BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Certified Information Systems Security Professional (CISSP)

Course Introduction

CISSP is the premier certification for today’s information systems security professional. The International Information Systems Security Certification Consortium, Inc. (ISC)2, regularly updates the test by using subject matter experts (SMEs) to make sure the material and the questions are relevant in today’s security environment. By defining eight security domains that comprise a CBK, industry standards for the information systems security professional have been established.

This training course is designed to help participants expand their knowledge by addressing the essential elements of the eight domains that comprise a Common Body of Knowledge (CBK) for information systems security professionals, and let them ahead of the most critical security topics and build resilience.

Target Audience

- Cloud Computing Engineer
- Computer Network Specialist
- Computer Support Specialist
- Database Administrator
- Information Technology Analyst
- Information Technology Leadership
- Information Security Specialist
- Software/Application Developer
- Web Developer
- Technology sales consultant

Learning Objectives

- Gain the expertise to manage a best-practice information security system, aligned to globally accepted standards, that ensures your organization's information assets are protected
- Learn the emerging threats, technologies, regulations, standards, and industry best practices, and how to stay informed
- Be familiar with industry accepted terminology and practices used by information security professionals
- Analyze components of the Security and Risk Management domain, Asset Security domain, Security Architecture and Engineering domain, Communication and Network Security domain, Identity and Access Management domain, Security Assessment and Testing domain, Security Operations domain, and Software Development Security domain.

Course Outline

- **Day 01**

Lesson 1: Security and Risk Management

  - Topic A: Security Concepts
  - Topic B: Security Governance Principles
  - Topic C: Compliance
  - Topic D: Professional Ethics
  - Topic E: Security Documentation
  - Topic F: Risk Management
  - Topic G: Threat Modeling
  - Topic H: Risk Response
  - Topic I: Business Continuity Plan Fundamentals
  - Topic J: Acquisition Strategy and Practice
  - Topic K: Personnel Security Policies
  - Topic L: Security Awareness and Training

Lesson 2: Asset Security

- Topic A: Asset Classification
- Topic B: Secure Data Handling
- Topic C: Resource Provisioning and Protection
- Topic D: Manage Data Lifecycle
- Topic E: Asset Retention
- Topic F: Data Security Controls

• **Day 02**

Lesson 3: Security Architecture and Engineering

- Topic A: Security in the Engineering Lifecycle
- Topic B: System Component Security
- Topic C: Security Models
- Topic D: Controls and Countermeasures in Enterprise Security
- Topic E: Information System Security Capabilities
- Topic F: Design and Architecture Vulnerability Mitigation
- Topic G: Vulnerability Mitigation in Emerging Technologies
- Topic H: Cryptography Concepts
- Topic I: Cryptography Techniques
- Topic J: Cryptanalytic Attacks
- Topic K: Site and Facility Design for Physical Security
- Topic L: Physical Security Implementation in Sites and Facilities

Lesson 4: Communication and Network Security

- Topic A: Network Protocol Security
- Topic B: Network Components Security
- Topic C: Communication Channel Security
- Topic D: Network Attack Mitigation

- **Day 03**

  Lesson 5: Identity and Access Management

    - Topic A: Physical and Logical Access Control
    - Topic B: Identification and Authentication
    - Topic C: Identity as a Service
    - Topic D: Authorization Mechanisms
    - Topic E: Access Control Attack Mitigation

  Lesson 6: Security Assessment and Testing

    - Topic A: System Security Control Testing
    - Topic B: Software Security Control Testing
    - Topic C: Security Process Data Collection
    - Topic D: Audits
- **Day 04**

  Lesson 7: Security Operations

    - Topic A: Security Operations Concepts
    - Topic B: Change Management
    - Topic C: Physical Security
    - Topic D: Personnel Security
    - Topic E: Detective and Preventive Measures
    - Topic F: Patch and Vulnerability Management
    - Topic G: Logging and Monitoring
    - Topic H: Incident Response
    - Topic I: Investigations
    - Topic J: Disaster Recovery Planning
    - Topic K: Disaster Recovery Strategies
    - Topic L: Disaster Recovery Implementation
- **Day 05**

Lesson 8: Software Development Security

- Topic A: Security Principles in the System Lifecycle
- Topic B: Security Principles in the Software Development Lifecycle
- Topic C: Security Controls in the Development Environment
- Topic D: Database Security in Software Development
- Topic E: Software Security Effectiveness Assessment

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
May 11, 2025	May 15, 2025	5 days	4250.00 $	KSA - El Dammam
Aug. 17, 2025	Aug. 21, 2025	5 days	2150.00 $	Virtual - Online
Sept. 8, 2025	Sept. 12, 2025	5 days	4950.00 $	Spain - Madrid
Dec. 22, 2025	Dec. 26, 2025	5 days	4250.00 $	UAE - Abu Dhabi
Oct. 6, 2025	Oct. 10, 2025	5 days	4250.00 $	UAE - Dubai