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 youâ€™re an expert aligning information systems with the Risk Management Framework (RMF). The CAP certification covers the RMF at an extensive level. And itâ€™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) forCAP, ensuring students successfully prepare for the CAP certification exam while also enhancing their overallcompetencies 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 acceptableto the enterprise and a satisfactory security plan is complete.

CAP Training Objectives * Describe the Risk Management Framework(RMF)
* Describe and Distinguish between the RMFSteps
* Identify Roles and Define Responsibilities
* Understand and Describe How the RMFProcess Relates to Key Factors
* Understand the Relationship between theRMF and System Development Life Cycle(SDLC)
* Understand Legal, Regulatory, and OtherSecurity Requirements

Domain 2: Categorization of Information SystemsCategorization of the information system is based onan impact analysis. It is performed to determine thetypes of information included within the securityauthorization boundary, the security requirementsfor the information types, and the potential impacton the organization resulting from a securitycompromise. The result of the categorization is usedas the basis for developing the security plan,selecting security controls, and determining the riskinherent in operating the system.

CAP Training Objectives * Categorize the System
* Describe the Information System
* Register the System

Domain 3: Selection of Security ControlsThe security control baseline is established bydetermining specific controls required to protect thesystem based on the security categorization of thesystem. The baseline is tailored and supplemented inaccordance with an organizational assessment of riskand local parameters. The security control baseline,as well as the plan for monitoring it, is documentedin 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 ImplementationThe security controls specified in the security planare implemented by taking into account theminimum organizational assurance requirements.The security plan describes how the controls areemployed within the information system and itsoperational environment. The security assessmentplan documents the methods for testing thesecontrols and the expected results throughout thesystems life-cycle.

CAP Training Objectives * Implement Selected Security Controls
* Document Security Control Implementation

Domain 5: Security Control AssessmentThe 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 InitialRemediation Actions
* Develop Final SAR and Optional Addendum

Domain 6: Information Systems AuthorizationThe residual risks identified during the securitycontrol assessment are evaluated and the decision ismade to authorize the system to operate, deny itsoperation, or remediate the deficiencies. Associateddocumentation is prepared and/or updateddepending 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 ControlsAfter an Authorization to Operate (ATO) is granted,ongoing continuous monitoring is performed on allidentified security controls as well as the political,legal, and physical environment in which the systemoperates. Changes to the system or its operationalenvironment are documented and analyzed. Thesecurity state of the system is reported to designatedresponsible officials. Significant changes will causethe system to re-enter the security authorizationprocess. Otherwise, the system will continue to bemonitored on an ongoing basis in accordance withthe organization\'s monitoring strategy.

CAP Training Objectives * Determine Security Impact of Changes toSystem and Environment
* Perform Ongoing Security ControlAssessments
* Conduct Ongoing Remediation Actions
* Update Key Documentation
* Perform Periodic Security Status Reporting
* Perform Ongoing Risk Determination andAcceptance

* Decommission and Remove System