Certified Information Systems Security Professional Preparation

Course Content

This is a 5-day learner-centered Instructor-Lead Training (ILT) CISSP Preparation. Our goal to provide you with practical knowledge you can actually use in your profession together while enhancing your proficient in security principles, concept and frameworks.

We are not only enabling you to experience the real-world skills, but also preparing you for the Certified Information System Security Professional (CISSP®) certification, the premier security certification created and administered by the International Systems Security Certification Consortium (ISC2).

Prerequisites

Participants should have the following experience to criteria to achieve CISSP:

Candidates must have a minimum of 5 years cumulative paid full-time work experience in 2 or more of the 8 domains of the CISSP CBK. Earning a 4-year college degree or regional equivalent or an additional credential from the (ISC)^2 approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience.

A candidate that doesn’t have the required experience to become a CISSP may become an Associate of (ISC)^2 by successfully passing the CISSP examination. The Associate of (ISC)^2 will then have 6 years to earn the 5 years required experience.

Course Details

Course Introduction and Exam Preparation Strategy. CISSP Domain:

Domain 1: Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand, adhere to, and promote professional ethics
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

Domain 2: Asset Security

- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

Domain 3: Security Architecture and Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform
- Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution Elements
- Assess and mitigate vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices
- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

Domain 4: Communication and Network Security

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Domain 5: Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

Domain 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

Domain 7: Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Securely provisioning resources
- Understand and apply foundational security operations concepts
- Apply resource protection techniques
- Conduct incident management
- Operate and maintain detective and preventative measures

- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Domain 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards

Review Exam Questions

Who Should Attend?

The CISSP credential is ideally for IT Professionals, Security Professionals, Mid-Level Managers, and Senior-Level Managers I is ideal for mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers. This course is designed for professionals who wish to attain CISSP certification and facilitate their growth as a security professional.

Course Duration

5 days