hkpc Academy 生產力學院

Official Training Partner

ISC2 OFFICIAL TRAINING PARTNER

Certified Information Systems Security Professional (CISSP®) Official Training (2023 New Version)

CISSP® Certified Information Systems Security Professional

THE INDUSTRY LEADING CREDENTIAL

CONNECTION TECHNOLOGY 裝備未來 FUTURESKILLS

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

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

Applying RTTP

This is an (ISC)² official training of Certified Information Systems Security Professional (CISSP) 2023 version.

The course content has been refreshed based on the latest new CISSP exam outline to address information security trends:

- Cyber crimes, risks, ransomware, vulnerability management, threat intelligence, UEBA.
- Cloud: cloud access security broker, microservices, containers.
- Identity and access management: risk-based access control, 2FA/MFA, OIDC, Oauth, SSO, JIT, privilege escalation.
- 5G, AI /machine learning tools.
- Development: CI/CD, SOAR, software defined security.
- Supply chain risk management.

Programme code	10014524-01
Duration and time	26-28 September and 3-4 October 2023 5 Days(40 hours in total) 09:00 – 18:00
Venue	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 29 August 2023** Staff of Organiser, Member of (ISC)² or Supporting Organisation: **HK$17,200** per person - Non-member: **HK$18,200** per person **Regular Price** - Staff of Organiser, Member of (ISC)² or Supporting Organisation: **HK$18,500** per person - Non-member: **HK$19,500** per person
Remarks	Deadline for submission is 5 September 2023. Late submission will NOT be considered.

Global Recognition

CISSP is the most recognised **global standard** of achievement in the security industry and is found in **over 135 countries.** The credential is recognised by government organisations, including

- **Hong Kong Monetary Authority (HKMA)** in Enhanced Competency Framework on Cybersecurity (2019 Jan)
- **UK National Academic Recognition Information Centre (NARIC)** recognised CISSP certification at RQF Level 7 Master degree standard (2020 May)
- **United States DoD** 8140.01/8570.01 approved and listed in IAT Level III, IAM Level II, IAM Level III, IASAE I and IASAE II
- Other countries: **Australia –IRAP, Cyber Skills Framework; Japan –NICT; Singapore -NICF; Thailand -ETDA**

This Training Course is the **official training offered by (ISC)²**, with **standard content and duration** (40 hours) and conducted by experienced **authorised trainers of (ISC)²**. The well-designed contents distributed across 8 domains assist participants to gain the latest knowledge pertinent security challenges to make a well thought out decision in security strategy.

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.

Course Content

The content of this course is based on the current CISSP exam outline. It has been refreshed to reflect the most pertinent issues such as supply chain attack happened in year 2023. It also covers best practices for emerging technologies (e.g. 5G, IoT, cloud, container), threat intelligence and hunting.

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines. Successful candidates are competent in the following eight domains.

Note: Effective 1 May 2023, the CISSP has a new exam outline. The domains and their weights are updated.

Date	Activities
Day 1	• Security and Risk Management • Asset Security
Day 2	• Asset Security • Security Architecture and Engineering
Day 3	• Security Architecture and Engineering • Communication and Network Security • Identity and Access Management (IAM)
Day 4	• Identity and Access Management (IAM) • Security Assessment and Testing • Security Operations
Day 5	• Security Operations • Software Development Security

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

Training Outline

* Topics related to new cyber security trends

1. Security and Risk Management

1.1 Understand, adhere to, and promote professional ethics
- (ISC)² Code of Professional Ethics
- Organizational code of ethics

1.2 Understand and apply security concepts
- Confidentiality, integrity and availability, authenticity and nonrepudiation

1.3 Evaluate and apply security governance principles
- Alignment of the 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

1.4 Determine compliance and other requirements
- Contractual, legal, industry standards and regulatory requirements
- Privacy requirements

1.5 Understand legal and regulatory issues that pertain to information security in a holistic context
- Cybercrimes and data breaches
- Licensing and Intellectual Property (IP) requirements
- Import/export controls
- Transborder data flow
- Privacy

1.6 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

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

1.8 Identify, analyze and prioritize Business Continuity (BC) requirements
- Business Impact Analysis (BIA)
- Develop and document the scope and the plan

1.9 Contribute to and enforce personnel security policies and procedures
- Candidate screening and hiring
- Employment agreements and policies
- Onboarding, transfers and termination processes
- Vendor, consultant and contractor agreements and controls
- Compliance policy requirements
- Privacy policy requirements

1.10 Understand and apply risk management concepts
- Identify threats and vulnerabilities
- Risk assessment/analysis
- Risk response
- Countermeasure selection and implementation

Training Outline

* Topics related to new cyber security trends

1. Security and Risk Management (Cont.)

- Applicable types of controls (e.g., preventive, detective, corrective)
- Control assessments (security and privacy)
- Monitoring and measurement
- Reporting
- Continuous improvement(e.g., Risk maturity modeling)
- Risk frameworks

1.11 Understand and apply threat modeling concepts and methodologies

1.12 Apply Supply Chain Risk management (SCRM) concepts

- Risks associated with hardware, software and services
- Third-party assessment and monitoring
- Minimum security requirements
- Service level requirements

1.13 Establish and maintain a security awareness, education and training program

- Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)
- Periodic content reviews
- Program effectiveness evaluation

2. Asset Security

2.1 Identify and classify information and assets

- Data classification
- Asset classification

2.2 Establish information and asset handling requirements

2.3 Provision resources securely

- Information and asset ownership
- Asset inventory (e.g., tangible, intangible)
- Asset management

2.4 Manage data life cycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection
- Data location
- Data maintenance
- Data retention
- Data remanence
- Data destruction

