

## Course Title

(CISSP)<sup>®</sup> Course/Seminar



## Overview

The (ISC)<sup>2</sup> **Certified Information Systems Security Professional (CISSP)** course is the most comprehensive review seminar discussing information systems security industry best practices, known as the (ISC)<sup>2</sup> CBK – Common Body of Knowledge. The review seminar helps you review the 10 domains of the information security practice. It also serves as a strong learning tool for mastering concepts and topics related to all aspects of information systems security. The only official training course for CISSP certification.

## Length

5 days (Monday to Friday)

## Delivery

Instructor-led. Post-Seminar Self-Assessment

## Trainer

Authorised (ISC)<sup>2</sup> Trainer. CISSP Certified.

## Who should attend the class?

Information Security Managers, IT Managers, IT Security Managers, IT Security Administrators/Engineers, Project Managers, Project Coordinators. Those involved in formulating IT or Security policies for their organisations. Those involved in managing information security for their organisation.

## Course Outline

The course material, covering the 10 CISSP domains of the CBK, is redesigned and updated for every Review Seminar to reflect the latest information system security issues, concerns, and countermeasures. The following domains are covered in the seminar modules.

- **Security Management Practices** - Security Management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. Management tools such as data classification and risk assessment/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.
- **Security Architecture and Models** - The Security Architecture and Models domain contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality.
- **Access Control Systems and Methodology** - Access Controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

# COURSE INFORMATION

- **Application Development Security** - This domain addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.
- **Operations Security** - Operations Security is used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.
- **Physical Security** - The Physical Security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.
- **Cryptography** - The Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- **Telecommunications, Network, and Internet Security** - The Telecommunications, Network, and Internet Security domain discusses the:
  - Network structures
  - Transmission methods
  - Transport formats
  - Security measures used to provide availability, integrity, and confidentiality
  - Authentication for transmissions over private and public communications networks and media
- **Business Continuity Planning** - The Business Continuity Plan (BCP) domain addresses the preservation and recovery of business operations in the event of outages.
- **Law, Investigations, and Ethics** - The Law, Investigations, and Ethics domain addresses:
  - Computer crime laws and regulations
  - The measures and technologies used to investigate computer crime incidents

## Venue

One of the leading hotels in Bandar Seri Begawan  
**(Buffet Lunch and Tea breaks inclusive)**

## Tentative Date

Please contact eSuria Learning Centre representatives for confirmation.

## Course Fee (excluding exam fees)

**Early-Bird : BND 4,242 per participant**

(Confirmation received more than 30 days prior to course date).

**Standard : BND 4,582 per participant**

(Confirmation received less than 30 days prior to course date).

## Group Discounts

Special discounts provided for group registrations of 15 or more participants.

## Examination Information (Optional)

(CISSP)<sup>®</sup>

### Global Recognition for Top Information Security Professionals

As the first ANSI ISO accredited credential in the field of information security, the Certified Information Systems Security Professional (CISSP) certification provides information security professionals with not only an objective measure of competence but a globally recognized standard of achievement. The CISSP credential demonstrates competence in the 10 domains of the (ISC)<sup>2</sup> CISSP CBK.

The CISSP credential is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.

### Prerequisites

To sit for the CISSP examination, a candidate must:

- Submit the examination fee.
- Assert that he or she possesses a minimum of **four years** of professional experience in the information security field or three years plus a college degree. Additionally, a Master's Degree in Information Security from a National Center of Excellence can substitute for one year toward the four-year requirement.
- Complete the Candidate Agreement, attesting to the truth of his or her assertions regarding professional experience and legally commit to adhere to the CISSP Code of Ethics.
- Successfully answer four questions regarding criminal history and related background.

### Certification

To be issued a certificate, a candidate must:

- Pass the CISSP exam with a scaled score of 700 points or greater.
- Submit a properly completed and executed Endorsement Form.
- Successfully pass an audit of their assertions regarding professional experience, if the candidate is selected for audit.

### Venue

eSuria

Please contact eSuria Learning Centre representatives for confirmation.

### Date

To be announced.

(Please contact eSuria Learning Centre representatives for confirmation).

### Exam Fee

**Early-Bird : BND 848 per candidate**

(Confirmation received more than 30 days prior to exam date).

**Standard : BND 1,018 per candidate**

(Confirmation received less than 30 days prior to exam date).

## Trainer Profile

**Kevin Henry**  
**CISSP-ISSEP, CAP, SSCP, CISA**  
Vice President - Educational Services  
(ISC)<sup>2</sup> Institute



Kevin Henry, CISSP, is the Vice President of Educational Services at (ISC)<sup>2</sup> Institute. He is responsible for the management, support and delivery of all (ISC)<sup>2</sup> courses and examinations worldwide. Kevin has over twenty years experience providing Information Security and Audit services for many large corporations, state and local government and other organizations.

Kevin Henry is globally recognized as premier speaker and instructor at conferences and seminars, with an engaging and informative style of delivery, and his ability to impart his passion for the field of security and meet the needs of all types of audiences from security experts to senior management and users. Kevin graduated as a Computer Programmer Analyst from Red River College and has an Advanced Graduate Diploma in Management from Athabasca University.

Kevin has previously facilitated CISSP Seminars in Brunei Darussalam.

# COURSE INFORMATION

## Contact Info

Contact:	Nurin Almas Abdul Kadir or Rozy Hj Ahmad
Location:	Unit 9 First Floor, Block A Kiarong Complex, Bandar Seri Begawan BE1318, Brunei Darussalam.
Email:	<a href="mailto:learning@esuria.com.bn">learning@esuria.com.bn</a> <i>Please include your Name and Contact number in your email to us.</i>
Mobile:	(673)-8722636
Office:	(673)-2423721
Fax:	(673)-2454076
Website	<a href="http://www.esuria.com.bn/learning/offerings.htm">http://www.esuria.com.bn/learning/offerings.htm</a>