

## Course Introduction

The (ISC)2® CISSP® certification is the world most recognized for security professionals. CISSP holders are world-wide accepted as the master of information security. To attain the certificate, the walk-ins are mere possible to achieve, it will need a proper preparation. This is the most comprehensive review seminar discussed in information systems security industry best practices, known as the (ISC)2 CBK®.

The review seminar helps you review the 10 domains of the information security practices. It also serves as a strong learning tool for mastering concepts and topics related to all aspects of information systems security.

To attend the CISSP CBK Review Seminar an attendee does not need to have the prerequisite experience for the examination. It is encouraged that all people working in the field of IT and Information Security attend the CISSP seminar to give them a thorough understanding of Information Security even if they do not intend to sit for the examination.

## Course Objectives

- To review of the main topics of CISSP CBK (Common Body of Knowledge).
- To prepare for a CISSP examination

## Course Highlights

- The only official course by official training center in Thailand
- All standard material from ISC2
- Official exam example from ISC2
- Free membership for ACIS Alumni
  - Access to the latest information related to the course subjects
  - A life-time class re-sit

## Learning Level

- Expert

## Course Duration

- 5 Days (30 Hours)

## Prerequisites

- None

## Target Group

- CIO,CISO, IT manager, IT Consultant, IT security professionals, IT Auditor

## Course Outline

### Domain 1: Access Control

- Module 1: Introduction to Access Control
- Module 2: Access Control Key Concepts, Methodologies, and Techniques
- Module 3: System Logging and Monitoring
- Module 4: Access Control Attacks and Threats
- Module 5: Access Control Effectiveness
- Module 6: Identify and Access Provisioning Lifecycle

### Domain 2: Application Security

- Module 1: Introduction to Telecommunications and Network Security
- Module 2: Network Models and System Architecture
- Module 3: The Network and IT Security
- Module 4: Understanding the Attack
- Module 5: Tools and Tasks in Network Security
- Module 6: Layer 1: Physical Layer
- Module 7: Layer 2: Data-link Layer
- Module 8: Layer 3: Network Layer
- Module 9: Layer 4: Transport Layer
- Module 10: Layer 5: Session Layer
- Module 11: Layer 6: Presentation Layer
- Module 12: Layer 7: Application Layer

### Domain 3: Business Continuity and Disaster Recovery Planning

- Module 1: Introduction to Information Security Governance and Risk Management
- Module 2: Information Security Governance
- Module 3: The Risk Management Process
- Module 4: Ethical Considerations in Information Security

### Domain 4: Cryptography

- Module 1: System Life Cycle Security
- Module 2: Systems Development Methodologies
- Module 3: Security Issues with Programming Languages
- Module 4: Assessing the Effectiveness of Software Security
- Module 5: Security Controls
- Module 6: Database Security

- Module 7: Application and Database Security Issues

## **Domain 5: Information Security and Risk Management**

- Module 1: Key Concepts and Common Terminology Used in Cryptography
- Module 2: Historical Aspect of Cryptography
- Module 3: Uses of Cryptography
- Module 4: The Cryptographic Life Cycle
- Module 5: Methods of Cryptography
- Module 6: The Different Encryption Systems
- Module 7: Algorithm Concepts
- Module 8: Methods of Cryptanalytic Attacks
- Module 9: Maintaining Network Security
- Module 10: Maintaining Application Security
- Module 11: Information Hiding Alternatives

## **Domain 6: Legal, Regulations, Compliance and Investigation**

- Module 1: Key Concepts and Definitions
- Module 2: Types of Security Models
- Module 3: Components of an Architecture
- Module 4: Basic Principles of System Design
- Module 5: Evaluation Models of Information Systems
- Module 6: Common Security Frameworks
- Module 7: Vulnerabilities and Threats

## **Domain 7: Operations Security**

- Module 1: Security Concepts and Activities
- Module 2: Protection of Resources
- Module 3: Preventive Measures
- Module 4: Change Management and Configuration Management
- Module 5: System Resilience and Fault Tolerance Requirements

## **Domain 8: Physical (Environmental) Security**

- Module 1: Processes Required for Planning the Project
- Module 2: Defining the Organization
- Module 3: Plan Implementation

## **Domain 9: Security Architecture and Design**

- Module 1: The Major Legal Systems in Information Security
- Module 2: International Law in Information Security



- Module 3: Supporting the Investigation
- Module 4: The Forensic Investigation
- Module 5: Hardware/Embedded Device Analysis
- Module 6: Compliance Processes and Procedures
- Module 7: Ensure Security in Contractual Agreements and Procurement Processes

## **Domain 10: Telecommunications and Network Security**

- Module 1: Definitions and Key Concepts
- Module 2: Site and Facility Design Considerations
- Module 3: Implementation and Operation of Perimeter Security
- Module 4: Implementation and Operation of Internal Security
- Module 5: Implementation and Operation of Facilities Security
- Module 6: Equipment Protection
- Module 7: Personnel Privacy and Safety

## **Recommended Courses**

- CISA : CISA Examination Preparation Program (CISA Certification)
- CISSP-BC : CISSP Exam Preparation Boot Camp

**สำรองที่นั่งและขอรับรายละเอียดเพิ่มเติมกรุณาติดต่อ (FOR MORE INFORMATION & REGISTRATION PLEASE CONTACT)**

คุณธนภัทร ไชยพิมล

Mr. Tanapat Chaipimol

Tel:(66) 2-650-5771 Ext.105 Fax: (66) 2-650 5776

Mobile: (66) 86-330-8532

Email: tanapat.ch@acisonline.net

คุณกิตมณี นิยมญาติ

Ms. Kitmanee Niyomyat

Tel:(66) 2-650-5771 ext. 108 Fax: (66) 2-650 5776

Mobile: (66) 86-325-7129

Email: kitmanee.ni@acisonline.net

### ACIS Professional Center Co.Ltd.

2101, 21 Fl., 62 The Millennia Building, Lungsuan Rd., Lumpini, Pathumwan, Bangkok 10330

Tel: +(66)2-650-5771 Fax: +(66)2-650-5776 Hotline: +(66)86-352-7129 Email: [registration@acisonline.net](mailto:registration@acisonline.net)

Website: [www.acisonline.net](http://www.acisonline.net)

