Cloud Security Certification | CCSP® – Certified Cloud Security Professional

Course code: 10006308

Prove You're on the Forefront of Cloud Security

In the ever-changing world of the cloud, you face unique security challenges every day — from new threats to 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)² and Cloud Security Alliance — leading stewards for information security and cloud computing security.

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

Training Date	:	8 – 12 October 2018 (Mon - Fri)
Time	:	09:00 – 18:00
Venue	:	1/F, HKPC Building, 78 Tat Chee Avenue, Kowloon
Enquiry Hotline	:	(852) 2788 5884 - Ms. Tracy Choy

Organizers:

HKPC Hong Kong Productivity Council 香港生產力促進局

(ISC)² OFFICIAL TRAINING PROVIDER

Supporting Organizations:

ACFE Association of Certified Fraud Examiners Hong Kong Chapter

CSA cloud security alliance

CAHK 香港通訊業聯會 Communications Association of Hong Kong

HKCERT

Hong Kong Computer Society

WTIA 香港無線科技商會

HTCIA High Technology Crime Investigation Association Asia Pacific Chapter

ISSA

Internet Society Hong Kong Chapter

CPS 澳門電腦學會 Macao Computer Society

PISA

Course Introduction and Objective

The CCSP represents the highest standard for cloud security expertise and 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 organizations 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)^2 course provides a comprehensive review of cloud security concepts and industry best practices, covering the 6 domains of the CCSP CBK®: Architectural concepts and design requirements, cloud data security, cloud platform and infrastructure security, cloud application security, operations, legal and compliance.

Day 1 8 Oct 2018 (Mon)	**Architectural Concepts & Design Requirements** (Domain 1) – Cloud computing concepts & definitions based on the ISO/IEC 17788 standard; security concepts and principles relevant to secure cloud computing.
Day 2 9 Oct 2018 (Tue)	**Cloud Data Security** (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.
Day 3 10 Oct 2018 (Wed)	**Cloud Platform & Infrastructure Security** (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.
Day 4 11 Oct 2018 (Thu)	**Cloud Application Security** (Domain 4) – Processes involved with cloud software assurance and validation; and the use of verified secure software. **Operations** (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 12 Oct 2018 (Fri)	**Operations** (Domain 5 Part 2) **Legal & Compliance** (Domain 6) – Addresses ethical behavior 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.

    - Recognize 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 behavior 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®).

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)²'s CISSP credential can be substituted for the entire CCSP experience requirement.

Don't have the required work experience yet?
You can take and pass the CCSP exam to earn an Associate of (ISC)² designation. Then, 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)² courseware.
- Taught by an authorized (ISC)² instructor.
- Student handbook.
- Collaboration with classmates.
- Real-world learning activities and scenarios.

Trainer – Dr. Ricci Ieong

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)²-Authorized Instructor
Principal Consultant and Founder
eWalker Consulting Limited

Dr. Ieong 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 specialized 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 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 organization 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 recognized by HKSAR law enforcement team. In year 2002, Dr. Ieong 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)^2 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 authorized (ISC)^2 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)²-Authorized Instructor
Senior Consultant
eWalker Consulting Limited

Rafael currently serves as senior consultant of eWalker Consulting Ltd. And has more than 7 years of industry experience specializing 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 Ieong for various organization, such as Hewlett-Packard (HPE), Hong Kong Productivity Council (HKPC) and so on.

He is authorized $(ISC)^2$ Certified Cloud Security Professional (CCSP) and Certificate of Cloud Security Knowledge (CCSK) trainer.

Regarding to 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

Computer Room - Based Training

- Ideal for hands-on learners. The most thorough review of the CCSP CBK, industry concepts and best practices.
- Five-day training event delivered in a computer setting. Eight hours a day.
- Available at (ISC)² facilities and through (ISC)² Official Training Providers worldwide.
- Led by authorized 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 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)^2.

CCSP Examination Procedures

You can visit the computer-based testing partner at 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 for enquiry.

Coud Security Certification | CCSP® – Certified Cloud Security Professional

ENROLLMENT FORM

*** EARLY BIRD price on or before 21 September 2018**

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

	Early Bird Price		Normal Price	
	Non-Member	Member of Organizer/ Supporting Organization	Non-Member	Member of Organizer/ Supporting Organization
Training Date: (8 – 12 Oct 2018)	□ HK$12,500	□ HK$11,500	□ HK$13,500	□ HK$12,500

CPE Hours: A number of supporting organizations 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 organization for the level of credits you will be entitled to receive.

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

*Company/ Organization:		
*Name: (Shown on Training Attendance Certificate only)	*Surname	*First Name
*Position:		
*Phone:		
*Mobile:		
*Email:		
*Address:		
Name of Supporting Organization (if any):		

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 $(ISC)^2$.