



DEEP CREEK CENTER

Delivering Results

CISSP: CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL COURSE (5 DAYS)

Overview

Welcome to Certified Information Systems Security Professional (CISSP): Second Edition. With your completion of the prerequisites and necessary years of experience, you are firmly grounded in the knowledge requirements of today's security professional. This course will expand upon your knowledge by addressing the essential elements of the 10 domains that comprise a Common Body of Knowledge (CBK) for information systems security professionals. The course offers a job-related approach to the security process, while providing the basic skills required to prepare for CISSP certification.

COURSE OBJECTIVE

You will analyze a wide range of information systems security subjects that are organized into 10 domains for CISSP exam certification.

TARGET STUDENT

This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals, who are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current computer security careers or to migrate to a related career. Through the study of all 10 CISSP CBK domains, students will validate their knowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certification exam. Additional CISSP certification requirements include a minimum of five years of direct professional work experience in one or more fields related to the 10 CBK security domains, or a college degree and four years of experience.

PREREQUISITES

It is highly recommended that students have certifications in Network+ or Security+, or possess equivalent professional experience upon entering CISSP training. It will be beneficial if students have one or more of the following security-related or technology-related certifications or equivalent industry experience: MCSE, MCTS, MCITP, SCNP, CCNP, RHCE, LCE, CNE, SSCP, GIAC, CISA, or CISM.

DELIVERY METHOD

Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

PERFORMANCE-BASED OBJECTIVES

Upon successful completion of this course, students will be able to:

- analyze information systems access control.
- analyze security architecture and design.
- analyze network security systems and telecommunications.
- analyze information security management goals.
- analyze information security classification and program development.
- analyze risk management criteria and ethical codes of conduct.
- analyze application security.
- analyze cryptography characteristics and elements.
- analyze physical security.
- analyze operations security.
- apply business continuity and disaster recovery plans.
- identify legal issues, regulations, compliance standards, and investigation practices relating to information systems security.

COURSE CONTENT

Lesson 1: Information Systems Access Control

Topic 1A: Data Access Principles

Topic 1B: System Access and Authentication

Topic 1C: Penetration Tests

Lesson 2: Security Architecture and Design

Topic 2A: Security Models

Topic 2B: Security Modes

Topic 2C: System Assurance

Lesson 3: Network and Telecommunications Security

Topic 3A: Data Network Design

Topic 3B: Remote Data Access

Topic 3C: Data Network Security

Topic 3D: Data Network Management

Lesson 4: Information Security Management Goals

Topic 4A: Organizational Security

Topic 4B: The Application of Security Concepts

Lesson 5: Information Security Classification and Program Development

Topic 5A: Information Classification

Topic 5B: Security Program Development

Lesson 6: Risk Management and Ethics

Topic 6A: Risk Management

Topic 6B: Ethics

Lesson 7: Application Security

Topic 7A: Software Configuration Management

Topic 7B: Software Controls

Topic 7C: Database System Security

Lesson 8: Cryptography

Topic 8A: Ciphers and Cryptography

Topic 8B: Symmetric-Key Cryptography

Topic 8C: Asymmetric-Key Cryptography

Topic 8D: Hashing and Message Digests

Topic 8E: Email, Internet, and Wireless Security

Topic 8F: Cryptographic Weaknesses

Lesson 9: Physical Security

Topic 9A: Physical Access Control

Topic 9B: Physical Access Monitoring

Topic 9C: Physical Security Methods

Topic 9D: Facilities Security

Lesson 10: Operations Security

Topic 10A: Operations Security Control

Topic 10B: Operations Security Auditing and Monitoring

Topic 10C: Operational Threats and Violations

Lesson 11: Business Continuity and Disaster Recovery Planning

Topic 11A: Business Continuity Plan Fundamentals

Topic 11B: Business Continuity Plan Implementation

Topic 11C: Disaster Recovery Plan Fundamentals

Topic 11D: Disaster Recovery Plan Implementation

Lesson 12: Legal, Regulations, Compliance, and Investigations

Topic 12A: Computer Crime Laws and Regulations

Topic 12B: Computer Crime Incident Response