Course code: 10006308

Prove you have what it takes to protect your organization from malicious hackers and threats with the **Certified Information Systems Security Professional (CISSP®) certification**. Demonstrate your knowledge, advance your career and become a member of a 130,000-strong community of cybersecurity leaders setting the bar for professionals across the information security workforce.

Training Date	:	25 – 29 June 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

Organizer:

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 特許詐騙審查師學會-香港分會

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

PISA

Course Introduction and Objective

Get the Premier Cybersecurity Certification

You live and work on the forefront of information security. Every day malicious hackers grow smarter. You always have to stay one step ahead to keep your company safe.

Prove you have what it takes with the CISSP certification!

This cybersecurity certification is an elite way to demonstrate your knowledge, advance your career and become a member of a community of cybersecurity leaders. It shows you have all it takes to design, engineer, implement and run an information security program.

The CISSP is an objective measure of excellence. It’s the most globally recognized standard of achievement in the industry. And this cybersecurity certification was the first information security credential to meet the strict conditions of ISO/IEC Standard 17024.

Training Topics

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security.

Day 1 25 Jun 2018 (Mon)	– Security and Risk Management – Asset Security
Day 2 26 Jun 2018 (Tue)	– Asset Security – Security Architecture and Engineering
Day 3 27 Jun 2018 (Wed)	– Security Architecture and Engineering – Communication and Network Security – Identity and Access Management (IAM)
Day 4 28 Jun 2018 (Thu)	– Identity and Access Management (IAM) – Security Assessment and Testing – Security Operations
Day 5 29 Jun 2018 (Fri)	– Security Operations – Software Development Security

Training Outline

1. Security and Risk Management

1.1 Understand and apply concepts of confidentiality, integrity and availability

1.2 Evaluate and apply security governance principles

- Alignment of security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks
- Due care/due diligence

1.3 Determine compliance requirements

- Contractual, legal, industry standards, and regulatory requirements
- Privacy requirements

1.4 Understand legal and regulatory issues that pertain to information security in a global context

- Cyber crimes and data breaches
- Licensing and intellectual property requirements
- Import/export controls
- Trans-border data flow
- Privacy

1.5 Understand, adhere to, and promote professional ethics

- (ISC)² Code of Professional Ethics
- Organizational code of ethics

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements

- Develop and document scope and plan
- Business Impact Analysis (BIA)

1.8 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policies
- Onboarding and termination processes
- Vendor, consultant, and contractor agreements and controls
- Compliance policy requirements
- Privacy policy requirements

1.9 Understand and apply risk management concepts
- Identify threats and vulnerabilities
- Risk assessment/analysis
- Risk response
- Countermeasure selection and implementation
- Applicable types of controls (e.g., preventive, detective, corrective)
- Security Control Assessment (SCA)
- Monitoring and measurement
- Asset valuation
- Reporting
- Continuous improvement
- Risk frameworks

1.10 Understand and apply threat modeling concepts and methodologies
- Threat modeling methodologies
- Threat modeling concepts

1.11 Apply risk-based management concepts to the supply chain
- Risks associated with hardware, software, and services
- Third-party assessment and monitoring
- Minimum security requirements
- Service-level requirements

1.12 Establish and maintain a security awareness, education, and training program
- Methods and techniques to present awareness and training
- Periodic content reviews
- Program effectiveness evaluation

2. Asset Security

2.1 Identify and classify information and assets
- Data classification
- Asset Classification

2.2 Determine and maintain information and asset ownership

2.3 Protect privacy
- Data owners
- Data processers
- Data remanence
- Collection limitation

2.4 Ensure appropriate asset retention
2.5 Determine data security controls
- Understand data states
- Scoping and tailoring
- Standards selection
- Data protection methods

2.6 Establish information and asset handling requirements

3. Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles
3.2 Understand the fundamental concepts of security models
3.3 Select controls based upon systems security requirements
3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems
- Distributed systems
- Internet of Things (IoT)

3.6 Assess and mitigate vulnerabilities in web-based systems
3.7 Assess and mitigate vulnerabilities in mobile systems
3.8 Assess and mitigate vulnerabilities in embedded devices
3.9 Apply cryptography
- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)

3.10 Apply security principles to site and facility design
3.11 Implement site and facility security controls
- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression

4. Communication and Network Security

4.1 Implement secure design principles in network architectures
- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking
- Implications of multilayer protocols
- Converged protocols
- Software-defined networks
- Wireless networks

4.2 Secure network components
- Operation of hardware
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security
- Content-distribution networks

