Certified Information Systems Security Professional (CISSP)

40 Hours

Course Description

In this engaging and comprehensive online training course, you receive in-depth instruction covering the 8 CISSP domains. Expertise in these domains is critical in today's information technology world. As you architect, design, and manage IT solutions, your knowledge and expertise, proven by your CISSP certification, can enhance the security posture of your company or your clients.

The CISSP domains include Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Skills Learned

After completing this online training course, students will be able to:

- 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

None, but we recommend CompTIA Security+ certification or equivalent knowledge.

Who Should Attend

CISSP certification aids job-seekers interested in positions such as Security Architect, Security Auditor, IT Director, Chief Information Security Officer, Network Architect, and more. CISSP is an advanced security certification, as evidenced by its requirement of 5 years of full time experience in a security-related position. Anyone seeking to enhance their current skillset in the security and provide evidence of competency in many areas of security should seek the CISSP certification.

Course Outline

1. Security and Risk Management

Understand, adhere to, and promote professional ethics

Understand and apply security concepts

Evaluate, apply, and sustain security governance principles

Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

Understand requirements for investigation types

Develop, document, and implement security policy, standards, procedures, and guidelines

Identify, analyze, assess, prioritize, and implement 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 supply chain risk management (SCRM) concepts

Establish and maintain a security awareness, education, and training program

2. Asset Security

Identify and classify information and assets

Establish information and asset handling requirements

Provision information and assets securely

Manage data lifecycle

Ensure appropriate asset retention

Determine data security controls and compliance requirements

3. Security Architecture and Engineering

Research, 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

Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

Select and determine cryptographic solutions

Understand methods of cryptanalytic attacks

Apply security principles to site and facility design

Design site and facility security controls

Manage the information system lifecycle

04. Communication and Network Security

Apply secure design principles in network architectures

Secure network components

Implement secure communication channels according to design

5. Identity and Access Management (IAM)

Control physical and logical access to assets
Design identification and authentication strategy
Federated identity with a third-party service
Implement and manage authorization mechanisms
Manage the identity and access provisioning lifecycle
Implement authentication systems

6. Security Assessment and Testing

Design and validate assessment, test, and audit strategies
Conduct security controls testing
Collect security process data
Analyze test output and generate report
Conduct or facilitate security audits

7. Security Operations

Understand and comply with investigations
Conduct logging and monitoring activities
Perform configuration management (CM)
Apply foundational security operations concepts
Apply resource protection
Conduct incident management
Operate and maintain detection 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 plan (DRP)
Participate in Business Continuity (BC) planning and exercises
Implement and manage physical security
Address personnel safety and security concerns

8. Software Development Security

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