HKIB The Hong Kong Institute of Bankers | CERTIFIED BANKER

Associate Cybersecurity Professional (ACsP)

<QF Level 4>*

Programme Handbook

(Syllabus, Regulations and General Information)

* The Professional Qualification "Associate Cybersecurity Professional (ACsP)" is recognised under the QF at Level 4. (QR Registration No.: 20/000537/L4) (Validity Period from 01/08/2020 to 31/07/2030)

CSP-P-002
Last updated: 24 February 2026

Table of Contents

1. Introduction

With the aim of supporting capacity building and talent development for banking professionals, the Hong Kong Monetary Authority (HKMA) has been working together with the banking industry to introduce an industry-wide competency framework – **the Enhanced Competency Framework (ECF) for Banking Practitioners** – in Hong Kong.

Since the implementation of ECF in 2018, various programmes for different job functions in banking industry have been developed and integrated into The Hong Kong Institute of Bankers' ("HKIB") flagship Certified Banker (CB) Programme which offer generalist, specialist, and strategic topics. The rationale for putting all programme under one professional banking qualification is to promote an industry-based common qualifications benchmark. While ECF pro-grammes offer "role-based" knowledge and certification to relevant practitioners, CB is offering a vocational qualification pathway for further career advancement, being continuously enhanced to nurture more holistic banking professionals and ultimately, supporting the industry to develop a continuous learning culture and a sustainable talent pool so as to maintain the competitiveness of Hong Kong as an international financial centre.

The Enhanced Competency Framework on Cybersecurity (ECF-Cybersecurity) was introduced to develop a sustainable pool of Cybersecurity practitioners for the banking industry. It targeted new entrants or existing practitioners engaged by authorized institutions to perform in roles ensuring operational cyber resilience.
Given the growing number of cyberattacks to financial institutions in recent years, it becomes essential to develop a sustainable pool of banking practitioners who is working in cybersecurity and also to attract the talents to join the cybersecurity related sector in banking.

This Handbook provides the programme details and relevant information for the learner who intends to complete the ECF on Cybersecurity training and examination with the intent of obtaining the Professional Qualification of "**Associate Cybersecurity Professional (ACsP)**" which offered by HKIB.

For more details related to the ECF on Cybersecurity, please refer to the HKMA's Guide to ECF on Cybersecurity issued by HKMA dated 19 December 2016 or you may visit HKIB's ECF on Cybersecurity webpage.

2. Background

2.1 Aims

The aims of the ECF on Cybersecurity are twofold:

(i) To develop a sustainable talent pool of cybersecurity practitioners for the workforce demand in this sector; and

(ii) To raise and maintain the professional competence of cybersecurity practitioners in the banking industry.

2.2 Competency Standards

They are set at two levels:

Core Level – This level is applicable for entry-level staff with less than five years of relevant work experience in the cybersecurity function; and

Professional Level – This level is applicable for staff with five years or more of relevant work experience in the cybersecurity function.

The qualification structure is driven by the key roles based upon the three lines of defence concept under cyber risk governance.

– First line of defence: IT Security Operations and Delivery
– Second line of defence: IT Risk Management and Control
– Third line of defence: IT Audit

2.3 Scope of Application

The ECF on Cybersecurity is targeted at 'Relevant Practitioners', including new entrants and existing practitioners, engaged by an Authorized Institution (AI)[1] to perform cybersecurity job roles in Hong Kong. Relevant Practitioners who have less than five years of relevant work experience in the following areas should pursue the Core Level of the ECF on Cybersecurity:

(a) Perform IT security operations and delivery, for example, apply daily administrative operational processes

(b) Perform IT risk management and control, for example, assist in development and communication of control processes

(c) Perform IT Audit, for example, conduct and document audits

Relevant Practitioners who have five years or more of relevant work experience in the following areas should pursue the Professional Level of the ECF on Cybersecurity:

[1] An institution authorized under the Banking Ordinance to carry on the business of taking deposits. Hong Kong maintains a Three-tier Banking System, which comprises banks, restricted license banks and deposit-taking companies. Authorized institutions are supervised by the HKMA.

