Document Generated: 12/18/2025

Learning Style: Virtual Classroom

Technology:

Difficulty: Intermediate

Course Duration: 4 Days

Federal Risk Management Framework (RMFR-R40-CC) Implementation 4.0 and CAP Exam Prep (RMFR-R40-CC)

About this course:

The course Federal Risk Management Framework (RMF) implementation 4.0 is designed around the Risk Management framework prescribed by NIST Standards. It also covers the goals and objectives of ISC2 Certified Authorization Professional (CAP) certification exam.

This latest 4.0 edition updated as of August 2017, incorporates the revisions to NIST Special Publications (SP 800-160, 800-171, 800-53, etc.), the development and publication of the CNSSI-1253, change 2 and CNSSI-1254 for the IC, additional NIST Special Publications produced to support RMF steps and activities, and the passage of FISMA 2014, as well as practical experience as SCA and ISSE for over 10 ATO efforts under RMF over the past several years. It is beneficial in cyber security training.

The courseware is quite comprehensive; it can also be used by students preparing for ISC2 Certified Authorization Professional (CAP) certification exam. All CAP exam topics are mentioned within every chapter. Downloadable material such as

guides and handouts of policies and references are included. A disk is also provided with the course which covers all the reference materials, NIST publications, sample documents and rules book. An exam with answer key for instructors is also part of the course.

Course Outline:

Introduction

- Introductions
- About the CAP exam
- Table of Contents

Chapter 1: Introduction

- RMF overview
- Key concepts including assurance, assessment, authorization
- Security controls

Chapter 2: Cybersecurity Policy Regulations and Framework

- Security laws, policy, and regulations
- Documents for cyber security guidance
- Assessment and Authorization transformation goals

Chapter 3: RMF Roles and Responsibilities

- Tasks and responsibilities for RMF roles

Chapter 4: Risk Analysis Process

- Four-step risk management process
- Impact level
- Level of risk
- Effective risk management options

Chapter 5: Step 1: Categorize

- Step 1 key references
- Sample SSP
- Task 1-1: Security Categorization
- Task 1-2: Information System Description
- Task 1-3: Information System Registration
- Lab Step 1: Categorize

Chapter 6: Step 2: Select

- Step 2 key references
- Task 2-1: Common Control Identification
- Task 2-2: Select Security Controls

- Task 2-3: Monitoring Strategy
- Task 2-4: Security Plan Approval
- Lab Step 2: Select Security Controls

Chapter 7: Step 3: Implement

- Step 3 key references
- Task 3-1: Security Control Implementation
- Task 3.2: Security Control Documentation
- Lab Step 3: Implement Security Controls

Chapter 8: Step 4: Assess

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

Chapter 9: Step 5: Authorize

- Step 5 key references
- Task 5-1: Plan of Action and Milestones
- Task 5-2: Security Authorization Package
- Task 5-3: Risk Determination
- Task 5-4: Risk Acceptance
- Lab Step 5: Authorizing Information Systems

Chapter 10: Step 6: Monitor

- Step 6 key references
- Task 6-1: Information System and 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 and Acceptance
- Task 6-7: Information System Removal and Decommissioning
- Continuous Monitoring
- Security Automation Domains
- Lab Step 6: Monitoring Security Controls

Reference

- RMF process review
- RMF step checklists
- Acronym reference
- Review question answer key
- Lab question answer key