Federal Risk Management Framework (RMF) 2.0 Implementation, DoD/IC Edition R2.0 (4 Days)

Course Description

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).

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.

Downloadable ancillary materials include a study guide and a References and Policies handout.

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.

Course Outline

Chapter 1: Introduction

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

Chapter 2: Cybersecurity Policy Regulations & Framework

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

Chapter 3: RMF Roles and Responsibilities

- Tasks and responsibilities for RMF roles

Chapter 4: Risk Analysis Process

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

Chapter 5: 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

Chapter 6: 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

Chapter 7: Step 3: Implement

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

Chapter 8: 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