Certified Information Systems Security Professional (CISSP)

5 Days

Overview

CISSP training is an advanced course designed to meet the high demands of the information security industry by preparing students for the Certified Information Systems Security Professional (CISSP) exam. Led by an authorized instructor, this training course provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP CBK:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Prerequisites:

Candidates must have a minimum of five (5) years of cumulative paid full-time professional security work experience in two or more of the 8 domains of the CISSP CBK.
Candidates may receive a one year experience waiver with a four-year college degree, or regional equivalent OR additional credential from the approved list, thus requiring four (4) years of direct full-time professional security work experience in two or more of the ten domains of the CISSP CBK.
Candidates who have not completed the 5 years of experience to take the CISSP, can take an Associate CISSP exam. This will give them a credential showing their knowledge until they are able to meet the experience requirements for the CISSP.

Course Outline:

Security and Risk Management
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

Asset Security
- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

Security Engineering
- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Communication and Network Security
- Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Identity and Access Management
- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g. cloud identity)
- Third-party identity services (e.g. on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

Security Assessment and Testing
- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

Security Operations
- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Software Development Security
- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact