CISSP: Certified Information System Security Professional

Length: 5 Days

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: Cybersecurity First Responder (CFR), MCSE, CCNP, RHCE, LCE, SSCP®, GIAC, CISA™, or CISM®.

Summary: This course prepares student to pass the premier security certification, the Certified Information Systems Security Professional (CISSP®).

COURSE CONTENT

Lesson 1: Security and Risk Management

Topic 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 Security

Topic A: Asset Classification
Topic B: Privacy Protection
Topic C: Asset Retention
Topic D: Data Security Controls
Topic E: Secure Data Handling

Lesson 3: Security Engineering

Topic 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 Security

Topic A: Network Protocol Security
Topic B: Network Components Security
Topic C: Communication Channel Security
Topic D: Network Attack Mitigation

Lesson 5: Identity and Access Management

Topic 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 Testing

Topic A: System Security Control Testing
Topic B: Software Security Control Testing
Topic C: Security Process Data Collection
Topic D: Audits

Lesson 7: Security Operations

Topic 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 Security

Topic 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