hkpc Academy 生產力學院

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong 香港九龍達之路 78 號生產力大樓 T +852 2788 6342 F +852 2788 6260 www.hkpcacademy.org

Exhibit Expertise at 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 unskilled internal team members.

Take command of the **Certified Cloud Security Professional (CCSP®)**, the premier cloud security certification, in order to address these challenges.

The CCSP is a global credential representing the highest standard of cloud security expertise. It is co-created by (ISC)² and Cloud Security Alliance – the leading stewards for information security and cloud computing security.

Acquiring this cloud security certification is a proof to the world that you have gained deep knowledge and hands-on experience on cloud security architecture, design, operations and service orchestration. Start pursuing your CCSP today!

Training Date:	17–19 & 24-25 March 2020 (5 days)
Time:	09:00 – 18:00, 40 Hours in Total
Venue:	HKPC Building, 78 Tat Chee Avenue, Kowloon Tong, Kowloon
Inquiry Hotline:	+852 2788 5884 (Ms Tracy CHOY)

Ideal for those performing the following roles:

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

Course Introduction and Objectives

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

- are an **experienced IT professional** engaging in IT architecture, web and cloud security engineering, information security, governance, risk and compliance or IT auditing;
- are **heavily involved in the cloud** application (or you would like to be) in a global environment. You are 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 cutting-edge technologies;
- are **passionate about cloud security;**
- want to **differentiate** yourself (or your business);
- want to **stay up-to-speed** with the ever-evolving cloud technologies, threats and mitigation strategies.

In addition, many professionals who pursue the CCSP find it useful in terms of working with organisations dedicated to DevSecOps, Agile or Bimodal IT practices.

Course Benefits

This training course helps participants review and refresh their cloud security knowledge and identify areas that they need to study for the CCSP examination and the required features.

- Official (ISC)² electronic courseware
- Taught by an authorised (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Organisers:

Supporting Organisations:

Training Topics

This official (ISC)² course provides a comprehensive overview of cloud security concepts and industry best practices, covering six 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 17 March 2020 (Monday)	**Cloud Concepts, Architecture and Design** (Domain 1) – Cloud computing concepts & definitions based on the ISO/IEC 17788 standard; security concepts and principles relevant to securing cloud computing.
Day 2 18 March 2020 (Tuesday)	**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 environment.
Day 3 19 March 2020 (Wednesday)	**Cloud Platform and Infrastructure Security** (Domain 3) – Knowledge of the cloud infrastructure components, both physical and virtual, existing threats, and mitigating and developing plans to deal with threats.
Day 4 24 March 2020 (Thursday)	**Cloud Application Security** (Domain 4) – Processes involving cloud software assurance and validation; the use of verified secure software as well as Secure Software Development Life Cycle Process; and Identity and Access Management Solutions for Cloud Environment. **Cloud Security Operations** (Domain 5 - Part 1) – Identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; requirements of cloud architecture on running and managing that infrastructure; definition of controls over hardware, media, and the operators with access privileges as well as the auditing and monitoring of mechanisms, tools and facilities.

Day 5 25 March 2020 (Friday)	**Cloud Security Operations** (Domain 5 - Part 2) **Legal, Risk and Compliance** (Domain 6) – Address topics related to ethical behaviour and compliance with regulatory frameworks, including investigative measures and techniques, gathering evidence (e.g. Legal Controls, eDiscovery, and Forensics); privacy issues and audit process and methodologies; implications of cloud environment in relation to enterprise risk management. **Revision and Mock Examination.**

Training Outlines

CCSP Domains

1. Cloud Concepts, Architecture and Design

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

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Evaluate Cloud Service Providers

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 environment.

- Describe Cloud Data Concepts
- Design and Implement Cloud Data Storage Architecture
- Design and Apply Data Security Technologies and Strategies
- Implement Data Discovery
- Implement Data Classification
- Design and Implement Information Rights Management (IRM)
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

3. Cloud Platform and Infrastructure Security

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

- Comprehend Cloud Infrastructure Components
- Design a Secure Data Centre
- Analyse Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery (DR) and Business Continuity (BC)

4. Cloud Application Security

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

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

5. Cloud Security Operations

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

1. Implement and Build Physical Infrastructure for Cloud Environment
2. Operate Physical and Logical Infrastructure for Cloud Environment
3. Manage Physical and Logical Infrastructure for Cloud Environment
4. Implement Operational Controls and Standards (e.g. Information Technology Infrastructure Library (ITIL), International Organisation for Standardisation / International Electrotechnical Commission (ISO/IEC) 20000-1)
5. Support Digital Evidence
6. Manage Communication with Relevant Parties
7. Manage Security Operations

6. Legal, Risk and Compliance

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

- Articulate Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues
- 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

Target Participants

To be eligible 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 requirements.

