CSSLP

The Official CSSLP CBK Review Seminar (Accredited Training by (ISC²)

Course Introduction

The CSSLP CBK® Education Program is the exclusive way to learn security best practices and industry standards for the software lifecycle - critical information to a CSSLP. This is where you will learn tools and processes on how security should be built into each phase of the software lifecycle. The CSSLP CBK contains the largest, most comprehensive, collection of best practices, policies, and procedures, to ensure a security initiative across all phases of application development, regardless of methodology.

You will get an in-depth breakdown of the CSSLP Domains, while identifying key study areas, including:

- post-seminar self-assessment
- 100% up-to-date material
- Contributions from CSSLPs, (ISC)2 Authorized Instructors and subject matter experts
- An overview of the scope of security within software development

Course Objectives

- To offers a high-level review of the main topics of CSSLP CBK.
- To identify areas students need to study.
- To provide an overview of the scope of the information security field.
- To study for CSSLP examination

Course Highlights

- 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

- Secure Software Development Lifecycle (SSDLC)

Target Group

- Chief Information Officer / Chief Information Security Officer
- Network Infrastructure Manager /Director

- System Manager /Director
- Information Security Manager /Director

Course Outline

Domain 1 Secure Software Concepts

Security implications and methodologies within centralized and decentralized environments across the enterprise's computer systems in software development

Domain 2 Secure Software Requirements

Capturing security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.

Domain 3 Secure Software Design

Translating security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.

Domain 4 Secure Software Implementation/Coding

Involves the application of coding and testing standards, applying security testing tools including 'fuzzing', static-analysis code scanning tools, and conducting code reviews.

Domain 5 Secure Software Testing

Integrated QA testing for security functionality and resiliency to attack.

Domain 6 Software Acceptance

Security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, Common Criteria and methods of independent testing.

Domain 7 Software Deployment, Operations, Maintenance and Disposal

Security issues around steady state operations and management of software. Security measures that must be taken when a product reaches its end of life.

Recommended Course tracks

- CISSP : The Official CISSP CBK Review Seminar (Accredited Training by ISC²)

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
Website: www.acisonline.net