

# The Official (ISC)<sup>2</sup>® CISSP® CBK® Review Seminar

Most information security professionals specialise in only one or two of the CBK domains and typically have varying degrees of knowledge in the other eight or nine. In-depth knowledge of all 10 domains is required to pass the exam. For this reason (ISC)<sup>2</sup> has developed this intensive, five-day review seminar that will refresh your knowledge and broaden your understanding of all 10 CISSP CBK domains.

## The Seminar provides:

- a complete overview of the scope of the CISSP CBK;
- a comprehensive review and discussion of the topics, subtopics, and sub-subtopics of the CISSP CBK domains;
- extensive knowledge-based materials and presentations developed by (ISC)<sup>2</sup> -authorised instructors and subject matter experts;
- a self-assessment consisting of 100 questions that test your knowledge of the CISSP CBK;
- a personal critique of your results to help you focus on the topic where you need more study;
- a comprehensive student guide that addresses all materials covered by the course

## The 10 Domains of the CISSP CBK

### Information Security and Risk Management

Identification of an organisation's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines.

- a. Governance
- b. Organisational Behaviour
- c. Security Awareness, Training and Education
- d. Risk Management
- e. Ethics

### Access Control

A collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

- a. Information Classification
- b. Access Control Categories, Types and Threats
- c. Identity and Access Management
- d. IDS and IPS

### Cryptography

The principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

- a. Encryption Systems
- b. Message Integrity Controls
- c. Digital Signatures
- d. Encryption Management
- e. Cryptanalysis and Attacks

### Physical (Environmental) Security

Protection techniques for the entire facility, including all of the information system resources.

- a. Site Location and Layered Defense
- b. Building Infrastructure Protection
- c. Physical Control Types

### Security Architecture and Design

Concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and controls used to enforce various levels of availability, integrity, and confidentiality.

- a. Components and Principles
- b. Security Models and Architecture Theory
- c. Security Evaluations Methods and Criteria

### Business Continuity and Disaster Recovery Planning

Addresses the preservation of the business in the event of outages to normal business operations.

- a. Project Scope Development and Planning
- b. Business Impact Analysis
- c. Emergency Assessment
- d. Business Continuity and Recovery Strategy
- e. Implementation

### Telecommunications and Network Security

Includes network structures, transmission methods, transport formats, security measures, and authentication.

- a. Network Types and Architectures
- b. Wireless Transmission Technologies
- c. Network Protocols and Attacks
- d. Traditional and VOIP Telephony

### Application Security

Outlines the environment where software is designed and developed and explains the critical role software plays in providing security to the information system.

- a. System Life Cycle Security
- b. Application Environment and Security Controls
- c. Databases
- d. System Threats and Vulnerabilities
- e. Malicious Code

### Operations Security

Used to identify the controls over hardware, media, and operators and administrators with access privileges to any of these resources.

- a. Resource Protection
- b. Physical Access Control
- c. Continuity of Operations
- d. Change Control Management
- e. Security Administrator Privileges

### Legal, Regulations, Compliance and Investigations

Addresses computer crime laws and regulations, investigative measures and techniques, and forensic evidence gathering.

- a. Major Legal Systems
- b. Information System and Internet Legal Concepts
- c. Intellectual Property
- d. Investigation
- e. Computer Forensics