2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

2.6 Determine data security controls

- Data states (e.g., in use, in transit, at rest)
- Scoping and tailoring
- Standards selection
- Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

Training Outline

* Topics related to new cyber security trends

3. Security Architecture and Engineering

3.1 Research, implement and manage engineering processes using secure design principles
- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Separation of Duties (SoD)
- Keep it simple
- Zero Trust
- Privacy by design
- Trust but verify
- Shared responsibility

3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems (IS) (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 (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing (HPC) Systems
- Edge computing systems
- Virtualized systems

3.6 Select and determine cryptographic solutions
- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures and digital certificates
- Non-repudiation
- Integrity (e.g., hashing)

3.7 Understand methods of cryptanalytic attacks
- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis
- Chosen ciphertext
- Implementation attacks
- Side-channel
- Fault injection
- Timing
- Man-in-the-Middle (MITM)
- Pass the hash
- Kerberos exploitation
- Ransomware

3.8 Apply security principles to site and facility design

3.9 Design 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
- Power (e.g., redundant, backup)

Training Outline

* Topics related to new cyber security trends

4. Communication and Network Security

4.1 Assess and implement secure design principles in network architectures
- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
- Secure protocols
- Implications of multilayer protocols
- Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
- Microsegmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
- Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)
- Cellular networks (e.g., 4G, 5G)
- Content Distribution Network (CDN)

4.2 Secure network components
- Operation of hardware (e.g., redundant power, warranty, support)
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security

4.3 Implement secure communication channels according to design
- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualised networks
- Third-party connectivity

5. Identity and Access Management (IAM)

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

5.2 Manage identification and authentication of people, devices and services
- Identity Management (IdM) implementation
- Single/Multi-Factor Authentication (MFA)
- Accountability
- Session management
- Registration, proofing and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems
- Single Sign On (SSO)
- Just-in-Time (JIT)

5.3 Federated identity with a third-party service
- On-premises
- Cloud
- Hybrid

Training Outline

* Topics related to new cyber security trends

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)
- Risk based access control

5.5 Manage the identity and access provisioning life cycle
- Account access review (e.g., user, system, service)
- Provisioning and deprovisioning (e.g., on/off boarding and transfers)
- Role definition (e.g., people assigned to new roles)
- Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

5.6 Implement authentication systems
- OpenID Connect (OIDC)/Open Authorization (Oauth)
- Security Assertion Markup Language (SAML)
- Kerberos
- Remote Authentication Dial-In User Service (RADIUS)/ Terminal Access Controller Access Control System Plus (TACACS+)

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
- Breach attack simulations
- Compliance checks

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
- Remediation
- Exception handling
- Ethical disclosure

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

Training Outline

* Topics related to new cyber security trends

7. Security Operations

7.1 Understand and comply with investigations
- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics and procedures
- Artifacts (e.g., computer, network, mobile device)

7.2 Conduct logging and monitoring activities
- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- User and Entity Behavior Analytics (UEBA)

7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

7.4 Apply foundational security operations concepts
- Need-to-know/least privilege
- Separation of Duties (SoD) and responsibilities
- Privileged account management
- Job rotation
- Service Level Agreements (SLAs)

7.5 Apply resource protection
- Media management
- Media protection techniques

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

7.7 Operate and maintain detective and preventative measures
- Firewalls (e.g., next generation, web application, network)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Machine learning and Artificial Intelligence (AI) based tools

Training Outline

* Topics related to new cyber security trends

7. Security Operations (Cont.)

7.8 Implement and support patch and vulnerability management

7.9 Understand and participate in change management processes

7.10 Implement recovery strategies
- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, High Availability (HA), Quality of Service (QoS) and fault tolerance

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

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

7.13 Participate in Business Continuity (BC) planning and exercises

7.14 Implement and manage physical security
- Perimeter security controls
- Internal security controls

7.15 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 (e.g., Agile, Waterfall, DevOps, DevSecOps)
- Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Operation and maintenance
- Change management
- Integrated Product Team (IPT)

Training Outline

* Topics related to new cyber security trends

8. Software Development Security(Cont.)

8.2 Identify and apply security controls in software development ecosystems
- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment (IDE)
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Security Orchestration, Automation and Response (SOAR)
- Software Configuration Management (SCM)
- Code repositories
- Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

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
- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

8.5 Define and apply secure coding guidelines and standards
- Security weaknesses and vulnerabilities at the source-code level
- Security of Application Programming Interfaces (APIs)
- Secure coding practices
- Software-defined security

Target Participants

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

Trainer

Mr Andy HO

Andy HO is an (ISC)² Certified Trainer with over 30 years of information security experience in the security profession and has worked throughout the Asia Pacific countries.

Andy took the Corporate Senior Security Manager role in IBM Asia Pacific, Japan and Greater China for more than 10 years when he held the regional responsibility to oversee corporate security investigations and IT forensic.

Andy is a Council Member of (ISC)² Asia-Pacific Advisory Council and as the founding president of the (ISC)² HK Chapter.

Mode of Delivery
Webinar/Classroom-based Training

- The most thorough review of the CISSP CBK, industry concepts and best practices
- Five-day classes; eight hours per day
- Available at (ISC)² facilities and through (ISC)² Official Training Providers worldwide

Prerequisites

To qualify for the 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 will have up to six years to earn your required work experience for the CISSP.

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 will 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/exams.

Effective 1 May 2023, the CISSP exam will be based on a new exam outline. The domains and their weights have changed. If you would like to understand more about the exam, kindly view the link: https://www.isc2.org/Register-for-Exam for your reference.

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.

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 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.)

https://www.hkpcacademy.org/en/**10014524-01**