Certified Information System Security Professional (CISSP)

Length: 5 Days

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

Course Objectives: Upon completion of this course, students have learned how to:

- 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.

Who Should Attend: The training seminar is ideal for those working in positions such as but not limited to:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect
- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Security Director
- Network Architect

Experience Needed: 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:

- CyberSec First Responder (CFR)
- Microsoft Certified Solutions Expert (MCSE)
- Cisco Certified Network Professional (CCNP)
- Red Hat Certified Engineer (RHCE)
- Linux Foundation Certified Engineer (LFCE)
- Systems Security Certified Practitioner (SSCP®)
- GIAC Security Essentials (GSEC)
- GIAC Information Security Fundamentals (GISF)
- Certified Information Systems Auditor (CISA™)
- Certified Information Security Manager (CISM®)

COURSE CONTENT

1: SECURITY AND RISK MANAGEMENT

- Security Governance Principles
- Security Concepts
- Compliance
- Professional Ethics
- Security Documentation
- Risk Management

- Threat Modeling
- Risk Response
- Business Continuity Plan Fundamentals
- Acquisition Strategy and Practice
- Personnel Security Policies
- Security Awareness and Training

2: ASSET SECURITY

- Asset Classification
- Resource Provisioning and Protection
- Asset Retention
- Data Security Control
- Manage Data Lifecycle
- Secure Data Handling

3: SECURITY ENGINEERING

- Security in the Engineering Lifecycle
- System Component Security
- Security Models
- Controls and Countermeasures in Enterprise Security
- Information System Security Capabilities
- Design and Architecture Vulnerability Mitigation
- Vulnerability Mitigation in Emerging Technologies
- Cryptography Concepts
- Cryptography Techniques
- Cryptanalytic Attacks
- Site and Facility Design for Physical Security
- Physical Security Implementation in Sites and Facilities

4: COMMUNICATIONS AND NETWORK SECURITY

- Network Protocol Security
- Network Components Security
- Communication Channel Security
- Network Attack Mitigation

5: IDENTITY AND ACCESS MANAGEMENT

- Physical and Logical Access Control
- Identification and Authentication,
- Identity as a Service
- Authorization Mechanisms
- Access Control Attack Mitigation

6: SECURITY ASSESSMENT AND TESTING

- System Security Control Testing
- Software Security Control Testing
- Security Process Data Collection
- Audits

7: SECURITY OPERATIONS

- Security Operations Concepts
- Change Management
- Physical Security
- Personnel Security
- Detective and Preventative Measures
- Patch and Vulnerability Management
- Logging and Monitoring
- Incident Response
- Investigations
- Disaster Recovery Planning
- Disaster Recovery Strategies
- Disaster Recovery Implementation

8: SOFTWARE DEVELOPMENT SECURITY

- Security Principles in the System Lifecycle
- Security Principles in the Software Development Lifecycle
- Database Security in Software Development
- Security Controls in the Development Environment
- Software Security Effectiveness Assessment