301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

CYBERPHOENIX

Federal Risk Management Framework (RMF) 2.0 Training Certification

Federal Risk Management Framework (RMF) 2.0 Implementation DoD/IC Edition focuses on the Risk Management Framework prescribed by NIST Standards. This edition focuses on RMF as implemented within the Department of Defense (DoD) and Intelligence Communities (IC).

Course Overview

Risk Management Framework (RMF) is the unified information security framework for the entire federal government that is replacing the legacy Certification and Accreditation (C&A) processes within federal government departments and agencies, the Department of Defense (DOD) and the Intelligence Community (IC). DoD officially began its transition from the legacy DIACAP process to the new “RMF for DoD IT” process.

This course can also be used to aid in preparation for the ISC2 Certified Authorization Professional (CAP) exam, although it does not cover 100% of the CAP exam requirements. If your goal is primarily to prepare for the CAP Exam, you should use our course, Federal Risk Management Framework (RMF) 2.0 Implementation with CAP Exam Review.

This course is current as of March 2019. It was revised due to NIST producing new and updated publications over the preceding two years, including SP 800-37, rev. 2; SP-800-53, rev. 5; SP 800-160, V1 and V2; and SP 800-171, rev. 1 among others. It was also revised due to additional DoD updates to DODI 8510.01. D

The course comes with a disk of reference materials including sample documents, NIST publications, and regulatory documents. Downloadable ancillary materials include a study guide and a References and Policies handout. Instructors will also be given access to an exam with answer key.

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Course Objectives

- Understand the Risk Management Framework for DoD IT Authorization process
- Understand FISMA and NIST processes for authorizing Federal IT systems
- Explain key roles and responsibilities
- Explain statutory and regulatory requirements
- Apply these principles to real-world activities and situations

Course Outline

Introduction

- RMF overview
- DoD- and IC- Specific Guidelines
- Key concepts including assurance, assessment, authorization
- Security controls

Cybersecurity Policy Regulations & Framework

- Security laws, policy, and regulations
- DIACAP to RMF
- System Development Life Cycle (SLDC)
- Documents for cyber security guidance

RMF Roles and Responsibilities

- Tasks and responsibilities for RMF roles

Risk Analysis Process

- Overview of risk management
- Four-step risk management process
- Tasks breakdown
- Risk assessment reporting and options

Step 1 – Categorize

- Step key references and overview
- Sample SSP
- Task 1-1: Security Categorization
- Task 1-2: Information System Description
- Task 1-3: Information System Registration
- Lab: The Security Awareness Agency

Step 2 – Select

- Step key references and overview
- Task 2-1: Common Control Identification
- Task 2-2: Select Security Controls
- Task 2-3: Monitoring Strategy
- Task 2-4: Security Plan Approval
- Lab: Select Security Controls

Step 3 – Implement

- Step key references and overview
- Task 3-1: Security Control Implementation
- Task 3.2: Security Control Documentation
- Lab: Security Control Implementation

Step 4 – Assess

- Step key references and overview
- Task 4-1: Assessment Preparation
- Task 4-2: Security Control Assessment
- Task 4-3: Security Assessment Report
- Task 4-4: Remediation Actions
- Task 4-5: Final Assessment Report
- Lab: Assessment Preparation

Step 5 – Authorize

- Step key references and overview

- Task 5-1: Plan of Action and Milestones
- Task 5-2: Security Authorization Package
- Task 5-3: Risk Determination
- Task 5-4: Risk Acceptance DoD Considerations
- Lab Step 5: Authorize Information Systems

Step 6 – Monitor

- Step key references and overview
- Task 6-1: Information System & Environment Changes
- Task 6-2: Ongoing Security Control Assessments
- Task 6-3: Ongoing Remediation Actions
- Task 6-4: Key Updates
- Task 6-5: Security Status Reporting
- Task 6-6: Ongoing Risk Determination & Acceptance
- Task 6-7: Information System Removal & Decommissioning
- Continuous Monitoring
- Security Automation Domains
- Lab: Info System & Environment Changes

DoD/IC RMF Implementation

- eMASS
- RMF Knowledge Service
- DoD/IC Specific Documentation
- RMF within DoD and IC process review

RMF Training FAQs

Who should take this course?

This course is designed for system owners, administrators, developers, integrators, and information assurance staff who need to understand
FISMA, RMF process (including Security Authorization or A&A), NIST baseline security controls, documentation package, and continuous monitoring process.

What is the recommended experience for this course?

Students should have knowledge and experience with information security systems and best practices.

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Included in this **Federal Risk Management Framework (RMF) 2.0 Training Certification**

- 4 days instructor-led training
- Federal Risk Management Framework (RMF) 2.0 Training Certification training book
- Eligible for MyCAA scholarship
- RMF follows NICE framework for the Securely Provision job category
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*