Haven't got the required work experience yet?

You can take the CCSP examination to earn an Associate of (ISC)² designation. Once you pass the exam, you will have up to six years to earn your required work experience for the CCSP.

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)² 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 Centre (also known as Penetration Test Centre) in Hong Kong. He has led and conducted over 100 security assessments, IT security audits, penetration tests and incident handling services for the HKSAR government departments, banks and multinational organisations 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 the HKSAR law enforcement team. In 2002, Dr LEONG was invited by the Hong Kong Police Force to the courtroom as the first expert witness in a Hong Kong computer crime investigation.

Dr LEONG was awarded the (ISC)² Asia-Pacific Information Security Leadership Achievements (ISLA) Honouree – 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 the Hong Kong University of Science & Technology (HKUST), HKU Space. Currently, he is the Adjunct Assistant Professor of the HKUST as well as part-time lecturer on cyber security course.

He is an authorised (ISC)² CCSP and Certificate of Cloud Security Knowledge (CCSK) trainer.

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

Assistant Trainer – Mr Rafael WONG

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

(ISC)² Authorised Instructor
Senior Consultant
eWalker Consulting (HK) Limited

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

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

He is an authorised (ISC)² CCSP and CCSK trainer.

Regarding 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 per day.
- Take place in (ISC)² facilities and through (ISC)² official training providers worldwide.
- Led by authorised instructors.

Medium of Instruction

Cantonese with training materials in English

Certificate of Training

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

RTTP Funding

This course is approved for Reindustrialisation and Technology Training Programme (RTTP), which offers up to 2/3 course fee reimbursement upon successful applications. For details: https://rttp.vtc.edu.hk.

RTTP Training Grant Application
Companies should submit their RTTP training grant application for their employee(s) via https://rttp.vtc.edu.hk/rttp/login at least two weeks before course commencement. Alternatively, application form could be submitted by email to rttp@vtc.edu.hk along with supporting documents.

CCSP Examination Procedures

You can visit the computer-based testing partner at www.pearsonvue.com/isc2 to set up your account, schedule your examination and settle payment directly. On your scheduled exam day, you will have four hours to complete the 125 exam questions. You must pass the exam with a scaled score of 700 points or more. For more details, please visit: https://www.isc2.org/Certifications/CCSP.

If you would like to understand more about the exam, kindly view the link: https://www.isc2.org/Register-for-Exam for your reference.

Enrolment & Payment Method

You may make payment by credit cards, EPS or cheques. Amount received will be imprinted on the official receipt. Only receipt printed with receipt printers at HKPC is valid. Receipt of cheque payment is subject to bank clearance.

HKPC will send an email confirmation to the registered participant after receiving the payment.

The deadline submission of the training application is scheduled on 6 March 2020. Late submission will NOT be considered.

1. Scan the QR code to complete the enrolment and payment online.

2. Enrolment form can be downloaded at https://www.hkpcacademy.org/en/enrollment.jspx.

3. Training Fee
   Early bird price ***on or before 21 February 2020***
   - Non-member: HK$12,500 per person
   - Member of Organiser / Supporting Organisation: HK$11,500 per person

   Regular Price
   - Non-member: HK$13,500 per person
   - Member of Organiser / Supporting Organisation: HK$12,500 per person

4. By Crossed Cheque
   Mail the crossed cheque with payee name "Hong Kong Productivity Council" (in HK dollar) and the application form should be mailed to Hong Kong Productivity Council, 2/F, HKPC Building, 78 Tat Chee Avenue, Kowloon (attention to Ms Tracy Choy). Please indicate the course name and your name on the envelope.

5. By Direct Bank Transfer / By e-Cheque
   Name of account : HONG KONG PRODUCTIVITY COUNCIL
   Banker's name : Standard Chartered Bank (Hong Kong) Limited
   Banker's address : 4-4A Des Voeux Road Central, Hong Kong
   HKD account no. : 447-1-071900-3 (Receipt of HKD and other currencies)
   SWIFT code : SCBLHKHHXXX
   Note: Please send payment advice/remittance/bank in slip to email : tracyc@hkpc.org or fax number : (852) 2190 9784

6. By Cheque/Cash/Credit Card Payment
   Visit the registration counter of HKPC Academy, Hong Kong Productivity Council (1st Floor, HKPC Building, 78 Tat Chee Avenue, Kowloon) to enrol and settle the course fee.
   Office hours: Monday to Friday 09: 00-21: 00 | Saturday 09: 00-17: 00

Inquiry

Please feel free to contact Ms Tracy CHOY at +852 2788 5884 or tracyc@hkpc.org for inquiry.