RMF), guiding participants through each step of the process—from system categorization and control selection to assessment, authorization, and continuous monitoring. The course emphasizes how RMF supports secure system development and risk-informed decision-making across the federal IT landscape.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**NIST SP 800-37 and SP-800-53**	**$124,610**	**Yes**

Course Overview

Learners will explore how recent changes in NIST guidance and federal policy affect RMF implementation, and how to apply these updates in practical, real-world scenarios. Through examples, exercises, and discussion, participants will gain a deeper understanding of how to collaborate with stakeholders, streamline documentation, and leverage automation to improve efficiency and outcomes.

Ideal for federal employees, contractors, and IT professionals working with government systems, this course is especially valuable for those in roles like ISSO, SCA, or anyone involved in system authorization and compliance. By the end, learners will be equipped to confidently support RMF activities and contribute to a stronger cybersecurity posture within their organization.

Understand the purpose and structure of the Risk Management Framework (RMF) and how it supports federal cybersecurity initiatives.

Identify and explain each step of the RMF process, including categorization, control selection, implementation, assessment, authorization, and continuous monitoring.

- Apply updated NIST guidance and federal policies to real-world RMF implementation scenarios.
- Recognize key roles and responsibilities within the RMF process, including those of the ISSO, SCA, and Authorizing Official.
- Use tools and templates to document RMF activities effectively and support system authorization packages.
- Collaborate with stakeholders to ensure security is integrated throughout the system development lifecycle.
- Leverage automation and continuous monitoring strategies to maintain system security and compliance.
- Prepare for and support system authorization efforts in alignment with current federal standards.

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Course Outline

- **Chapter 1: RMF overview**
  - Module A: Introduction to RMF
  - Module B: Cybersecurity policy regulations and framework
  - Module C: RMF roles and responsibilities
- **Chapter 2: Risk analysis**
  - Module A: Risk management
  - Module B: Risk assessment and the RMF process
- **Chapter 3: The RMF process**
  - Module A: Step 0—Prepare
  - Module B: Step 1—Categorize
  - Module C: Step 2—Select
  - Module D: Step 3—Implement
  - Module E: Step 4—Assess
  - Module F: Step 5—Authorize
  - Module G: Step 6—Monitor

Intended Audience

This course is designed for professionals who work with or support federal information systems and need a solid understanding of the Risk Management Framework. Ideal learners include:

- Information System Security Officers (ISSOs) who are responsible for overseeing system security and ensuring RMF compliance.
- Security Control Assessors (SCAs) and other assessment personnel who evaluate the effectiveness of security controls.

System Owners and Program Managers who need to understand how RMF fits into the system development lifecycle and impacts project planning.

Federal contractors and consultants supporting agencies with cybersecurity, compliance, or system authorization efforts.

IT professionals and engineers transitioning into federal cybersecurity roles or seeking to strengthen their understanding of federal risk management practices.

New hires or career changers entering the federal cybersecurity space who need foundational knowledge of RMF and its practical application.

This course is especially valuable for those working in or with civilian agencies, DoD environments, or any organization subject to federal cybersecurity requirements.

Prerequisites

- Basic understanding of cybersecurity concepts such as threats, vulnerabilities, and controls.
- Familiarity with federal IT environments or general knowledge of how government systems are developed and managed.
- Experience with system documentation or compliance processes is helpful but not required.
- Comfort with reading and interpreting policy or technical guidance, especially NIST publications like SP 800-37 and SP 800-53.

Follow-On Courses

Certified in Governance Risk and Compliance (CGRC)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.