

**Soft-Train®**



*At Soft-Train  
Technology Works*

# Certified Information Systems Security Professional (CISSP) (5 Days) ST45011

**COURSE GOAL:** The goal of this course is to prepare students to take the CISSP Certification Exam.

**PREREQUISITES:** Students must have fundamental networking skills.

**LEARNING OBJECTIVES:**  
Students will be able to understand the ten district domains as identified by the (ISC)<sup>2</sup>:

- Access Control
- Application Security
- Business Continuity and Disaster Recovery
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environment) Security
- Security Architecture and Design
- Telecommunications and Network Security

## **KEY TOPICS:**

### **I. Information Security and Risk Management**

- A. The Business Case for Information Security Management
- B. Information Security Management Governance
- C. Audit Frameworks for Compliance
- D. Organizational Behavior
- E. Responsibilities of the Information Security Officer
- F. Reporting Model
- G. Enterprise Wide Security Oversight Committee
- H. Security Planning
- I. Security Awareness, Training and Education
- J. Risk Management
- K. Ethics

### **II. Access Control**

- A. Definitions and Key Concepts
- B. Access Control Categories and Types
- C. Access Control Threats
- D. Access to Systems
- E. Access to Data
- F. Intrusion Detective and Prevention Systems
- G. Access Control Assurance

### **III. Cryptography**

- A. Key Concepts and Definitions
- B. Emerging Technology
- C. Protecting Information
- D. Uses of Cryptography

- E. Additional Features of Cryptographic Systems
- F. Methods of Cryptography
- G. Encryption Systems
- H. Asymmetric Algorithms
- I. Message Integrity Controls
- J. Message Authentication Code
- K. Encryption Management
- L. Cryptanalysis and Attacks
- M. Encryption Usage

#### **IV. Physical (Environment) Security**

- A. Physical (Environmental) Security Challenges
- B. Site Location
- C. The Layered Defense Model
- D. Physical Considerations
- E. Infrastructure Support Systems
- F. Building Entry Points
- G. Information Protection and Management Services

#### **V. Security Architecture and Design Components and Principles**

- A. Security Architecture and Design Components and Principles
- B. Hardware
- C. Software
- D. Security Models and Architecture Theory
- E. Security Product Evaluation Methods and Criteria

#### **VI. Business Continuity and Disaster Recovery Planning**

- A. CISSP Expectations
- B. Why Continuity Planning?
- C. Industry and Professional Standards
- D. Enterprise Continuity Planning and its Relationship to Business Continuity and Disaster Recovery Planning
- E. Organization of the BCP/DRP Domain Chapter

- F. Development Phase Description
- G. Implementation Phase Description
- H. Management Phase Description

#### **VII. Telecommunications and Network Security**

- A. Basic Concepts
- B. Layer 1: Physical Layer
- C. Layer 2: Data Link Layer
- D. Layer 3: Network Layer
- E. Layer 4: Transport Layer
- F. Layer 5: Session Layer
- G. Layer 6: Presentation Layer
- H. Layer 7: Application Layer

#### **VIII. Application Security**

- A. Domain Description and Introduction
- B. Applications Development and Programming Concepts and Protection
- C. Programming
- D. The Software Environment
- E. Threats in the Software Environment
- F. Application Development Security Protections and Controls
- G. Software Protection Mechanism
- H. Audit and Assurance Mechanisms
- I. Malicious Software (Malware)
- J. The Database and Data Warehousing Environment
- K. Database Interface Languages
- L. Data Warehousing
- M. Database Vulnerabilities and Threats
- N. DBMS Controls
- O. Web Application Environment

#### **IX. Operations Security**

- A. Privileged Entity Codes
- B. Resource Protection
- C. Threats to Operations
- D. Control Types
- E. Control Methods

- F. Media Types and Protection Methods
- G. Object Reuse
- H. Sensitive Media Handling
- I. Continuity of Operations
- J. Change Control Management

**X. Legal, Regulations, Compliance, and Investigations**

- A. Major Legal Systems
- B. Information Technology Laws and Regulations
- C. Intellectual Property Laws
- D. Incident Response
- E. Computer Forensics