# Certified Information Systems Security Professional (CISSP)

## Course Duration: 10 Days

## Course Overview

Led by an ISC2 authorized instructor, this training seminar 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
- Communications and Network Security
- Security Architecture and Engineering
- Identity and Access Management (IAM)
- Security Operations
- Security Assessment and Testing
- Software Development Security

Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam and features:

1. Official ISC2 courseware.
2. Taught by an authorized ISC2 instructor.
3. Student handbook.
4. Collaboration with classmates.
5. Real-world learning and scenarios.

## Upon Completion

Students will:

- Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure business environment.
- Ensure professionals stay current on emerging threats, technologies, regulations, standards, and practices through the continuing professional education requirements.

- Increase confidence that candidates are qualified and committed to information security.
- Ensure employees use a universal language, circumventing ambiguity with industry accepted terms and practices.
- Increase organizations credibility when working with clients.

## Who Should Attend?

- Security Consultant
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- IT Director/Manager
- Director of Security
- Network Architect
- Security systems Engineer
- Chief Information security Officer

## Course Content

| Module # | Module Topic | Description |
|---|---|---|
| **Chapter 01** | **The Information Security Environment** | Module 1: Understand, Adhere to and Promote Professional Ethics |
| | | Module 2: Understand and Apply Security Concepts |
| | | Module 3: Evaluate and Apply Security Governance Principles |
| | | Module 4: Understand the Legal Environment |
| | | Module 5: Understand Basic Secure Design Principles |
| | | Module 6: Chapter Review |

| | | |
|---|---|---|
| **Chapter 02** | **Information Asst Security** | **Module 1:** Manage Information Assets |
| | | **Module 2:** Manage the Data Security Lifecycle |
| | | **Module 3:** Determine Data Security Controls and Compliance Requirements |
| | | **Module 4:** Chapter Review |
| **Chapter 03** | **Identify and Access Management** | **Module 1:** Manage the Identity and Access Provisioning Lifecycle |
| | | **Module 2**: Implement and Manage Access Control Models and Mechanisms |
| | | **Module 3:** Manage People and Operations |
| | | **Module 4:** Control Physical and Logical Access to Assets |
| | | **Module 5:** Manage Identification and Authentication of People, Devices and Services |
| | | **Module 6:** Implement Authentication and Authorization Systems |
| | | **Module 7:** Chapter Review |
| **Chapter 04** | **Security Architecture and Engineering** | **Module 1:** Assess and Mitigate the Vulnerabilities of Security Architectures, Designs and Solution Elements |
| | | **Module 2:** Cryptographic Systems |
| | | **Module 3:** Hybrid Systems and the Public Key Infrastructure |
| | | **Module 4:** Cryptographic Systems Hygiene: Operation and Maintenance |
| | | **Module 5:** Cryptanalysis: Methods of Cryptanalytic Attacks |
| | | **Module 6:** Chapter Review |
| **Chapter 05** | **Communicate and Network Security** | **Module 1:** Open System Interconnection) and Transmission Control Protocol Over Internet Protocol Models |

| | | |
|---|---|---|
| | | **Module 2:** OSI Layer 1: Physical Layer |
| | | **Module 3:** OSI Layer 2: Data Link Layer |
| | | **Module 4:** OSI Layer 3: Network Layer |
| | | **Module 5:** OSI Layer 4: Transport Layer |
| | | **Module 6:** OSI Layer 5: Session Layer |
| | | **Module 7:** OSI Layer 6: Presentation Layer |
| | | **Module 8:** OSI Layer 7: Application Layer |
| | | **Module 9:** Assess and Implement Secure Design Principles in Network Architectures |
| | | **Module 10:** Secure Network Components |
| | | **Module 11:** Implement Secure Communication Channels According to Design |
| | | **Module 12:** Chapter Review |
| **Chapter 06** | **Software Development Security** | **Module 1:** Why so Many Software Systems are Unsecure |
| | | **Module 2:** Security Weaknesses at the Source Code Level: Why so Much Software is Unsecure |
| | | **Module 3:** Why Databases can be Unsecure |
| | | **Module 4:** Why Websites can be Unsecure |
| | | **Module 5**: Malware, Ransomware and Ransom Attacks: The Software Perspective |
| | | **Module 6**: "Baking In" Security: Development Management Choices |
| | | **Module 7**: Security Controls in Software Development Ecosystems |
| | | **Module 8:** Risk Analysis and Mitigation for Software Apps and Systems |
| | | **Module 9:** Chapter Review |

| | | |
|---|---|---|
| **Chapter 07** | **Security Assessment and Testing** | **Module 1:** Design and Validate Assessment, Test and Audit Strategies |
| | | **Module 2:** Conduct Security Control Assessment |
| | | **Module 3:** Collect Security Process Data |
| | | **Module 4:** Analyze and Report on Organizational Performance |
| | | **Module 5:** Chapter Review |
| **Chapter 08** | **Security Operation** | **Module 1:** Conduct Logging and Monitoring Activities |
| | | **Module 2:** Perform Change Management |
| | | **Module 3:** Basic Incident Response Concepts |
| | | **Module 4:** Conduct Incident Management |
| | | **Module 5:** Operate and Maintain Detective and Preventive Measures |
| | | **Module 6:** Implement Backup and Recovery Strategies |
| | | **Module 7:** Apply Security Principles to Site and Facility Design |
| | | **Module 8:** Site and Facility Security Controls |
| | | **Module 9:** Personnel Safety and Security Concerns |
| | | **Module 10:** Chapter Review |
| **Chapter 09** | **Putting It All Together** | **Module 1:** Security Governance: The Ultimate Administrative Control Set |
| | | **Module 2:** Security Frameworks in Operational Use |
| | | **Module 3:** Forensic Investigations |
| | | **Module 4:** Building Organizational Capacity to Address BCDR Requirements |
| | | **Module 5:** Contribute to and Enforce Personnel Security Policies and Procedures |

| | | |
|---|---|---|
| | | Module 6: Operationalizing Risk Management |
| | | Module 7: Apply IT Supply Chain Risk Management (SCRM) Concepts |
| | | Module 8: Establish and Maintain a Security Awareness, Education and Training Program |
| | | Module 9: Chapter Review |