(a) Perform IT security operations and delivery, for example, manage information systems security operations

(b) Perform IT risk management and control, for example, manage IT risk management and control procedures and policies

(c) Perform IT Audit, for example, plan and execute audit and assessments

For more details about the key tasks, please refer to the Annex 1 – Example of key tasks for roles under ECF-C of the HKMA Guide to ECF on Cybersecurity.

2.4 Certification and Public Register

Relevant Practitioners who have completed the "ECF on Cybersecurity (Core Level)" training and passed the relevant examination may apply for the "Associate Cybersecurity Professional (ACsP)".

By going through HKIB certification process successfully, the ACsP holders are then registered as Certified Individuals and included in the public register on HKIB website. HKIB will also grant the ACsP holders a professional membership of HKIB.

Learners who have successfully completed a HKIB professional qualification programme (including training and examination requirements) but yet to fulfil the requirement of Relevant Practitioners or required years of relevant work experience for certification will be automatically granted as ECF Affiliate. ECF Affiliate holders are then registered as Certified Individuals and included in the public register on HKIB website. Ordinary Membership with membership fee for the awarding year waived will also be granted to learners.

2.5 Annual renewal of certification and CPD Requirements

Certification of ACsP is subject to annual renewal by HKIB. PQ holders are required to meet the annual Continuing Professional Development (CPD) requirements and pay an annual certification renewal fee to renew the certification.

For the core level qualification, a minimum of 20 CPD hours each year and a minimum of 120 CPD hours over every 3 years period is required.

For ECF Affiliate, at least 3-hours of CPD within the scopes mentioned in HKIB CPD Scheme is required annually for certification renewal.

No CPD is required in the year when the ACsP certification / ECF Affiliate is granted. The CPD

requirement starts in the following calendar year.

Please refer to the Overview of the HKIB CPD Scheme and HKIB CPD Requirements webpage for more details.

3. ECF on Cybersecurity (Core Level) Programme Overview

3.1 Entry Requirements

The Programme is open to members and non-members of HKIB. Candidates must fulfil the stipulated minimum entry requirements:

- Students of Associate Degree (AD) / Higher Diploma (HD) in any disciplines (QF L4);
- Equivalent qualifications or above; OR
- Mature applicants with 3 years of relevant banking experience with recommendations from employer

Remarks:

1. *Mature applicants (aged 21 or above) who do not possess the above academic qualifications but with relevant banking experience and recommendation from their employers will be considered on individual merit.*

3.2 Programme Objectives

This programme is developed with the aim to nurture a sustainable talent pool of cybersecurity practitioners for the banking industry. Learners will learn the technical foundation of cybersecurity and the cybersecurity controls used in the banking environment. Also, learners will be equipped with the essential knowledge and tools to gain a better understanding of computer security vulnerabilities and typical security pitfalls, enabling them to identify potential security threats and apply early intervention to common cybersecurity problems.

3.3 Programme Intended Outcomes

Upon completion of the Programme, learners should be able to:

- Describe the foundation of various network protocols and their hierarchical relationship in hardware and software;
- Apply the principles and knowledge of international standards to enhance network and system security;
- Apply cybersecurity related monitoring measures for managing different types of cybersecurity threats;
- Conduct a security incident response process and present an analysis of the results for management's review;
- Assess security risks in the cyber environment and IT systems by applying the IT Risk Management and Control principles; and
- Conduct IT audits and security testing to assess cybersecurity risk protection.

3.4 Learning Hours

The programme design adopts a blended learning approach. Learners are advised to spend not less than 200 Learning Hours. Learning time refers to the amount of time an average learner is expected to take to complete all learning pertaining to the Programme and achieve the learning outcomes expected. It includes time spent on all learning modes and activities such as training class, self-study and assessment hours.

3.5 Integration in Certified Banker (CB)

The "ECF on Cybersecurity (Core Level)" is integrated in the CB (Stage I) as one of the elective modules. CB (Stage I) is a professional banking qualification programme developed and offered by HKIB. It is intended to raise the professional competency of banking and financial practitioners in Hong Kong to meet modern demands, while providing a transparent standard with international recognition.

