Official Training Partner

Course Fee: HK$19,500 (May apply up to HK$13,000 subsidy)

* Maximum saving, with the final grant subjects to approval.

In the ever-changing world of cloud computing, there are 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, to address these challenges through this official training.

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

Programme code	10016345
Date and time	20-22/11 & 25-26/11/2024 (40 hours) 09:00 - 18:00 (40 hours in total)
Venue	Physical Class : 1/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, H.K.
Medium	Cantonese with training materials in English
Fee	**Early bird price: 6 weeks before course start date** - Staff of Organiser, Member of ISC2 or Supporting Organisation: **HK$17,200** per person - Non-member: **HK$18,200** per person **Regular price** - Staff of Organiser, Member of ISC2 or Supporting Organisation: **HK$18,500** per person - Non-member: **HK$19,500** per person
Remarks	Deadline for submission is 4 weeks before course start date. Late submission will NOT be considered.

Exhibit Expertise at the Forefront of Cloud 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!

Ideal for those performing the following roles:

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

This course is subject to approval under the Reindustrialisation and Technology Training Programme (RTTP) with up to 2/3 course fee reimbursement upon successful applications. For details: https://rttp.vtc.edu.hk.

Who Should Attend

The CCSP represents the highest standard for cloud security expertise. 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;
- **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;
- an **early adopter** who loves cutting-edge technologies;
- **passionate about cloud security;**
- eager to **differentiate** yourself (or your business);
- eager to **stay up-to-speed** with the ever-evolving cloud technologies, threats and mitigation strategies.

In addition, professionals who pursue the CCSP for collaborating with organisations dedicated to DevSecOps, Agile or Bimodal IT practices.

Course Benefits

This course helps participants review and refresh their cloud security knowledge, get well-prepared for the CCSP examination.

- Official $(ISC)^2$ courseware
- Taught by an authorised $(ISC)^2$ instructor
- Comprehensive student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Inquiry Ms LEE| +852 2788 5704 | cybersec@hkpc.org
Mr WUT | +852 2788 5404 | cybersec@hkpc.org

Training Schedule and 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.

Date	Activities
Day 1	**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	**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	**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	**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.

Inquiry Ms LEE| +852 2788 5704 | cybersec@hkpc.org
Mr WUT | +852 2788 5404 | cybersec@hkpc.org

Date	Activities
Day 5	**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**

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

Classroom-based Training

- The most thorough review of CCSP CBK, industry concepts and best practices.
- Five-day training event delivered in a classroom setting. Eight hours per day.
- Take place in ISC2 facilities and through (ISC)² official training providers worldwide.
- Led by authorised instructors.

Prerequisite

To be eligible for 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 CCSP Common Body of Knowledge (CBK®).
- Earning CSA's CCSK certificate can be substituted for one year of experience in one or more of the six domains of CCSP CBK.
- Earning ISC2 CISSP credential can be substituted for the entire CCSP experience requirements.

Haven't got the required work experience yet?

You can take CCSP examination to earn an Associate of ISC2 designation. Once you pass the exam, you will have up to six years to earn your required work experience for CCSP.

Inquiry Ms LEE| +852 2788 5704 | cybersec@hkpc.org
Mr WUT | +852 2788 5404 | cybersec@hkpc.org

Mr Bernard KAN

CISSP, CCSP, GCIA, GCIH, CWSP, CCNP, MCSE, CEC
(ISC)² Authorised Instructor

Bernard KAN is an (ISC)2 Certified Trainer with over 20 years of information security experience as a security team leader in Banking, Telecommunication industry and CERT community.

Bernard has been delivering information security training to enterprises, talks to the public in security conference and sharing sessions to NGOs and he was a frequent speaker for security awareness training. He was a part-time lecturer for City University of Hong Kong for a post-graduate Information Security certificate course for 6 years. Bernard acquired several professional certifications including CISSP, GCIA, GCIH, CWSP, CCNP, MCSE and CEC. He also has a Master of Science degree in E-Commerce.

Dr Ricci IEONG

CISSP, CISA, CCSK, CCSP, CCFP, CEH, F.ISFS, ISSMP, ISSAP, ISO 27001LA, STAR Auditor

Dr Ieong has over 15 years of experience in the Information Technology Industry and 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.

Dr Ieong is the founding member and Council member of the Information Security and Forensics Society (ISFS). He recently founded the Cloud Security Alliance Hong Kong and Macau Chapter and participated as Director of Education. He has conducted over 20 technical IT security training and workshop on cloud computing security, and provided cloud security awareness training to the public.

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., ISC2.**

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 Methods

1. Scan the QR code to complete the enrolment.
2. 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, 3/F, HKPC Building, 78 Tat Chee Avenue, Kowloon (attention to Ms June LEE). Please indicate the course name and course code on the envelope.

   (Only receipt printed with receipt printers at HKPC is valid. Receipt of cheque payment is subject to bank clearance.)

NITTP Training Grant Application

Companies should submit their NITTP training grant application for their employee(s) via https://nittp.vtc.edu.hk/rttp/login at least **five weeks before** course commencement. Alternatively, application form could be submitted to the Secretariat in person, by post, by fax or by email to nittp@vtc.edu.hk together with supporting documents.

Supporting Organisations (in arbitrary order)

ACFE Association of Certified Fraud Examiners Hong Kong Chapter 特許詐欺審查師學會香港分會

iTLE

CSA cloud security alliance CSA Hong Kong and Macau Chapter

CAHK Communications Association of Hong Kong

香港工業總會 FHKI Federation of Hong Kong Industries

HKCERT

Hong Kong Computer Society 香港電腦學會

Information Security Group Hong Kong www.hkisg.org

Hong Kong Software Industry Association 香港軟件行業協會

WTIA 香港無線科技商會

isfs Information Security and Forensics Society

HTCIA High Technology Crime Investigation Association

ISSA

Internet Society Hong Kong Chapter

ISACA Macao Chapter

澳門電腦學會 Macao Computer Society

PISA

HKAECE 香港電腦教育學會 The Hong Kong Association for Computer Education