



Course code: 10008390

## Prove You on the Forefront of Cloud Security

In the ever-changing world of the cloud, you will face unique security challenges every day — from new threats, sensitive data, to uneducated internal teams.

Take command with the CCSP: the premier cloud security certification.

The CCSP is a global credential that represents the highest standard for cloud security expertise. It was co-created by (ISC)<sup>2</sup> and Cloud Security Alliance - leading stewards for information security and cloud computing security.

When you earn this cloud security certification, you prove to the world that you have deep knowledge and hands-on experience with cloud security architecture, design, operations and service orchestration. Start earning your CCSP today!

Training Date:	15 – 19 July 2019 (Mon – Fri)
Time:	09:00 – 18:00
Venue:	HKPC Building, 78 Tat Chee Avenue, Kowloon Tong, Kowloon
Enquiry Hotline:	(852) 2788 5884 - Ms Tracy Choy

Organiser:



Supporting Organisations:



## Course Introduction and Objective

The CCSP represents the highest standard for cloud security expertise. It demonstrates your deep knowledge and hands-on experience with cloud security architecture, design, operations and service orchestration. Is this cloud security certification right for you? The answer is yes, if you:

- Are an **experienced IT professional** who's involved with IT architecture, web and cloud security engineering, information security, governance, risk and compliance or IT auditing.
- Are **heavily involved with the cloud** (or you'd like to be) in a global environment. You're responsible for migrating to, managing or advising on the integrity of cloud-based software, such as Salesforce, Office 365, Optum, Impact Cloud, JIRA Software, SharePoint or CTERA.
- Are an **early adopter** who loves being on the leading edge of technology.
- Are **passionate about cloud security**.
- Want to **differentiate** yourself (or your business).
- Want to **stay up-to-speed** on rapidly evolving cloud technologies, threats and mitigation strategies.

In addition, many professionals who pursue the CCSP find it useful for working with organisations committed to DevSecOps, Agile or Bimodal IT practices.

The CCSP is ideal for those working in roles such as:

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

## Training Topics

This Official (ISC)<sup>2</sup> course provides a comprehensive review of cloud security concepts and industry best practices, covering the 6 domains of the CCSP CBK<sup>®</sup>: Architectural concepts and design requirements, cloud data security, cloud platform and infrastructure security, cloud application security, operations, legal and compliance.

<b><u>Day 1</u></b> 15 July 2019 (Mon)	<b>Architectural Concepts &amp; Design Requirements</b> (Domain 1) – Cloud computing concepts & definitions based on the ISO/IEC 17788 standard; security concepts and principles relevant to secure cloud computing.
<b><u>Day 2</u></b> 16 July 2019 (Tue)	<b>Cloud Data Security</b> (Domain 2) – Concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability in cloud environments.
<b><u>Day 3</u></b> 17 July 2019 (Wed)	<b>Cloud Platform &amp; Infrastructure Security</b> (Domain 3) – Knowledge of the cloud infrastructure components, both the physical and virtual, existing threats, and mitigating and developing plans to deal with those threats.
<b><u>Day 4</u></b> 18 July 2019 (Thu)	<b>Cloud Application Security</b> (Domain 4) – Processes involved with cloud software assurance and validation; and the use of verified secure software. <b>Operations</b> (Domain 5) – Identifying critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; requirements of cloud architecture to running and managing that infrastructure; definition of controls over hardware, media, and the operators with access privileges as well as the auditing and monitoring are the mechanisms, tools and facilities.

**Day 5**

19 July 2019 (Fri)

**Operations**

(Domain 5 Part 2)

**Legal & Compliance**

(Domain 6) – Addresses ethical behaviour and compliance with regulatory frameworks. Includes investigative measures and techniques, gathering evidence (e.g., Legal Controls, eDiscovery, and Forensics); privacy issues and audit process and methodologies; implications of cloud environments in relation to enterprise risk management.

**Revision and Mock Examination.**

# Training Outline

## CCSP Domains

### 1. Architectural Concepts & Design Requirements

Cloud computing concepts & definitions based on the ISO/IEC 17788 standard; security concepts and principles relevant to secure cloud computing.

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Identify Trusted Cloud Services

### 2. Cloud Data Security

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

- Understand Cloud Data Lifecycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

### 3. Cloud Platform & Infrastructure Security

Knowledge of the cloud infrastructure components, both the physical and virtual, existing threats, and mitigating and developing plans to deal with those threats.

- Comprehend Cloud Infrastructure Components
- Analyze Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery and Business Continuity Management

## 4. Cloud Application Security

Processes involved with cloud software assurance and validation; and the use of verified secure software.