Individuals who have completed the "ECF on Cybersecurity (Core Level)" programme and obtained a pass at the relevant examination are encouraged to join the CB (Stage I) Programme.

3.6 Qualifications Framework

The Professional Qualification Associate Cybersecurity Professional (ACsP) is recognised under the QF at Level 4. (QR Registration No.: 20/000537/L4) (Validity Period from 01/08/2020 to 31/07/2030).

4. Learning Support

HKIB provides learners with a range of support services to help you throughout the learning journey. These services include answering your enquiries, managing the certification process, providing access to library resources, offering study materials, and maintaining an online learning platform. The aim of these services is to facilitate learners and increase the chances of success in the training and examination. Here are some highlights for your attention.

4.1 Video-On-Demand

To facilitate the learners to get better preparation for the examination, HKIB provides the Video-On-Demand service for the learners to watch the recorded training sessions of a particular training class. Video-On-Demand service is available for up to 90 days before the examination.

4.2 Professional Qualification Programme Scholarship Scheme

Each year, HKIB selects the top two candidates from Core Level and award them with the scholarship as recognition. This is the way for HKIB to promote academic excellence and motivate future students to push themselves to achieve same high level of performance.

The two top candidates in Core Level, provided that all other granting requirements are met, can be awarded with a cash incentive (HKD4,000 for Core Level), and a study coupon which can provide candidates to study one more professional qualification offered by HKIB with all training and examination fees waived.

4.3 HKIB Resources Corner Support

The Resources Corner situated at the premises of HKIB provides the required learning resources required for study. Copies of the Recommended Readings are available in the Corner for borrowing. To provide updated learning resources to the members, HKIB has provided FREE internet and library service to the members.

Learners are encouraged to prepare the examination by acquiring relevant market information and module knowledge through various channels, e.g. reference readings, business journals, websites etc. Learners should be aware that such market information may be important and pertinent to the examinations.

4.4 Market Information Updates

HKIB regularly organises training courses, CPD programmes, conference, seminars and luncheon talks,

industry events on current issues and developments in financial markets that learners may find essential, helpful, and relevant to their learning. Besides, HKIB provides members with updated market information through complimentary bi-monthly journal Banking Today, weekly e-news and first-hand internship opportunities.

For more details, please refer to Events & Industry Initiatives and HKIB eLearning under HKIB website.

4.5 E-learning Courses

HKIB also supports the E-learning. More than 500 courses are organized into 51 course libraries spanning about 700 hours of E-learning, covering areas of Banking, Accounting, Insurance, Risk Management and Cybersecurity.

A new e-learning course on “Cybersecurity Essentials” is developed with the common topics related to Cybersecurity, such as “What is cybersecurity?”, “Cybersecurity attack life cycle”, “The most common threats and attacker attack types” and “Security Best Practices”. It will provide a quick guide to non-IT background learners to acquire fundamental knowledge on Cybersecurity in order to better understand what cybersecurity is and the common terminologies used. This e-learning course is now available in HKIB e-learning portal.

For more details, please refer to HKIB eLearning under HKIB website.

4.6 Mock Examination Paper for Examination Preparation

To facilitate the learners to get better preparation for the examination, HKIB provides the mock examination paper for the learners as reference to better understand the examination format, structure and approach. Thus, all the questions shared from the mock examination paper will NOT be used in the official examination.

4.7 Learning Consultation Services

For learners require any learning consultation services related to the banking profession-al qualifications offered by HKIB, they may contact us through our customer service hot-line at (852) 2153 7800 for making arrangement.

5. Programme Syllabus

A. Module Objective

The module has been developed with the aim to nurture a sustainable talent pool of cybersecurity practitioners for the banking industry. Candidates will learn the technical foundation of cybersecurity and the cybersecurity controls used in the banking environment. Also, candidates will be equipped with the essential knowledge and tools to gain a better understanding of computer security vulnerabilities and typical security pitfalls, enabling them to identify potential security threats and apply early intervention to common cybersecurity problems.