4.3 Implement secure communication channels according to design
- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks

5. Identity and Access Management (IAM)

5.1 Control physical and logical access to assets
- Information
- Systems
- Devices
- Facilities

5.2 Manage identification and authentication of people, devices, and services
- Identity management implementation
- Single/multi-factor authentication
- Accountability
- Session management
- Registration and proofing of identity
- Federated Identity Management (FIM)
- Credential management systems

5.3 Integrate identity as a third-party service
- On-premise
- Cloud
- Federated

5.4 Implement and manage authorization mechanisms
- Role Based Access Control (RBAC)
- Rule-based access control
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Attribute Based Access Control (ABAC)

5.5 Manage the identity and access provisioning lifecycle
- User access review
- System account access review
- Provisioning and deprovisioning

6. Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies
- Internal
- External
- Third-party

6.2 Conduct security control testing
- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing

6.3 Collect security process data (e.g., technical and administrative)
- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

6.4 Analyze test output and generate report

6.5 Conduct or facilitate security audits
- Internal
- External
- Third-party

7. Security Operations

7.1 Understand and support investigations
- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

7.2 Understand requirements for investigation types
- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

7.3 Conduct logging and monitoring activities
- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring

7.4 Securely provisioning resources
- Asset inventory
- Asset management
- Configuration management

7.5 Understand and apply foundational security operations concepts
- Need-to-know/least privileges
- Separation of duties and responsibilities
- Privileged account management
- Job rotation
- Information lifecycle
- Service Level Agreements (SLA)

7.6 Apply resource protection techniques
- Media management
- Hardware and software asset management

7.7 Conduct incident management
- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.8 Operate and maintain detective and preventative measures
- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management

7.10 Understand and participate in change management processes

7.11 Implement recovery strategies
- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, high availability, Quality of Service (QoS), and fault tolerance

7.12 Implement Disaster Recovery (DR) processes
- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness

7.13 Test Disaster Recovery Plans (DRP)
- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.16 Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress

8. Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies
- Maturity models
- Operation and maintenance
- Change management
- Integrated product team

8.2 Identify and apply security controls in development environments

- Security of the software environments
- Configuration management as an aspect of secure coding
- Security of code repositories

8.3 Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces
- Secure coding practices

Target Participants

To qualify for this cybersecurity certification, you must have:

- At least five years of cumulative, paid, full-time work experience.

- In two or more of the eight domains of the $(ISC)^2$ CISSP Common Body of Knowledge (CBK).

- Don't have enough work experience yet? There are two ways you can overcome this obstacle.

You can satisfy one year of required experience with:

- A four-year college degree (or a regional equivalent).

- Or, an approved credential from the CISSP Prerequisite pathway.

Your second option is to take and pass the CISSP 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 CISSP.

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 CISSP 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.
- A certificate of completion

Trainer – Mr. Frank Chow

Frank Chow has more than twenty years of extensive solid working experience in the cyber security industry across Asia-Pacific. He is an advocate of a number of international leading practices, such as implementing ISO27001 information security management, ISO27017 cloud security, ISO20000 IT service management, and ISO22301 business continuity management. He is a high profile speaker for major industry events and training sessions.

Over the years, he received recognition for his efforts - $(ISC)^2$ Asia Pacific Information Security Leadership Achievements Program and BCI Asia Business Continuity Awards and HKCS Outstanding ICT Achiever Award.

He holds a variety of professional certificates such as the CCSP, CISSP, ISSAP, ISSMP, CSSLP, C|CISO, CGEIT, CRISC, CISM, CISA, CBCP, TOGAF, PMP, CCSK etc.

Mode of Delivery

Computer Room-based Training

- Ideal for hands-on learners. The most thorough review of the CISSP 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 (ISC)^2.

CISSP Examination Procedures

(ISC)² has introduced Computerized Adaptive Testing (CAT) for all English CISSP exams worldwide. 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 THREE hours to complete the 100 - 150 exam questions. You must pass the exam with a scaled score of 700 points or greater. For more details, please visit: www.isc2.org/Certifications/CISSP/CISSP-Cat.

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that CISSP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

If you would like to understand more about the examination, kindly download the CISSP 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.

ENROLLMENT FORM

*** EARLY BIRD price on or before 15 June 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: (25 – 29 June 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 Information Systems Security Professional (CISSP). 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 un-ticking the box below:

☐ I agree to the proposed use of my personal data in any marketing activities arranged by HKPC.

☐ I agree to the proposed transfer of my personal data in any marketing activities arranged by $(ISC)^2$.