Cyber Security Institute

CAP Boot Camp

Cyber Security's Certified Authorization Professional (CAP) Boot Camp focuses on preparing students for the CAP exam through extensive mentoring and drill sessions, review of all 7 CAP domains of knowledge, and practical question and answer scenarios, all through a high-energy seminar approach. This class is the product of a wide range of leading industry experts and authors, and our training materials are considered the absolute best for CAP preparation.

The Certified Authorization Professional (CAP) credential applies to professionals who need to setup the formal processes used to assess risk and establish security requirements based on regulatory standards. It's a very important job which ensures that information systems have appropriate security controls to mitigate potential risk, as well as protecting against damage to assets or individuals. The credential is sought after by civilian, state and local governments, as well as system integrators supporting these organizations.

Cyber Security's 3-Day CAP Boot Camp focuses on preparing students for the CAP exam through extensive mentoring and drill sessions, review of the entire body of knowledge, and practical question and answer scenarios, all through a high-energy seminar approach.

Cyber Security Institute

Course Objectives

Upon completing our 3 day CAP Boot Camp you will gain valuable knowledge and skills including the ability to:

- Understanding the Purpose of Information Systems Security Authorization
- Defining Systems Authorization
- Describing and Decide When Systems Authorization Is Employed
- Defining Roles and Responsibilities
- Understanding the Legal and Regulatory Requirements for C&A
- Initiating the Authorization Process
- Establishing Authorization Boundaries
- Determining Security Categorization
- Performing Initial Risk Assessment
- Selecting and Refining Security Controls
- Documenting Security Control
- Performing Certification Phase
- Assessing Security Control
- Documenting Results
- Conducting Final Risk Assessment
- Generating and Presenting an Authorization Report
- Performing Continuous Monitoring
- Monitoring Security Controls
- Monitoring and Assessing Changes That Affect the Information System
- Performing Security Impact Assessment As Needed
- Documenting and Monitoring Results of Impact Assessments

What's Included

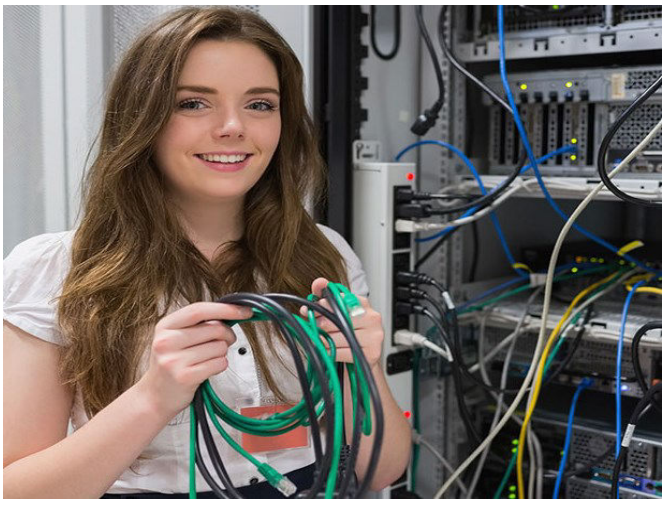
- Cyber Security Custom CAP Textbook with Review Questions
- Exam Review, In-Class Mentoring
- Pre-Shipment of Textbook
- Catered Lunch
- (ISC)2 Exam Fee
- Course Registration Fee
- Re-Sit Guarantee

Exam Pass Guarantee (Live-Online Only)

Prerequisites

To achieve the CAP credential, you need a minimum of two years of direct full-time information systems security authorization professional experience in one or more of these seven (ISC) CAP domains:

1. Risk Management Framework (RMF)
2. Categorization of Information Systems
3. Selection of Security Controls
4. Security Control Implementation
5. Security Control Assessment
6. Information System Authorization
7. Monitoring of Security Controls



Cyber Security Institute

Who Should Attend

Employees who perform functions such as authorization officials, system owners, information owners, information system security officers, and certifiers, as well as all senior system managers, can benefit from this training, including:

- System Administrators
- Information Security Professionals

Anyone involved in a NIST-based information systems security authorization process. Manage security, including basic firewall and SELinux configuration

Certification Exam

- Time Limit: 3 Hours
- Number of Questions: 125
- Question Format: Multiple Choice Questions

Passing Grade: 700 out of 1000 Points

CONTACT US :