B. Module Intended Outcomes

Upon completion of this module, learners should be able to:

- Describe the foundation of various network protocols and their hierarchical relationship in hardware and software;
- Apply the principles and knowledge of international standards to enhance network and system security;
- Apply cybersecurity related monitoring measures for managing different types of cybersecurity threats;
- Conduct a security incident response process and present an analysis of the results for management's review;
- Assess security risks in the cyber environment and IT systems by applying the IT Risk Management and Control principles; and
- Conduct IT audits and security testing to assess cybersecurity risk protection.

C. Syllabus

Chapter 1: Technical Foundation of Cybersecurity	
1.1	**Importance of Cybersecurity in the Banking Industry**
1.1.1	- Cybersecurity applied in the banking industry
1.1.2	- Importance of Cybersecurity on the operation of a bank
1.2	**Foundation of a Network**
1.2.1	- OSI and TCP/IP Model
1.2.2	- An Overview of Internet Architecture
1.3	**IT Security Principles**
1.3.1	- Confidentiality, Integrity, Availability
1.3.2	- Accountability, Non-repudiation
1.3.3	- Types of Security Controls
1.3.4	- Least Privilege
1.3.5	- Segregation of Duties

1.3.6	- IT Asset Management
1.4	**Foundation of Access Control**
1.4.1	- Access Control Concepts
1.4.2	- Identification, Authentication, Authorisation
1.4.3	- Identity and Access Management
1.4.4	- Common Access Control Implementation
1.5	**Foundation of Cryptography**
1.5.1	- Hashing
1.5.2	- Salting
1.5.3	- Symmetric/Asymmetric Encryption
1.5.4	- Digital Signatures
1.5.5	- Cryptographic Key Management
1.6	**Foundation of Cloud Computing**
1.6.1	- Virtualisation
1.6.2	- Infrastructure as a Service, Software as a Service and Platform as a Service
1.6.3	- Cloud Computing Strategy
1.6.4	- Data Governance on Cloud Computing
1.6.5	- Concerns about Jurisdiction
1.6.6	- Major Cloud Security Considerations
1.6.7	- Guidance on Cloud Computing
Chapter 2: Bank IT Security Controls	
2.1	**International Standards and Regulatory Requirements**
2.1.1	- ISO 27001 Principles and Process
2.1.2	- ISO 27002 Control Objectives
2.1.3	- HKMA Technology Risk Management and Cybersecurity Fortification Initiatives
2.1.4	- Well-known International Security Organizations
2.2	**Network Security Administration**
2.2.1	- Common Network Protocols
2.2.2	- Common Network Attacks
2.2.3	- DMZ and Network Segmentation
2.2.4	- Wireless Network Infrastructure
2.2.5	- Firewalls and Proxy
2.2.6	- Intrusion Detection System and Intrusion Prevention System
2.2.7	- Understanding Wireless Security
2.2.8	- Protecting the Network Infrastructure
2.2.9	- Protecting the Network Management Platform
2.2.10	- Network Vulnerability Management and Patch Management
2.2.11	- Mobile Commerce Security
2.3	**System Security Administration**
2.3.1	- Database Security
2.3.2	- System Hardening
2.3.3	- Sandboxing
2.3.4	- Application Whitelisting
2.3.5	- Virtual Desktop
Chapter 3: Cybersecurity Monitoring	
3.1	**Malware and Malicious Activities**
3.1.1	- Malware
3.1.2	- Rootkits
3.1.3	- Botnets
3.1.4	- Advanced Persistent Threat (APT)

