

# Certified Authorization Professional (CAP) Boot Camp - \$4295



Length: 5 days

Format: Bootcamp

Time: Day



## About This Course

Take your commitment to security assessment and authorization to a new level with the CAP certification. This leading information security certification proves you're an expert aligning information systems with the Risk Management Framework (RMF). The CAP certification covers the RMF at an extensive level. And it's the only certification under the DoD8570 Mandate that aligns to each of the RMF steps.

The CAP shows you have the knowledge, skills and abilities to authorize and maintain information systems within the RMF. Specifically, it validates that you know how to formalize processes to assess risk and establish security documentation throughout the entire lifecycle of a system.

## Required Exams

CAP Certification exam

## Audience Profile

The CAP is ideal for IT, information security and information assurance practitioners and contractors who use the RMF in:

- \* The U.S. federal government, such as the U.S. Department of State or the Department of Defense (DoD)
- \* The military
- \* Civilian roles, such as federal contractors
- \* Local governments
- \* Private sector organizations

## Course Objectives

This official (ISC)2 training is based on the seven domains found on the Common Body of Knowledge (CBK) for CAP, ensuring students successfully prepare for the CAP certification exam while also enhancing their overall competencies in authorizing and maintaining information systems.

- \* Domain 1: Risk Management Framework (RMF)

- \* Domain 2: Categorization of Information Systems
- \* Domain 3: Selection of Security Controls
- \* Domain 4: Security Control Implementation
- \* Domain 5: Security Control Assessment
- \* Domain 6: Information Systems Authorization
- \* Domain 7: Monitoring of Security Controls

## Outline

**Domain 1: Risk Management Framework (RMF)** Security authorization includes a tiered risk management approach to evaluate both strategic and tactical risk across the enterprise. The authorization process incorporates the application of a Risk Management Framework (RMF), a review of the organizational structure, and the business process/mission as the foundation for the implementation and assessment of specified security controls. This authorization management process identifies vulnerabilities and security controls and determines residual risks. The residual risks are evaluated and deemed either acceptable or unacceptable. More controls must be implemented to reduce unacceptable risk. The system may be deployed only when the residual risks are acceptable to the enterprise and a satisfactory security plan is complete.

**CAP Training Objectives** \* Describe the Risk Management Framework(RMF)

- \* Describe and Distinguish between the RMF Steps
- \* Identify Roles and Define Responsibilities
- \* Understand and Describe How the RMF Process Relates to Key Factors
- \* Understand the Relationship between the RMF and System Development Life Cycle(SDLC)
- \* Understand Legal, Regulatory, and Other Security Requirements

**Domain 2: Categorization of Information Systems** Categorization of the information system is based on an impact analysis. It is performed to determine the types of information included within the security authorization boundary, the security requirements for the information types, and the potential impact on the organization resulting from a security compromise. The result of the categorization is used as the basis for developing the security plan, selecting security controls, and determining the risk inherent in operating the system.

**CAP Training Objectives** \* Categorize the System

- \* Describe the Information System
- \* Register the System

**Domain 3: Selection of Security Controls** The security control baseline is established by determining specific controls required to protect the system based on the security categorization of the system. The baseline is tailored and supplemented in accordance with an organizational assessment of risk and local parameters. The security control baseline, as well as the plan for monitoring it, is documented in the security plan (SP).

**CAP Training Objectives** \* Identify and Document Common Controls

- \* Select, Tailor, and Document Security Controls
- \* Develop Security Control Monitoring Strategy
- \* Review and Approve SP

**Domain 4: Security Control Implementation** The security controls specified in the security plan are implemented by taking into account the minimum organizational assurance requirements. The security plan describes how the controls are employed within the information system and its operational environment. The security assessment plan documents the methods for testing these controls and the expected results throughout the system's life-cycle.

**CAP Training Objectives**

- \* Implement Selected Security Controls

- \* Document Security Control Implementation

**Domain 5: Security Control Assessment** The security control assessment follows the approved plan, including defined procedures, to determine the effectiveness of the controls in meeting security requirements of the information system. The results are documented in the Security Assessment Report.

- \* Prepare for Security Control Assessment
- \* Develop Security Control Assessment Plan
- \* Assess Security Control Effectiveness
- \* Develop Initial Security Assessment Report (SAR)
- \* Review Interim SAR and Perform Initial Remediation Actions
- \* Develop Final SAR and Optional Addendum

**Domain 6: Information Systems Authorization** The residual risks identified during the security control assessment are evaluated and the decision is made to authorize the system to operate, deny its operation, or remediate the deficiencies. Associated documentation is prepared and/or updated depending on the authorization decision.

**CAP Training Objectives**

- \* Develop Plan of Action and Milestones (POAM)

- \* Assemble Security Authorization Package
- \* Determine Risk
- \* Determine the Acceptability of Risk
- \* Obtain Security Authorization Decision

**Domain 7: Monitoring of Security Controls** After an Authorization to Operate (ATO) is granted, ongoing continuous monitoring is performed on all identified security controls as well as the political, legal, and physical environment in which the system operates. Changes to the system or its operational environment are documented and analyzed. The security state of the system is reported to designated responsible officials. Significant changes will cause the system to re-enter the security authorization process. Otherwise, the system will continue to be monitored on an ongoing basis in accordance with the organization's monitoring strategy.

**CAP Training Objectives**

- \* Determine Security Impact of Changes to System and Environment

- \* Perform Ongoing Security Control Assessments
- \* Conduct Ongoing Remediation Actions
- \* Update Key Documentation
- \* Perform Periodic Security Status Reporting
- \* Perform Ongoing Risk Determination and Acceptance

\* Decommission and Remove System