ProTech *"Charting the Course ...*

protechtraining.com

*... to Your Success!"*

# Certified Authorization Professional (CAP)

## Course Summary

**Description**

The Certified Authorization Professional (CAP) is an information security practitioner who champions system security commensurate with an organization's mission and risk tolerance, while meeting legal and regulatory requirements. CAP confirms an individual's knowledge, skill, and experience required for authorizing and maintaining information systems within the Risk Management Framework as outlined in NIST SP 800-37 Rev 1.

The broad spectrum of topics included in the CAP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 7 domains:

- Risk Management Framework (RMF)
- Categorization of Information Systems
- Selection of Security Controls
- Security Control Implementation
- Security Control Assessment
- Information System Authorization
- Monitoring of Security Controls

CAP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

CAP Examination Information

- Length of exam – 3 hours
- Number of questions – 125
- Question format – Multiple choice
- Passing grade – 700 out of 1000 points
- Exam availability – English
- Testing center – Pearson VUE Testing Center

**Topics**

- Risk Management Framework (RMF)
- Categorization of Information Systems
- Selection of Security Controls
- Security Control Implementation
- Security Control Assessment
- Information System Authorization
- Monitoring Security Controls

**Audience**

The CAP is ideal for IT, information security and information assurance practitioners, and contractors who use the Risk Management Framework (RMF). Many who pursue the CAP are:

- ISSOs, ISSMs and other infosec/information assurance practitioners who are focused on security assessment and authorization (traditional C&A) and continuous monitoring issues.
- Executives who must "sign off" on Authority to Operate (ATO).
- Inspector generals (IGs) and auditors who perform independent reviews.
- Program managers who develop or maintain IT systems.
- IT professionals interested in improving cybersecurity and learning more about the importance of lifecycle cybersecurity risk management.

**Prerequisites**

Before taking this course, candidates must have a minimum of 2 years cumulative paid full-time work experience in 1 or more of the 7 domains of the CAP CBK. A candidate that doesn't have the required experience to become a CAP may become an Associate of $(ISC)^2$ by successfully passing the CAP examination. The Associate of $(ISC)^2$ will then have 3 years to earn the 2 year required experience.

**Duration**

Two days

ProTech "Charting the Course ...

protechtraining.com

... to Your Success!"

# Certified Authorization Professional (CAP)

## Course Outline

**I. Risk Management Framework (RMF)**

A. Describe the Risk Management Framework (RMF)
   1. Distinguish between applying risk management principles and satisfying compliance requirements
   2. Identify and maintain information systems inventory
   3. Explain the importance of securing information
   4. Understand organizational mission and operations

B. Describe and Distinguish Between the RMF Steps
   1. Categorize information system
   2. Select security controls
   3. Implement security controls
   4. Assess security controls
   5. Authorize information system
   6. Monitor security controls

C. Identify Roles and Define Responsibilities
   1. Head of agency (Chief Executive Officer)
   2. Risk executive (Function)
   3. Chief information officer
   4. Information owner/steward
   5. Senior information security officer
   6. Authorizing official
   7. Authorizing official designated representative
   8. Common control provider
   9. Information system owner
   10. Information system security officer
   11. Information security architect
   12. Information system security engineer
   13. Security control assessor

D. Understand and Describe How the RMF Process Relates to:
   1. Organization-wide risk management
   2. Enterprise and information security architecture
   3. Information System boundaries
   4. Authorization decisions
   5. Security control assessor independence
   6. Security controls in external environments (e.g., third-party, cloud)
   7. Security control allocation (e.g., resources, common controls, component level)

E. Understand the Relationship between the RMF and System Development Life Cycle (SDLC)
   1. Promote security integration within SDLC (e.g., policy, procedures, standards)
   2. Collaborate with stakeholders (e.g., integrated project teams, architects, developers, management)

F. Understand Legal, Regulatory, and Other Security Requirements
   1. Federal information security and privacy legislation
   2. Office of Management and Budget (OMB)
   3. Committee on National Security Systems (CNSS)
   4. National Institute of Standards and Technology (NIST) publications

**II. Categorization of Information Systems**

A. Categorize the System
   1. Identify the information types
   2. Determine confidentiality, integrity, and availability values
   3. Determine potential impact on organizations and individuals
   4. Categorize information types
   5. Categorize information system
   6. Document categorization in the Security Plan (SP)
   7. Perform Privacy Threshold Analysis and Privacy Impact Assessment

# Certified Authorization Professional (CAP)

## Course Outline (cont'd)

B. Describe the Information System (Including the Security Authorization Boundaries)
C. Register the System

**III. Selection of Security Controls**
A. Identify and Document Common (Inheritable) Controls
B. Select, Tailor, and Document Security Controls
C. Develop Security Control Monitoring Strategy
D. Review and Approve SP

**IV. Security Control Implementation**
A. Implement Selected Security Controls
B. Document Security Control Implementation

**V. Security Control Assessment**
A. Prepare for Security Control Assessment
   1. Establish objectives and scope
   2. Establish points of contact, provide notifications and timelines
   3. Select security control assessor (e.g., independence, competency)
   4. Collect and review artifacts (e.g., previous assessments, system documentation, policies)
B. Develop Security Control Assessment Plan
   1. Determine security assessment methods and level of effort
   2. Obtain necessary approvals (e.g., security assessment plan, rules of engagement, resources)
C. Assess Security Control Effectiveness
   1. Apply standard assessment methods (e.g., examine, interview, test)
   2. Collect and inventory assessment evidence
D. Develop Initial Security Assessment Report (SAR)
   1. Analyze assessment results
   2. Determine root causes of identified weaknesses
   3. Propose remediation actions
E. Review Interim SAR and Perform Initial Remediation Actions
   1. Determine initial risk responses
   2. Apply initial remediations
   3. Reassess and validate the remediated controls
F. Develop Final SAR and Optional Addendum

**VI. Information System Authorization**
A. Develop Plan of Action and Milestones (POAM) (e.g., Resources, Schedule, Requirements)
B. Assemble Security Authorization Package
C. Determine Risk
D. Determine the Acceptability of Risk
E. Obtain Security Authorization Decision

**VII. Monitoring Security Controls**
A. Determine Security Impact of Changes to System and Environment
B. Perform Ongoing Security Control Assessments (e.g., continuous monitoring, internal and external assessments)
C. Conduct Ongoing Remediation Actions (resulting from incidents, vulnerability scans,
D. audits, vendor updates, etc)
E. Update Key Documentation (e.g., SP, SAR, POAM)
F. Perform Periodic Security Status Reporting
G. Perform Ongoing Risk Determination and Acceptance
H. Decommission and Remove System