View Full Course Details including Latest Schedule Online

(ISC)²

CAP Certification Training

Earning the (ISC)² CAP certification is a key factor in advancing within your Information Security career; it verifies an individual's skills and knowledge for implementing Risk Management Framework, identifying security controls and vulnerabilities for measuring organizational risks.

Course Overview

Our 3-day, instructor-led CAP (Certified Authorization Professional) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is aimed at information systems professionals responsible for making vital security decisions based on risk assessment. It covers seven domains:

1. Risk Management Framework (RMF)
2. Categorization of information systems
3. Selection of security controls
4. Implementation of security controls
5. Assessment of security controls
6. Information systems authorization
7. Monitoring of security control

This course will fully prepare you for the (ISC)²® CAP® Certification exam.

Before enrolling in the course, you should have at least two years of experience in one or more of the previously listed CAP® domains. You should also be familiar with NIST documentation.

Course Outline

This course provides an in-depth review of the seven domains that are covered in the (ISC)²® CAP exam. These are the domains and outline effective as of October 15th, 2018:

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Information Security Risk Management Program

- Understand the Foundation of an Organization-Wide Information Security Risk Management Program
- Principles of information security
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- RMF and System Development Life Cycle (SDLC) integration
- Information System (IS) boundary requirements
- Approaches to security control allocation
- Roles and responsibilities in the authorization process
- Understand Risk Management Program Processes
- Enterprise program management controls
- Privacy requirements
- Third-party hosted Information Systems (IS)
- Understand Regulatory and Legal Requirements
- Federal information security requirements
- Relevant privacy legislation
- Other applicable security-related mandates

Categorization of Information Systems (IS) Define the Information System (IS)

- Identify the boundary of the Information System (IS)
- Describe the architecture
- Describe Information System (IS) purpose and functionality
- Determine Categorization of the Information System (IS)
- Identify the information types processed, stored, or transmitted by the
- Information System (IS)
- Determine the impact level on confidentiality, integrity, and availability for each information type
- Determine Information System (IS) categorization and document results

Selection of Security Controls Identify and Document Baseline and Inherited Controls

- Select and Tailor Security Controls
- Determine applicability of recommended baseline
- Determine appropriate use of overlays
- Document applicability of security controls
- Develop Security Control Monitoring Strategy
- Review and Approve Security Plan (SP)

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Implementation of Security Controls Implement Selected Security Controls

- Confirm that security controls are consistent with enterprise architecture
- Coordinate inherited controls implementation with common control providers
- Determine mandatory configuration settings and verify implementation (e.g., United States Government Configuration Baseline (USGCB), National Institute of Standards and Technology (NIST) checklists, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) benchmarks)
- Determine compensating security controls
- Document Security Control Implementation
- Capture planned inputs, expected behavior, and expected outputs of security controls
- Verify documented details are in line with the purpose, scope, and impact of the Information System (IS)
- Obtain implementation information from appropriate organization entities (e.g., physical security, personnel security)

Assessment of Security Controls Prepare for Security Control Assessment (SCA)

- Determine Security Control Assessor (SCA) requirements
- Establish objectives and scope
- Determine methods and level of effort
- Determine necessary resources and logistics
- Collect and review artifacts (e.g., previous assessments, system documentation, policies)
- Finalize Security Control Assessment (SCA) plan
- Conduct Security Control Assessment (SCA)
- Assess security control using standard assessment methods
- Collect and inventory assessment evidence
- Analyze assessment results and identify weaknesses
- Propose remediation actions
- Review Interim Security Assessment Report (SAR) and Perform Initial Remediation Actions
- Determine initial risk responses
- Apply initial remediations
- Reassess and validate the remediated controls
- Develop Final Security Assessment Report (SAR) and Optional Addendum

Authorization of Information Systems (IS) Develop Plan of Action and Milestones (POAM)

- Analyze identified weaknesses or deficiencies

- Prioritize responses based on risk level
- Formulate remediation plans
- Identify resources required to remediate deficiencies
- Develop schedule for remediation activities
- Assemble Security Authorization Package
- Compile required security documentation for Authorizing Official (AO)
- Determine Information System (IS) Risk
- Evaluate Information System (IS) risk
- Determine risk response options (i.e., accept, avoid, transfer, mitigate, share)
- Make Security Authorization Decision
- Determine terms of authorization

Continuous Monitoring Determine Security Impact of Changes to Information System (IS) and Environment

- Understand configuration management processes
  Analyze risk due to proposed changes
  Validate that changes have been correctly implemented
  Perform Ongoing Security Control Assessments (SCA)
  Determine specific monitoring tasks and frequency based on the agency's strategy
  Perform security control assessments based on monitoring strategy
  Evaluate security status of common and hybrid controls and interconnections
  Conduct Ongoing Remediation Actions (e.g., resulting from incidents, vulnerability scans, audits, vendor updates)
  Assess risks
  Formulate remediation plans
  Conduct remediation tasks
  Update Documentation
  Determine which documents require updates based on results of the continuous monitoring process
  Perform Periodic Security Status Reporting
  Determine reporting requirements
  Perform Ongoing Information System (IS) Risk Acceptance
  Determine ongoing Information System (IS)
  Decommission Information System (IS)
  Determine Information System (IS) decommissioning requirements
  Communicate decommissioning of Information System (IS)

Exam Information

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

CAP Certification Exam Overview:

The CAP exam will test the breadth and depth of a student's knowledge by primarily focusing on the seven domains which make up the topics of CAP CBK®, taxonomy of information security:

1. Information Security Risk Management Program (15%)
2. Categorization of Information Systems (IS) (13%)
3. Selection of Security Controls (13%)
4. Implementation of Security Controls (15%)
5. Assessment of Security Controls (14%)
6. Authorization of Information Systems (IS) (14%)
7. Continuous Monitoring (16%)

CAP Certification Exam Details:

- Questions on the Exam: 125
- Score Needed to Pass: at least 700/1,000
- Duration of the Exam: 3 Hours
- Format of the Exam: multiple choice
- Delivery Details: The CAP exam is offered through the global network of Pearson VUE testing centers as a computer-based test.

CAP Certification Training FAQs

Who should take this class?

This certification is sought after by Authorization Officials, Information System Security Officers, Information Owners, System Owners and Senior System Managers.

What is the average salary with an (ISC)² CAP Certification?

According to payscale.com, professionals with the CAP certification earn an average salary of $100,000.

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

This **CAP Certification Training** course includes:

- 3 days of instructor-led training
- (ISC)² CAP practice exams
- (ISC)² CAP official CBK
- (ISC)² CAP Certification Training book
- Pre and post assessments
- CAP onsite exam scheduling
- Certificate of completion for up to 24 CEUs/CPEs to be used toward renewing relevant certifications
- CAP course retake guarantee
- CAP certification satisfies DOD 8570 IAM Level II
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

**denotes this benefit is only available at participating locations.*