Federal Risk Management Framework (RMF) Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

Learn how to confidently implement the updated Federal Risk Management Framework to support secure, compliant systems across the federal IT landscape.

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 2025 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.

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.

Who Should Attend?

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

Federal Risk Management Framework (RMF) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- 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.

What You Will Learn

- 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.

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

Federal Risk Management Framework (RMF) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700