Certified Information Systems Security Professional (CISSP)

Course #: 1276-100-ZZ-W

Hours: 35

Course Content

Course Description:

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

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 software development 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.

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. The CISSP exam is intentionally difficult and should not be taken lightly. Even students with years of security experience should assume that they will have additional study time after class. Because the domains are so varied, it is unlikely that any one student will have experience in all 10 domains. 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.

Certified Information Systems Security Professional (CISSP)

Course #: 1276-100-ZZ-W

Hours: 35

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®.

Topics:

Module 1: Information Systems Access Control
- Data Access Principles
- System Access and Authentication
- Attacks and Penetration Tests

Module 2: Security Architecture and Design
- Security Architecture Frameworks and Security Models
- Security Modes
- System Assurance

Module 3: Network and Telecommunications Security
- Data Network Design
- Remote Data Access
- Data Network Security
- Data Network Management

Module 4: Information Security Management Goals
- Organizational Security
- The Application of Security Concepts

Module 5: Information Security Classification and Program Development
- Information Classification
- Security Program Development

Module 6: Risk Management and Ethics
- Risk Management
- Ethics

Module 7: Software Development Security
- Software Configuration Management
- Software Controls
- Database System Security

Module 8: Cryptography
- Ciphers and Cryptography
- Symmetric-Key Cryptography
- Asymmetric-Key Cryptography
- Hashing and Message Digests
- Email, Internet, and Wireless Security
- Cryptographic Weaknesses

Module 9: Physical Security
- Physical Access Control
- Physical Access Monitoring
- Physical Security Methods
- Facilities Security

Module 10: Operations Security
- Operations Security Control
- Operations Security Auditing and Monitoring
- Operational Threats and Violations

Certified Information Systems Security Professional (CISSP)

Course #: 1276-100-ZZ-W

Hours: 35

Module 11: Business Continuity and Disaster Recovery Planning

- Business Continuity Plan Fundamentals
- Business Continuity Plan Implementation
- Disaster Recovery Plan Fundamentals
- Disaster Recovery Plan Implementation

Module 12: Legal, Regulations, Compliance, and Investigations

- Computer Crime Laws and Regulations
- Computer Crime Incident Response

Appendix A: Mapping CISSP® Course Content to the (ISC)² CISSP Exam Objectives