CAP: Certified Authorization Professional (ISC2)

Days: 4

Prerequisites: Individuals who have at least one full year of experience using the federal RMF or comparable experience gained from the ongoing management of information system authorizations such as ISO 27001

Audience: This course is designed for the information security practitioner who champions system security commensurate with an organization's mission and risk tolerance, while meeting legal and regulatory requirements, as well as preparing for the CAP certification exam.

Description: This course is designed for the information security practitioner who champions system security commensurate with an organization's mission and risk tolerance while meeting legal and regulatory requirements. The Certified Authorization Professional (CAP) certification course conceptually mirrors the National Institute of Standards and Technology (NIST) system authorization process in compliance with the Office of Management and Budget (OMB) Circular A-130, Appendix III.

OUTLINE:

DAY 1

CHAPTER 1: INTRODUCTION

- RMF overview
- DoD and Intelligence Community specific guidelines
- Key concepts including assurance, assessment, authorization
- Security controls

CHAPTER 2: CYBERSECURITY POLICY REGULATIONS AND FRAMEWORK

- Security laws, policy, and regulations
- DIACAP to RMF transition
- ICD 503
- CNSSI-1253
- SDLC and RMF
- Documents for cyber security guidance

CHAPTER 3: RMF ROLES AND RESPONSIBILITIES

- Tasks and responsibilities for RMF roles
- DoD RMF roles

CHAPTER 4: RISK ANALYSIS PROCESS

- DoD organization-wide risk management
- RMF steps and tasks
- RMF vs. C and A

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
- Registering a DoD sytem
- 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

CAP: Certified Authorization Professional (ISC2)

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
- About Assessment
- 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

CHAPTER 11: RMF FOR DOD AND THE INTELLIGENCE COMMUNITY

- eMASS
- RMF Knowledge Service
- DoD 8510.01
- DFAR 252.204-7012
- ICD 503
- CNSSI-1253
- FedRAMP
- RMF within DoD and IC process review

REFERENCE

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