Certified Information System Security Professional (CISSP)

Duration
Classroom Learning - 5 Day(s)
Online LIVE - 5 Day(s)

Overview
In this course, students will analyze a wide range of information systems security subjects that are organized into 8 domains for CISSP exam certification.

Who Should Attend
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 8 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 8 domains.

Prerequisite(s) or equivalent knowledge
CompTIA Network+ Certification

CompTIA Security+ Certification

Prerequisite Comments
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®.

Outline:

1 - Security & Risk Management

- Security & Risk Management
- Confidentiality, Integrity, and Availability
- Security Governance
- The Complete and Effective Security Program
- Compliance
- Global Legal and Regulatory Issues
- Understand Professional Ethics
- Develop and Implement Security Policy
- Business Continuity (BC) & Disaster Recovery (DR) Requirements
- Manage Personnel Security
- Risk Management Concepts
- Threat Modeling
- Acquisitions Strategy and Practice
- Security Education, Training, and Awareness

2 - Asset Security

- Asset Security
- Data Management: Determine and Maintain Ownership
- Data Standards
- Longevity and Use
- Classify Information and Supporting Assets
- Asset Management
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Standards Selection

3 - Security Engineering

- Security Engineering
- The Engineering Lifecycle Using Security Design Principles
- Fundamental Concepts of Security Models
- Information Systems Security Evaluation Models
- Security Capabilities of Information Systems
- Vulnerabilities of Security Architectures
- Database Security
- Software and System Vulnerabilities and Threats
- Vulnerabilities in Mobile Systems
- Vulnerabilities in Embedded Devices and Cyber-Physical Systems
- The Application and Use of Cryptography
- Site and Facility Design Considerations
- Site Planning
- Implementation and Operation of Facilities Security

4 - Communications & Network Security

- Communications & Network Security
- Secure Network Architecture and Design
- Implications of Multi-Layer Protocols
- Converged Protocols
- Securing Network Components
- Secure Communication Channels
- Network Attacks

5 - Identify & Access Management

- Identity & Access Management
- Physical and Logical Access to Assets
- Identification and Authentication of People and Devices
- Identity Management Implementation
- Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Identity and Access Provisioning Lifecycle

6 - Security Assessment & Testing

- Security Assessment & Testing
- Assessment and Test Strategies
- Collect Security Process Data
- Internal and Third-Party Audits

7 - Security Operations

- Security Operations
- Investigations
- Provisioning of Resources through Configuration Management
- Resource Protection
- Incident Response
- Preventative Measures against Attacks
- Patch and Vulnerability Management
- Change and Configuration Management
- The Disaster Recovery Process
- Test Plan Review
- Business Continuity and Other Risk Areas
- Access Control
- Personnel Safety

8 - Security in the Software Development Life Cycle

Security in the Software Development Life Cycle
Software Development Security Outline
Environment and Security Controls
Security of the Software Environment
Software Protection Mechanisms
Assess the Effectiveness of Software Security
Assess Software Acquisition Security

To register or for more information call our office **(208) 898-9036** or email **register@leapfoxlearning.com**