CISSP - Certified Information Systems Security Professional

Certified Information Systems Security Professional (CISSP®) training provides a comprehensive review of the knowledge required to effectively design, engineer and manage the overall security posture of an organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the CISSP exam. Content aligns with and comprehensively covers the eight domains of the (ISC)2 CISSP Common Body of Knowledge (CBK®), ensuring relevancy across all disciplines in the field of cybersecurity.

As an (ISC)2 Official Training Provider, we use courseware developed by (ISC)2 – creator of the CISSP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CISSP and have completed intensive training to teach (ISC)2 content.

Training features:

- Instruction from an (ISC)2 Authorized Instructor
- Official (ISC)2
- Student Training Guide
- Chapter quizzes
- Interactive flash cards to reinforce learnin
- Real-world learning activities and scenarios
- Post-course assessment questions to gauge exam readiness

Who Should Attend

This training course is intended for professionals who have at least five years of cumulative, paid work experience in two or more of the eight domains of the (ISC)2 CISSP CBK and are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current information security careers. 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

Course Agenda

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)
- Domain 6: Security Assessment and Testing
- Domain 7: Security Operations
- Domain 8: Software DevelopmentSecurity

Course Objectives

After completing this course, the student will be able to:

- Understand and apply fundamental concepts and methods related to the fields of information technology and security
- Align overall organizational operational goals with security functions and implementations
- Understand how to protect assets of the organization as they go through their lifecycle
- Understand the concepts, principles, structures and standards used to design, implement, monitor and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of confidentiality, integrity and availability
- Implement system security through the application of security design principles and application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures
- Understand the importance of cryptography and the security services it can provide in today's digital and information age
- Understand the impact of physical security elements on information system security and apply secure design principles to evaluate or recommend appropriate physical security protections
- Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function
- List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1-7
- Identify standard terms for applying physical and logical access controls to environments related to their security practice
- Appraise various access control models to meet business security requirements
- Name primary methods for designing and validating test and audit strategies that support business requirements
- Enhance and optimize an organization's operational function and capacity by applying and utilizing appropriate security controls and countermeasures
- Recognize risks to an organization's operational endeavors and assess specific threats, vulnerabilities and controls
- Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it; identify which security control(s) are appropriate for the development environment; and assess the effectiveness of software security
- Identify appropriate practices for the secure handling of sensitive information.