Certified Information Systems Security Professional (CISSP®) Official Training

CISSP® Certified Information Systems Security Professional

THE INDUSTRY LEADING CREDENTIAL

This globally recognized certification in cyber security is elite to demonstrating your knowledge in designing, engineering, implementing and running an information security programme, providing opportunities for you to advance your career.

Prove you have what it takes to protect your organisation from malicious hackers and threats with the Certified Information Systems Security Professional (CISSP®) Official Training.

Programme code	10010399
Date and time	22 August 2020 – 3 October 2020 *Physical Class (4 classes)* 09:00 – 13:00 (Sat) *Online Class (8 classes)* 19:00 – 22:00 (Tue & Thu)
Venue	Online Class - By Zoom Physical Class - 1/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
Medium	Cantonese with training materials in English
Fee	Early bird price (on or before 22 July 2020) - Non-member: HK$12,500 per person - Member of Organiser / Supporting Organisation: HK$11,500 per person Regular Price (after 22 July 2020) - Non-member: HK$13,500 per person - Member of Organiser / Supporting Organisation: HK$12,500 per person
Remarks	Deadline for submission is **8 August 2020**. Late submission will NOT be considered.

Get the Premier Cybersecurity Certification

The CISSP is an objective measure of excellence, being used as the most globally recognised standard of achievement in the industry. This cyber security certification is the first information security credential to meet the strict conditions of ISO/IEC Standard 17024.

Ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles. Suitable for :

- Chief Information Security Officer
- Director of Security
- Security Systems Engineer
- Security Manager
- Security Architect
- Network Architect
- Chief Information Officer
- IT Director/Manager
- Security Analyst
- Security Auditor
- Security Consultant

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org

Certified Information Systems Security Professional (CISSP®) Official Training

Course Topics at a Glance

The Certified Information Systems Security Professional (CISSP) is the most globally recognised certification in the information security market. It 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 organisation.

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.

Date	Activities
22 August 2020 (Sat)	• Security and Risk Management (Domain 1)*
29 August 2020 (Sat)	• Asset Security (Domain 2)*
1 September 2020 (Tue)	• Security Architecture and Engineering (Domain 3)**
3 September 2020 (Thu)	• Security Architecture and Engineering (Domain 3)**
8 September 2020 (Tue)	• Communication and Network Security (Domain 4)**
10 September 2020 (Thu)	• Identity and Access Management (IAM) (Domain 5)**
15 September 2020 (Tue)	• Security Assessment and Testing (Domain 6)**
17 September 2020 (Thu)	• Security Assessment and Testing (Domain 6)**
22 September 2020 (Tue)	• Security Operations (Domain 7)**
24 September 2020 (Thu)	• Security Operations (Domain 7)**
26 September 2020 (Sat)	• Software Development Security (Domain 8)*
3 October 2020 (Sat)	• Software Development Security (Domain 8)*

Note: * Physical Class from 09:00 – 13:00 ** Online Class from 19:00 – 22:00

Course Benefits

This course will help participants review and refresh their cloud security knowledge and identify areas they need to study for the CISSP exam and features:

- Official $(ISC)^2$ courseware
- Taught by an authorised $(ISC)^2$ instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios
- A certificate of completion

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org

Certified Information Systems Security Professional (CISSP®) Official Training

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
- Organisational 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
- Organisational code of ethics

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

1.7 Identify, analyse, 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

Certified Information Systems Security Professional (CISSP®) Official Training

Training Outline

1. Security and Risk Management

- 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 programme

- 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

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org

Training Outline

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

Certified Information Systems Security Professional (CISSP®) Official Training

Training Outline

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

Certified Information Systems Security Professional (CISSP®) Official Training

Training Outline

5. Identity and Access Management (IAM)

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

Training Outline

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

7.3 Industry standards

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

Training Outline

7. Security Operations

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

Certified Information Systems Security Professional (CISSP®) Official Training

Training Outline

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

Mode of Delivery

Online & Classroom-based Training

- The most thorough review of the CISSP CBK, industry concepts and best practices
- Total 40 hours per training

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org

Certified Information Systems Security Professional (CISSP®) Official Training

Trainers

Mr Frank CHOW

Frank CHOW is an (ISC)^2 Certified Trainer and 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.

Mr Peter CHEUNG

Peter CHEUNG is an (ISC)^2 Certified Trainer with over 20 years of experience in IT industry. He is currently working in MNC as Regional Security Officer and Operational Security Readiness Manager, with experience in vulnerability management, incident management, risk management, security assessment and review. Before that, he worked in a global IT vendor as Network Security Specialist and Network Manager of a Datacenter.

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.

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. 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.

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org

Certified Information Systems Security Professional (CISSP®) Official Training

Certificate Award

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.**

CISSP Examination Procedures

(ISC)² has introduced Computerised 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: https://www.isc2.org/Certifications/CISSP.

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 method

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

https://www.home.hkpcacademy.org/en/10010399

Organisers:

Supporting Organisations:

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org