CompTIA Certification

CASP+004: CompTIA CASP+ Certification Training (Exam CAS-004)

$2,795.00

- 5 Days
- Includes authorized courseware, practice tests, and hands-on labs.

Upcoming Dates

Course Description

This course can benefit you in two ways. If you intend to pass the CompTIA CASP+ (Exam CAS-004) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of cybersecurity. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your information security skill set so that you can confidently perform your duties as an advanced security practitioner.

Course Outline

Lesson 1: Performing Risk Management Activities

- Topic 1A: Explain Risk Assessment Methods
- Topic 1B: Summarize the Risk Life cycle
- Topic 1C: Assess & Mitigate Vendor Risk

Lesson 2: Summarizing Governance & Compliance Strategies

- Topic 2A: Identifying Critical Data Assets
- Topic 2B: Compare and Contrast Regulation, Accreditation, and Standards
- Topic 2C: Explain Legal Considerations & Contract Types

Lesson 3: Implementing Business Continuity & Disaster Recovery

- Topic 3A: Explain the Role of Business Impact Analysis
- Topic 3B: Assess Disaster Recovery Plans
- Topic 3C: Explain Testing and Readiness Activities

Lesson 4: Identifying Infrastructure Services

- Topic 4A: Explain Critical Network Services
- Topic 4B: Explain Defensible Network Design
- Topic 4C: Implement Durable Infrastructures

Lesson 5: Performing Software Integration

- Topic 5A: Explain Secure Integration Activities
- Topic 5B: Assess Software Development Activities
- Topic 5C: Analyze Access Control Models & Best Practices
- Topic 5D: Analyze Development Models & Best Practices

Lesson 6: Explain Virtualization, Cloud, and Emerging Technology

- Topic 6A: Explain Virtualization and Cloud Technology
- Topic 6B: Explain Emerging Technologies

Lesson 7: Exploring Secure Configurations and System Hardening

- Topic 7A: Analyze Enterprise Mobility Protections
- Topic 7B: Implement Endpoint Protection

Lesson 8: Understanding Security Considerations of Cloud and Specialized Platforms

- Topic 8A: Understand Impacts of Cloud Technology Adoption
- Topic 8B: Explain Security Concerns for Sector-Specific Technologies

Lesson 9: Implementing Cryptography

- Topic 9A: Implementing Hashing and Symmetric Algorithms
- Topic 9B: Implementing Appropriate Asymmetric Algorithms and Protocols

Lesson 10: Implementing Public Key Infrastructure (PKI)

- Topic 10A: Analyze Objectives of Cryptography and Public Key Infrastructure (PKI)
- Topic 10B: Implementing Appropriate PKI Solutions

Lesson 11: Understanding Threat and Vulnerability Management Activities

- Topic 11A: Explore Threat and Vulnerability Management Concepts
- Topic 11B: Explain Vulnerability and Penetration Test Methods
- Topic 11C: Explain Technologies Designed to Reduce Risk

Lesson 12: Developing Incident Response Capabilities

- Topic 12A: Analyzing and Mitigating Vulnerabilities
- Topic 12B: Identifying and Responding to Indicators of Compromise
- Topic 12C: Exploring Digital Forensic Concepts

Audience

The Official CompTIA CASP+ Guide (Exam CAS-004) is the primary course you will need to take if your job responsibilities include risk management, enterprise security operations, security engineering and security architecture, research and collaboration, and integration of enterprise security. You can take this course to prepare for the CompTIA CASP+ (Exam CAS-004) certification examination.

Prerequisites

To ensure your success in this course, you should have minimum of ten years of general hands-on IT experience, with at least five of those years being broad hands-on IT security experience. CompTIA Network+, Security+, CySA+, Cloud+, and PenTest+ certification, or the equivalent knowledge, is strongly recommended.

What You Will Learn

On course completion, you will be able to:

- Perform risk management activities.
- Summarize governance and compliance strategies.
- Implement business continuity and disaster recovery.
- Identify infrastructure services.
- Perform software integration.
- Explain virtualization, cloud, and emerging technology.
- Explore secure configurations and system hardening.
- Understand security considerations of cloud and specialized platforms.
- Implement cryptography and public key infrastructure.
- Understand threat and vulnerability management activities.
- Develop incident response capabilities.