Federal Risk Management Framework (RMF) 2.0 Implementation, With CAP Exam Review R1.1

Days: 4

Prerequisites: There are no specific prerequisites for this course. However, general computer user knowledge is assumed. Any additional experience having worked with forms and/or databases will be helpful.

Audience: It is intended to support risk management framework (RMF) & CAP assessment and accreditation.

Description: Federal Risk Management Framework (RMF) 2.0 Implementation with CAP Exam Review focuses on the Risk Management Framework prescribed by NISTStandards. This course can also be used to aid in preparation for the ISC2 Certified Authorization Professional (CAP) exam, as it covers 100% of the CAP exam requirements.

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 to incorporate ISC2's update to the CAP Exam criteria and domain content in October 2018.

The printed book comes with a CD of reference materials including sample documents, NIST publications, and regulatory documents. Downloadable ancillary materials include a study guide and a references and policies handout. Verified instructors will also be given access to a sample CAP exam with answer key.

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

Federal Risk Management Framework (RMF) 2.0 Implementation, With CAP Exam Review R1.1

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

CHAPTER 9: 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

CHAPTER 10: 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
- Appendix A: Supplement Reference
- Appendix B: RMF/CAP Review and Step Checklist
- Appendix C: Acronym Reference
- Appendix D: Answer Keys
- Answers to Review Questions
  Lab Exercise Answers