Certified Information Systems Security Professional (CISSP)

Introduction

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following eight domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Course Highlights

This course teaches you about core aspects such as;

- Security and risk management
- Asset security architecture and design
- Cryptography OSI and TCP IP models
- IP addresses
- Network security
- Identity and access management
- Security assessment and testing
- Software development security

Course Outline

MODULE 1: Security and Risk Management

1.1 Understand, adhere to and promote professional ethics
1.2 Understand and apply security concepts
1.3 Evaluate and apply security governance principles
1.4 Determine compliance and other requirements
1.5 Understand legal and regulatory issues that pertain to information security in a holistic context
1.6 Understand requirements for investigation types
1.7 Develop, document, and implement security policy, standards, procedures, and guidelines
1.8 Identify, analyze, and prioritize Business Continuity (BC) requirements
1.9 Contribute to and enforce personnel security policies and procedures
1.10 Understand and apply risk management concepts
1.11 Understand and apply threat modeling concepts and methodologies
1.12 Apply Supply Chain Risk Management (SCRM) concepts
1.13 Establish and maintain a security awareness, education, and training program

MODULE 2: Asset Security

2.1 Identify and classify information and assets
2.2 Establish information and asset handling requirements
2.3 Provision resources securely
2.4 Manage data lifecycle
2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
2.6 Determine data security controls and compliance requirements

MODULE 3: Security Architecture and Engineering

3.1 Research, implement, and manage engineering processes using secure design principles
3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
3.3 Select controls based upon systems security requirements
3.4 Understand security capabilities of Information Systems (IS)
3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
3.6 Select and determine cryptographic solutions
3.7 Understand methods of cryptanalytic attacks
3.8 Apply security principles to site and facility design
3.9 Design site and facility security controls

MODULE 4: Communication and Network Security

4.1 Assess and implement secure design principles in network architectures
4.2 Secure network components
4.3 Implement secure communication channels according to design

MODULE 5: Identity and Access Management (IAM)

5.1 Control physical and logical access to assets
5.2 Manage identification and authentication of people, devices, and services
5.3 Federated identity with a third-party service
5.4 Implement and manage authorization mechanisms
5.5 Manage the identity and access provisioning lifecycle
5.6 Implement authentication systems

MODULE 6: Security Assessment and Testing

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

MODULE 7: Security Operations

7.1 Understand and comply with investigations
7.2 Conduct logging and monitoring activities
7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
7.4 Apply foundational security operations concepts
7.5 Apply for resource protection
7.6 Conduct incident management
7.7 Operate and maintain detective and preventative measures
7.8 Implement and support patch and vulnerability management
7.9 Understand and participate in change management processes
7.10 Implement recovery strategies
7.11 Implement Disaster Recovery (DR) processes
7.12 Test Disaster Recovery Plans (DRP)
7.13 Participate in Business Continuity (BC) planning and exercises
7.14 Implement and manage physical security
7.15 Address personnel safety and security concerns

MODULE 8: Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)
8.2 Identify and apply security controls in software development ecosystems
8.3 Assess the effectiveness of software security

8.4 Assess security impact of acquired software
8.5 Define and apply secure coding guidelines and standards

Prerequisites

- Candidates who wish to take up the Certified Information Systems Security Professional (CISSP) training have a minimum of 5 years of work experience in two or more of the 8 domains prescribed by ISC2 in their CISSP Common Body of Knowledge (CBK)

- There can be a waiver of 1 year from the required 5-year experience if the candidate has a 4-year college degree or any additional certification credential from ISC2 approved course list.

Target Audience

Job roles that can take up CISSP training include, but are not limited to:

- Network Architects
- Security Consultants
- Security Architects
- Security Auditors
- Security Managers
- CIOs
- Directory of Security
- Security Analysts
- Security Systems Engineers
- Anybody who wants to gain knowledge of globally recognized CISSP information security standards
- Anybody who is looking to clear their CISSP Certification Exam

Duration

- 40 Hours Training Course