3.1.5	- Fileless Malware
3.1.6	- Distributed Denial of Service Attack (DDoS)
3.2	**Malware Infection Vectors**
3.2.1	- Social Engineering
3.2.2	- Spam, Phishing, Spear-phishing
3.2.3	- Social Networks
3.2.4	- Physical Media
3.2.5	- Software Vulnerability
3.2.6	- Zero-day Vulnerability
3.3	**Network Monitoring**
3.3.1	- Log Files and Log Management
3.3.2	- Security Event and Detection Mechanisms
3.3.3	- Monitoring Tools
3.3.4	- Monitoring of Wireless Attacks
3.4	**Endpoint Monitoring**
3.4.1	- Endpoint Detection and Response
3.4.2	- EDR Key Functions
3.5	**Analysis**
3.5.1	- SIEM Architecture and Components
3.5.2	- Correlation Rules
3.5.3	- Detection of Malicious Activities
3.5.4	- Cybersecurity Labs
Chapter 4: Security Incident Response	
4.1	**Security Incident Response Process**
4.1.1	- Containment
4.1.2	- Eradication
4.1.3	- Recovery
4.1.4	- Improvement
4.1.5	- ISO 27043 Incident Investigation Principles and Processes
4.2	**Digital Evidence**
4.2.1	- First Responder
4.2.2	- Evidence Handling
4.2.3	- Preservation of the Scene
4.2.4	- Evidence Related to Network Events
4.3	**Security Incident Communication**
4.3.1	- Internal Communication
4.3.2	- Preparing Management Reports
4.3.3	- Cyber Intelligence
4.3.4	- Communication between Banks and Other Parties
Chapter 5: Technology Risk Management and Control	
5.1	**Risk Management Process**
5.1.1	- Risk Management Concepts
5.1.2	- Risk Assessment
5.1.3	- Risk Treatment (Accept, Transfer, Mitigate, Avoid)
5.2	**Risk Monitoring and Compliance Checking**
5.2.1	- Risk Register and Risk Dashboard
5.2.2	- Compliance Self-assessments
5.3	**Risk Acceptance**
5.3.1	- Risk Ownership
5.3.2	- Risk Acceptance Process

5.4	**Third Party Risk Management**
5.5	**Security and Risk Awareness Training**
Chapter 6: IT Audit	
6.1	**Principles of IT Audit**
6.1.1	- Audit Organization Functions
6.1.2	- IT Audit
6.2	**Security and Compliance Control Testing**
6.2.1	- Major Steps in IT Audit
6.2.2	- Walkthrough and Control Verification
6.2.3	- Cybersecurity Audit
6.3	**Audit Reports and Follow-Up**
6.3.1	- Audit Report
Chapter 7: Security Test	
7.1	**Penetration Test Principles**
7.1.1	- Functions of Penetration Tests
7.1.2	- Types of Penetration Tests
7.1.3	- Cyber Attack Simulation Testing
7.2	**Penetration Test Process**
7.2.1	- Test Preparations
7.2.2	- Vulnerability Scanning and Assessment
7.2.3	- Network Penetration Test
7.2.4	- Application Penetration Test
7.2.5	- Common Vulnerabilities and Exposures (CVE)
7.2.6	- Lateral Movement
7.2.7	- Adversarial Tactics, Techniques, and Common Knowledge
7.3	**Red Team Approach**
Chapter 8: Impact of Emerging Technologies on Cybersecurity	
8.1	**Generative AI**
8.1.1	- Risks of Generative AI ("Gen AI")
8.1.2	- Risk Governance on Gen AI
8.2	**DLT / Digital Asset**
8.2.1	- Introduction of Digital Asset
8.2.2	- Risk & Control of Digital Asset
8.3	**Emerging Threat on E-banking**
8.3.1	- Emerging Threat on E-banking
8.3.2	- Proposed Mitigation Controls

Recommended Readings

Essential Readings:

1. HKIB Study Guide of ECF-Cybersecurity. (2025).

Supplementary Readings

1. Center for Internet security (CIS), https://www.cisecurity.org/cybersecurity-best-practices
2. Collins, M. S. (2016). *Network Security Through Data Analysis: Building Situational Awareness* (2nd ed.). "O'Reilly Media, Inc.".
3. Cybersechub, https://www.cybersechub.hk/en/home/cert

4. Dykstra, J. (2015). *Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems*. "O'Reilly Media, Inc."
5. E-learning on HKIB Website: Cybersecurity Essentials, https://secure.kesdee.com/ksdlms/?Partner=HKIB
6. European Union Agency for Network and Information Security (ENISA). (2017). *Cyber Security Culture in organisations ENISA*.

