OVERVIEW

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 CAP training course provides a comprehensive review of information systems security concepts and industry best practices, covering the 7 domains of the CAP CBK.

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CAP exam.

CERTIFIED AUTHORIZATION PROFESSIONAL (CAP)

COURSE OBJECTIVES

After completing this course, the participant will be able to:

- Describe the historical legal and business considerations that required the development of the Risk Management Framework (RMF), including related mandates.
- Identify key terminology and associated definitions.
- Describe the RMF components, including the starting point inputs (architectural description and organization inputs.
- Describe the core roles defined by the RMF, including primary responsibilities and supporting roles for each RMF step.
- Describe the core federal statutes, OMB directives, information processing standards (FIPS) and Special Publications (SP), and Department of Defense and Intelligence Community instructions that form the legal mandates and supporting guidance required to implement the RMF.
- Identify and understand the related processes integrated with the RMF.
- Identify key references related to RMF Step 1 – Categorize Information Systems.
- Identify key references related to RMF Step 2 – Select Security Controls.
- Identify key references related to RMF Step 3 – Implement Security Controls.
- Identify key references related to RMF Step 4 – Assess Security Controls.
- Identify key references related to RMF Step 5 – Authorize Information System.
- Identify key references related to RMF Step 6 – Monitor Security Controls.

TARGET STUDENT

The course is intended for students who have at least one full year of experience using the federal Risk Management Framework (RMF) or comparable experience gained from the ongoing management of information system authorizations, such as ISO 27001.

The CAP certification is an objective measure of the knowledge, skills, and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk and damage to assets or individuals. CAP is appropriate for commercial markets, civilian and local governments, and the U.S. Federal government, including the State Department and the Department of Defense (DoD). See CAP and DoD 8570. Job functions such as authorization officials, system owners, information owners, information system security officers, certifiers, and senior system managers are great fits as CAPs.

The ideal candidate should have the following experience, skills, or knowledge in:

- IT security
- Information assurance
- Information risk management
- Certification
- Systems administration
- One to two years of general technical experience
- Two years of general systems experience
- One to two years of database/systems development/network experience
- Information security policy
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or health care industries, and/or auditing firms
- Strong familiarity with NIST documentation.

COURSE CONTENT

Lesson 1: Risk Management Framework (RMF)

Lesson 2: Categorization of Information Systems

Lesson 3: Selection of Security Controls

Lesson 4: Security Control Implementation

Lesson 5: Security Control Assessment

Lesson 6: Information System Authorization

Lesson 7: Monitoring of Security Controls