BAI Information Security Consulting & Training
Risk Management Framework (RMF) Resource Center
1-800-RMF-1903 (763-1903)
www.rmf.org

Certified Authorization Professional (CAP) Exam Overview
Training Program Overview & Outline

Training Overview

This one-day day training program focuses on solidifying (ISC)2 CAP exam concepts covered in the RMF for DoD IT Training Program. It includes an overview of the CAP Common Body of Knowledge, including:

- Risk Management Framework (RMF)
- System Development Life Cycle (SDLC)
- Roles and Responsibilities
- Security Control Implementation/Assessment
- Key Publications

Practical "how to" guidance and sample questions are provided to enhance the students' exam readiness.

Note: BAI provides training and test preparation. The exam itself is administered by ISC2.

Introduction

Backed by (ISC)2, CAP credentialing aligns with the Risk Management Framework (RMF). The CAP recognizes knowledge, skills and abilities to authorize and maintain information systems within RMF. It demonstrates the ability to formalize processes to assess risk and establish security documentation.

Course Prerequisites

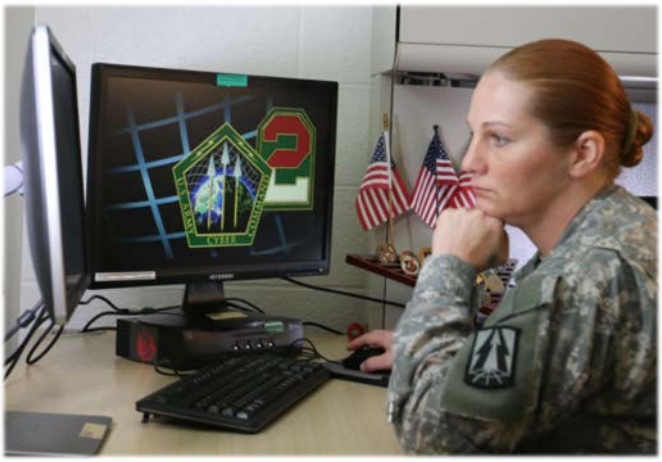
This training is intended to serve as an add-on to the RMF for DoD IT core curriculum which delivers the requisite content to sit for the CAP exam. It is expected that students enrolling in this course have completed RMF for DoD IT Fundamentals and RMF for DoD IT In-Depth.

Exam Prerequisites

CAP candidates must have two years of cumulative paid full-time experience in one or more of the seven domains of the CAP Common Body of Knowledge (CBK) to receive the CAP certification. If a candidate does not have enough work experience, they can take the CAP exam to earn an Associate of (ISC)2 designation.

Who Should Become a CAP

- U.S. federal government, such as DoD members
- Civilian roles, such as federal contractors
- Local government decision makers



CAP® Certified Authorization Professional

Certified Authorization Professional (CAP) Exam Overview – One-Day Course

- Risk Management Framework Review
- System Development Life Cycle (SDLC)
  - Initiation Phase
  - Development/Acquisition Phase
  - Implementation Phase
  - Operations & Maintenance Phase
  - Disposal Phase
  - RMF Alignment
- Roles and Responsibilities
- FISMA
- Key Publications
- Exam Structure
- Practice Question Workshop

Sample Questions

Which of the following objectives are defined by integrity in the C.I.A triad of information security systems? Each correct answer represents a part of the solution. Choose three.

A. It prevents the unauthorized or unintentional modification of information by the authorized users.
B. It preserves the internal and external consistency of information.
C. It prevents the intentional or unintentional unauthorized disclosure of a message's contents.
D. It prevents the modification of information by the unauthorized users.

Risk	Probability	Impact
A	0.55	-10,000
B	0.4	-65,000
C	0.3	-90,000
D	0.6	-25,000
E	0.45	-30,000
F	0.7	-245,000

What will be the expected monetary value of Risk C?

A. -$113,750
B. -$27,000
C. -$175,000
D. $175,000 if the risk event actually happens