   https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
7. Federal Office for Information Security. (n.d.). *A Penetration Testing Model*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf
8. GovCERT, https://www.govcert.gov.hk/en/index.html
9. HKCERT, https://www.hkcert.org/faq
10. HK Police CSTCB, https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/index.html
11. Hong Kong Monetary Authority. (2016, May 18). *Cyber Resilience Assessment Framework*. http://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf
12. Hong Kong Monetary Authority. (2020, November 3). *Cybersecurity Fortification Initiative 2.0*. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1a1.pdf
13. Hong Kong Monetary Authority. (2021, June 8).
    I. Opening remarks at HKAB Fintech Seminar: Next Phase of Hong Kong's Fintech Journey – "Fintech 2025". https://www.hkma.gov.hk/eng/news-and-media/speeches/2021/06/20210608-3/
    II. Media Briefing on "Fintech 2025" Strategy. https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20210608e1.pdf
14. Hong Kong Monetary Authority. (2024, September 27).
    I. Research Paper on Generative Artificial Intelligence in the Financial Services Sector. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240927e1.pdf
    II. Encl. Generative Artificial Intelligence in the Financial Services Space. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/GenAI_research_paper.pdf
15. Hong Kong Monetary Authority. (2024, September 27).
    I. Use of Artificial Intelligence for Monitoring of Suspicious Activities. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240909e1.pdf
    II. Annex - Use of Technologies to improve the Effectiveness and Operational Efficiency of

Monitoring for MLTF. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240909e1a1.pdf

16. Hong Kong Monetary Authority. (2024, April 16). Risk management considerations related to the use of distributed ledger technology. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240416e1.pdf
17. Hong Kong Monetary Authority. (2023, December 21).
    I. Managing cyber risk associated with third-party service providers.https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20231221e1.pdf
    II. Annex Managing cyber risk associated with third-party service providers. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20231221e1a1.pdf
18. Hong Kong Monetary Authority. (2023, October 31). Enhancement to security of electronic banking services. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20231031e1.pdf

Further Readings

1. Australian Signals Directorate. (2018). *Protect: Implementing Application Whitelisting*. https://www.asd.gov.au/publications/protect/application_whitelisting.htm
2. COBIT 5, ISACA
3. Hong Kong Monetary Authority. (2024, June 3). *General Principles for Technology Risk Management*. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf
4. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems requirements
5. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
6. Johansen, G. T. (2017). *Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents*. Packt Publishing.
7. Kavis, M. J. (2014). *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. Wiley.
8. Microsoft. (2016). *Anatomy of a Breach*. https://download.microsoft.com/download/E/9/2/E92BB61B-ED07-431C-A33B-971FD91B31D4/Anatomy_of_a_Breach_ebook_en-CA.pdf
9. National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework*. https://www.nist.gov/cyberframework
10. Sanders, C., & Smith, J. (2014). *Applied Network Security Monitoring: Collection, Detection, and*

Analysis. Syngress Publishing.

11. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). *MITRE ATT&CK: Design and Philosophy*. MITRE. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
12. The Institute of Internal Auditors. (2015). *Leveraging COSO across the Three Lines of Defense*. COSO.
13. Trull, J. C. (2016, October 16). *Use Security Education and Awareness Programs to Your Advantage*. Microsoft. https://cloudblogs.microsoft.com/microsoftsecure/2016/10/26/use-security-education-and-awareness-programs-to-your-advantage/
14. Data Security. Office of the Privacy Commissioner for Personal Data (PCPD). https://www.pcpd.org.hk/english/data_security/index.html

6. Training Application

6.1 Training Schedule

For the latest information about the training application period and class schedules, please contact HKIB staff or refer to HKIB website.

6.2 Training Duration

The training is set out as follows:

Training Mode	Lecture
Training Duration	15 Hours

6.3 Training Application

Applicants can submit the application via MyHKIB. Attention should be paid to the application deadline, or a late entry fee will be charged.

