Certified information Systems Security Professional(CISSP) Bootcamp

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

Official CISSP training draws from a comprehensive, up-to-date, global common body of knowledge thatensures you have a deep knowledge and understanding of new threats, technologies, regulations, standards,and practices. CISSP training covers the 8 domains you'll be tested on in the exam.

This course will expand upon your knowledge by addressing the essential elements of the eight domains thatcomprise a Common Body of Knowledge (CBK) for information systems security professionals. The courseoffers a job-related approach to the security process, while providing a framework to prepare for CISSPcertification.

Certified Information Systems Security Professional (CISSP) is the premier certification for today's informationsystems security professional. It remains the premier certification because the sponsoring organization, theInternational Information Systems Security Certification Consortium, Inc. (ISC)2®, regularly updates the test byusing subject matter experts (SMEs) to make sure the material and the questions are relevant in today'ssecurity environment. By defining eight security domains that comprise a CBK, industry standards for theinformation systems security professional have been established. The skills and knowledge you gain in thiscourse will help you master the eight CISSP domains and ensure your credibility and success within theinformation systems security field.

Required Exams

CISSP Certification exam

Audience Profile

This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, orinstructors, including network or security analysts and engineers, network administrators, information securityspecialists, and risk management professionals, who are pursuing CISSP training and certification to acquire thecredibility and mobility to advance within their current computer security careers or to migrate to a relatedcareer.

Through the study of all eight CISSP Common Body of Knowledge (CBK) domains, students will validate

theirknowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certificationexam.

Course Objectives

In this course, you will identify and reinforce the major security subjects from the eight domains of the CISSP CBK.

You will:

* Analyze components of the Security and Risk Management domain.
* Analyze components of the Asset Security domain.
* Analyze components of the Security Engineering domain.
* Analyze components of the Communications and Network Security domain.
* Analyze components of the Identity and Access Management domain.
* Analyze components of the Security Assessment and Testing domain.
* Analyze components of the Security Operations domain.
* Analyze components of the Software Development Security domain.

Outline

Lesson 1: Security and Risk ManagementTopic A: Security Governance Principles

Topic B: Compliance

Topic C: Professional Ethics

Topic D: Security Documentation

Topic E: Risk Management

Topic F: Threat Modeling

Topic G: Business Continuity Plan Fundamentals

Topic H: Acquisition Strategy and Practice

Topic I: Personnel Security Policies

Topic J: Security Awareness and Training

Lesson 2: Asset SecurityTopic A: Asset Classification

Topic B: Privacy Protection

Topic C: Asset Retention

Topic D: Data Security Controls

Topic E: Secure Data Handling

Lesson 3: Security EngineeringTopic A: Security in the Engineering Lifecycle

Topic B: System Component Security

Topic C: Security Models

Topic D: Controls and Countermeasures in Enterprise Security

Topic E: Information System Security Capabilities

Topic F: Design and Architecture Vulnerability Mitigation

Topic G: Vulnerability Mitigation in Embedded, Mobile, and Web-Based Systems

Topic H: Cryptography Concepts

Topic I: Cryptography Techniques

Topic J: Site and Facility Design for Physical Security

Topic K: Physical Security Implementation in Sites and Facilities

Lesson 4: Communications and Network SecurityTopic A: Network Protocol Security

Topic B: Network Components Security

Topic C: Communication Channel Security

Topic D: Network Attack Mitigation

Lesson 5: Identity and Access ManagementTopic A: Physical and Logical Access Control

Topic B: Identification, Authentication, and Authorization

Topic C: Identity as a Service

Topic D: Authorization Mechanisms

Topic E: Access Control Attack Mitigation

Lesson 6: Security Assessment and TestingTopic A: System Security Control Testing

Topic B: Software Security Control Testing

Topic C: Security Process Data Collection

Topic D: Audits

Lesson 7: Security OperationsTopic A: Security Operations Concepts

Topic B: Physical Security

Topic C: Personnel Security

Topic D: Logging and Monitoring

Topic E: Preventative Measures

Topic F: Resource Provisioning and Protection

Topic G: Patch and Vulnerability Management

Topic H: Change Management

Topic I: Incident Response

Topic J: Investigations

Topic K: Disaster Recovery Planning

Topic L: Disaster Recovery Strategies

Topic M: Disaster Recovery Implementation

Lesson 8: Software Development SecurityTopic A: Security Principles in the System Lifecycle

Topic B: Security Principles in the Software Development Lifecycle

Topic C: Database Security in Software Development

Topic D: Security Controls in the Development Environment

Topic E: Software Security Effectiveness Assessment