- Recognise the need for Training and Awareness in Application Security
- Understand Cloud Software Assurance and Validation
- Use Verified Secure Software
- Comprehend the Software Development Life-Cycle (SDLC) Process
- Apply the Secure Software Development Life-Cycle
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

## 5. Operations

Identifying critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; requirements of cloud architecture to running and managing that infrastructure; definition of controls over hardware, media, and the operators with access privileges as well as the auditing and monitoring are the mechanisms, tools and facilities.

- Support the Planning Process for the Data Center Design
- Implement and Build Physical Infrastructure for Cloud Environment
- Run Physical Infrastructure for Cloud Environment
- Manage Physical Infrastructure for Cloud Environment
- Build Logical Infrastructure for Cloud Environment
- Run Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)
- Conduct Risk Assessment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

## 6. Legal & Compliance

Addresses ethical behaviour and compliance with regulatory frameworks. Includes investigative measures and techniques, gathering evidence (e.g., Legal Controls, eDiscovery, and Forensics); privacy issues and audit process and methodologies; implications of cloud environments in relation to enterprise risk management.

- Understand Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues, Including Jurisdictional Variation
- Understand Audit Process, Methodologies, and Required Adaptions for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design
- Execute Vendor Management

## Target Participants

To qualify for the CCSP certification, you must have:

A minimum of five years cumulative, paid, full-time work experience in information technology, of which three years must be in information security and one year in one or more of the six domains of the CCSP Common Body of Knowledge (CBK<sup>®</sup>).

- a. Earning CSA's [CCSK certificate](#) can be substituted for one year of experience in one or more of the six domains of the CCSP CBK.
- b. Earning (ISC)<sup>2</sup>'s [CISSP credential](#) can be substituted for the entire CCSP experience requirement.

### Don't have the required work experience yet?

You can take the CCSP exam to earn an [Associate of \(ISC\)<sup>2</sup> designation](#). Once you pass the exam, you'll have up to six years to earn your required work experience for the CCSP.

## Course Benefits

This training course will help candidates review and refresh their cloud security knowledge and help identify areas they need to study for the CCSP exam and features.

- Official (ISC)<sup>2</sup> courseware.
- Taught by an authorised (ISC)<sup>2</sup> instructor.
- Student handbook.
- Collaboration with classmates.
- Real-world learning activities and scenarios.

## Trainer – Dr Ricci leong

**CISSP, CISA, CISM, CEH, CCFP, ACE, CCSK v3/v4, CCSP, F.ISFS, GPEN, GIAC Advisory Board Member, ISSAP, ISSMP, M.Phil, MAArb, ISO 27001 LA, Star Auditor**

(ISC)<sup>2</sup> Authorised Instructor  
Principal Consultant and Founder  
eWalker Consulting (HK) Limited

Dr leong has over 15 years of industry experience in the Information Technology Industry as well as more than 15 years of experience in IT Security area specialised in Security Risk Assessment, IT Audit, Ethical Hacking & Penetration Test, Smart Card & Biometrics System deployment and Computer Forensics Investigation. He currently serves as Principal Consultant of eWalker Consulting (HK) Ltd.

He has worked for HP and founded the first HP e-Security Center (also known as Penetration Test Center) in Hong Kong. He has led and conducted over 100 security assessments, IT Security Audits, penetration tests and incident handling services for HKSAR government departments, banks and multinational organisation in Hong Kong throughout these years. He is one of the founding instructors in the first diploma and graduate diploma course in computer security and forensics investigation recognised by HKSAR law enforcement team. In year 2002, Dr leong was invited by HKSAR government HK Police Force to courtroom as the first expert witness in HK Computer Crime Investigation.

He was awarded the (ISC)<sup>2</sup> Asia-Pacific Information Security Leadership Achievements (ISLA) Honoree – Senior Information Security Professional in 2017 for his contribution in conducting security education. He participated in developing the first Digital Forensics training in Hong Kong in 1999. Since then, he planned and conducted postgraduate digital forensics courses in HKUST, HKUSpace. Currently, he is the Adjunct Assistant Professor of the Hong Kong University of Science & Technology as well as part-time lecturer on CyberSecurity course.

He is authorised (ISC)<sup>2</sup> Certified Cloud Security Professional (CCSP) and Certificate of Cloud Security Knowledge (CCSK) trainer.

He is also the founding member and council member of Information Security and Forensics Society of Hong Kong, Vice President of Professional Development of Cloud Security Alliance (HK & Macau Chapter).