Application Requirements:

- The information provided for the training enrolment must be true and clear.
- Inaccurate or incomplete applications may not be accepted even if the applicant has paid the training fee.
- HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received your application, NO alterations to the training arrangement are allowed.
- HKIB reserves the right to change training dates and application deadlines at any time.

6.4 Training Fee and Payment

2025 Training Fee	HKD4,400 *

* *A digital version of training material (i.e. Study Guide and PPT Slides) will be provided before the training commencement. Printed version will only be available at an additional cost of HKD600 (including delivery fee) on request by learners.*

- Applicants should pay the training fee as follows:

(a) By credit card.

(b) By Alipay.

(c) By WeChat Pay.

- Application without successful payment will **NOT** be processed.
- All payments must be settled before the start of the Programme. **NO** fees are refunded or transferred

under any circumstances.

- Applicants are advised to keep a record of their payments.
- An email of training confirmation will be sent to applicants at least **five working days prior to the training date**.
- Late training enrolment will be accepted after the stipulated application deadline up to seven days before course commencement to allow us to administer the application. A late entry fee of HKD200 (in addition to the training fee) will apply.
- HKIB reserves the right to adjust training application, study guide and/or administration surcharge fees (if applicable), at any time.
- HKIB student members can enjoy 25% off training fee discount.

7. Examination Application and Regulations

7.1 Examination Mode and Format

The examination mode and format are as follows:

Examination Mode	Paper-based Examination	
Examination Duration	2.5 Hours	
Question Type	Multiple-choice Type Questions (MCQs)	
No. of Questions	80 MCQs	
Pass Mark	70%	
Grading	**Grade**	**Mark Range**
	Pass with Distinction	Above 90%
	Pass with Credit	80% - 90%
	Pass	70% - 79%
	Fail A	60% - 69%
	Fail B	50% - 59%
	Fail C	Below 50%
	Absent	N/A

7.2 Examination Timetable

- For latest information about the examination application period and examination dates, please contact HKIB staff or refer to Examination Schedule on HKIB website.

7.3 Examination Approaches

There are two examination approaches available and candidates may choose either one which is best for them.

- Face-to-face Examination: Traditional face-to-face examinations will be conducted at designated venues arranged by HKIB. Candidates are required to take examinations at specific locations allocated to them accordingly.
- "Remote Exam": As an alternative to the traditional face-to-face examination, HKIB had introduced an innovative initiative, "Remote Exam", allowing candidates to take examinations from their homes or workplaces with own computer equipment and internet access. "Remote Exam" offers greater

flexibility in terms of location and time saving on travelling for our candidates without jeopardising the quality standard of assessment.

Measures will be taken to align the same standard of fairness and effectiveness as that of the traditional face-to-face examination. A two device-approach will be adopted with one computer, either desktop or laptop, to access the "Remote Exam" platform for the examination and a mobile device, either smartphone or tablet, for invigilation and monitoring. Authentication of identity and real-time virtual invigilation will be conducted hassle-free with an automatic remote system to ensure the highest degree of integrity and data security.

To ensure smooth examination operations, candidates opting "Remote Exam" are required to participate in the "Rehearsal Practice Examination" to be held by HKIB before eligible to attend the formal examination. This arrangement will facilitate the candidates to get better preparation and understanding on the logistic arrangement of the "Remote Exam".

7.4 Examination Application

- Candidates taking current training classes can choose to sit for the current examination or any subsequent ones. They can choose to sit for subsequent examinations but if the corresponding programme has been changed or updated, they may be required to re-take the training in order to be eligible for module examination.
- Applicants can submit the application via MyHKIB. Attention should be paid to the application deadline, or a late entry fee will be charged. The information provided on the application form must be true and clear.
- Late examination enrolment will be accepted after the stipulated application deadline up to 14 days before examination date, to allow us to administer the application. A late entry fee of HKD 200 (in addition to the examination fee) will apply.
- Inaccurate or incomplete applications may not be accepted even if the applicant has paid the examination fee.
- Under no circumstances are changes to module entry allowed.
- HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received your application, NO alterations to the examinations and examination arrangements are allowed.
- HKIB reserves the right to change examination dates and application deadlines at any time.