## Assistant Trainer – Mr Rafael Wong

**CISSP, CISM, CISA, CCSP, CCSK, CEH, GPEN, GWAPT, GCFA**

(ISC)<sup>2</sup> Authorised Instructor  
Senior Consultant  
eWalker Consulting (HK) Limited

Rafael currently serves as Senior Consultant of eWalker Consulting (HK) Ltd. and has more than 7 years of industry experience specialising in Security Risk Assessment, IT Audit, Ethical Hacking, Penetration Test and Computer Forensics Investigation.

Throughout Rafael's career in IT security field, he has conducted numerous cloud security related training and workshop with Dr Ricci leong for various organisation, such as Hewlett-Packard (HPE), Hong Kong Productivity Council (HKPC) and so on.



He is authorised (ISC)<sup>2</sup> Certified Cloud Security Professional (CCSP) and Certificate of Cloud Security Knowledge (CCSK) trainer.

Regarding to the Cloud Assessment, Rafael has conducted corresponding security assessment and audit, including public and private cloud security review, cloud application penetration test, for various enterprises.

## Mode of Delivery

### Classroom - Based Training

- The most thorough review of the CCSP CBK, industry concepts and best practices.
- Five-day training event delivered in a classroom setting. Eight hours a day.
- Available at (ISC)<sup>2</sup> facilities and through (ISC)<sup>2</sup> Official Training Providers worldwide.
- Led by authorised instructors.

## Medium of Instruction

Cantonese with training materials in English

## Application Procedures

1. Please fill in the Enrollment Form in BLOCK LETTERS and send it by Email: [tracyc@hkpc.org](mailto:tracyc@hkpc.org) or Fax No. (852) 2190 9784.
2. Prepare a crossed cheque payable to “Hong Kong Productivity Council”, and mail it together with the completed enrollment form to the following address: Ms Tracy Choy, 2/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong.
3. HKPC will send an email confirmation to the registered participants after receiving the payment.

## Certificate of training

Participants who have attained at least 80% attendance of lecture will be awarded a **certificate of completion issued by The International Information System Security Certification Consortium, Inc., (ISC)<sup>2</sup>**.

## CCSP Examination Procedures

You can visit the computer-based testing partner at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2) to set up your account, schedule your exam and settle payment directly. On your scheduled exam day, you'll have four hours to complete the 125 exam questions. You must pass the exam with a scaled score of 700 points or greater.

If you would like to understand more about the examination, kindly download the CCSP Exam Outline (<https://cert.isc2.org/ccsp-exam-outline-form/>) for your reference.

Please feel free to contact Ms Tracy Choy at (852) 2788 5884 or [tracyc@hkpc.org](mailto:tracyc@hkpc.org) for enquiry.

# Cloud Security Certification | CCSP® – Certified Cloud Security Professional ENROLMENT FORM

**\* EARLY BIRD price on or before 14 June 2019**

1. Please "√" the training fee and complete the form below for reservation!

	Early Bird Price		Regular Price	
	Non-Member	Member of Organizer/ Supporting Organization	Non-Member	Member of Organizer/ Supporting Organization
<b>Training Date: (15 – 19 July 2019)</b>	<input type="checkbox"/> HK\$12,500	<input type="checkbox"/> HK\$11,500	<input type="checkbox"/> HK\$13,500	<input type="checkbox"/> HK\$12,500

CPE Hours: A number of supporting organisations have indicated that recognition credits will be awarded for attendance and participation in the Training on Certified Cloud Security Professional. Please check with your local organisation for the level of credits you will be entitled to receive.

2. Please fill in the form below to complete registration:

Company/Organisation:		
Name: (*Shown on Training Attendance Certificate)	*Surname	*First Name
Position:		
Phone:		
Mobile:		
Email:		
Address:		
Name of Supporting Organisation (if any):		
Course Fee pay/sponsor by:	<input type="checkbox"/> Myself	<input type="checkbox"/> Company/Organisation

### Consent statement

Personal data (including your name, phone number, fax number, correspondence address and email address) provided by you will be used for the purpose of the administration, evaluation and management of your registration by HKPC or HKPC's agent. You have the right to request access to, and amend your personal data in relation to your application. If you wish to exercise these rights, please send email to: edm@hkpc.org.

HKPC intends to use the personal data (including your name, phone number, correspondence address and email address) that you have provided to promote the latest development, consultancy services, events and training courses of HKPC. Should you find such use of your personal data not acceptable, please indicate your objection by ticking the box below:

- I disagree to the proposed use of my personal data in any marketing activities arranged by HKPC.
- I disagree to the proposed transfer of my personal data in any marketing activities arranged by (ISC)<sup>2</sup>.