7.5 Examination Fee and Payment

Examination Fee	HKD1,300 #

[#] HKIB student members can enjoy 50% off examination fee discount.

- Applicants should pay the examination fee as follows:
  (a) By credit card.
  (b) By Alipay.
  (c) By WeChat Pay.
- Application without successful payment will **NOT** be processed.
- All payments must be settled before the examination. **NO** fees are refunded or transferred under any circumstances.
- Applicants are advised to keep a record of their payments.
- HKIB reserves the right to adjust the examination, study guide and/or administration surcharge fees (if applicable), at any time.

7.6 Examination Attendance Notice

- Examination Attendance Notices (Attendance Notices) are sent to candidates via **email ONLY** approximately **two weeks** before the examination. Candidates must inform the Institute if they have not received it **one week** before the examination.
- Candidates are required to print a copy of the Attendance Notice on a sheet of plain A4 paper before attending each examination.
- Candidates MUST present their Attendance Notice at the examination along with a valid identification document (e.g. an HK Identity Card or passport) bearing a current photograph. Photocopies are not accepted.
- For candidates attending "Remote Exam", details regarding the prerequisite "Rehearsal Practice Examination" will also be attached.

7.7 Alteration / Transfer of Application for an Examination

- HKIB reserves the right to cancel, postpone and/or reschedule the examinations.
- If an examination is rescheduled, HKIB notifies candidates of the new date and time via email within one week of the original schedule. Under such circumstances, candidates are not required to re-register for the examination.
- Under no circumstances are any changes to or transfers of examination application allowed.

7.8 Examination Arrangements for Candidates with Special Needs

- Candidates with special needs may request special examination arrangements. Under these circumstances they are required to submit documentary evidence, such as medical proof issued by a registered medical practitioner, together with a written request, when applying for the examination.

Approval of the request is subject to final HKIB decision.

- Request for such arrangements may result in an additional charge.

7.9 Examination Preparation

- Candidates enrolled in the examination are required to study all the essential, recommended and further reading material, if applicable, as part of their examination preparation.

7.10 Examination Results

Examination Results Announcements

	*Examinations **before** March 2026*	*Examinations **after** March 2026*
Email notification on results	Yes	
Examinations with multiple-choice type questions ONLY	Results will be released within **four weeks** after the examination date	
Examinations with the presence of essay-type questions	Result will be released around **eight weeks** after the examination date of the last module of the exam diet	
Platform for result checking	HKIB online platform (valid for one month only after the result release date)	MyHKIB
Official examination result slip	Receive within two weeks after the result release date through HKIB online platform	MyHKIB

- Results are withheld from candidates who have not paid in full any monies due or payable to the Institute, including but not limited to examination application fees.

Examination Results Review

- Candidates may request rechecking or remarking of their examination scripts, within one month of the issue of examination results by submitting an official Examination Result Appeal Form via HKIB website.
- Rechecking fee of HKD500 per module is only applicable for multiple choice examinations and this fee covers the re-checking for technical errors only such as incorrect mark entries for multiple-choice answer sheets. Remarking fee of HKD1,700 per module is only applied to other types of examination.

7.11 General Examination Regulations

- An examination is governed by the regulations in force at the time of the examination and not at the time of application, in case there are discrepancies between the two sets of regulations.
- On all matters concerning interpretation of the regulations, the Professional Standard and Examination Board of the Institute has the final decision.
- Candidates must have completed the training class before taking the examination.
- The examination is conducted in English.
- Candidates must use an HB/2B pencil to answer the multiple-choice questions on the Answer Sheets.
- The examinations are conducted and invigilated by responsible persons appointed by HKIB.
- Examination Attendance Notices are sent to candidates via **email ONLY**. Candidates are required to print a copy on a plain sheet of A4 paper and **MUST** take their Attendance Notice to each examination, along with a valid identification document (e.g. HK Identity Card or passport). Attendance Notices are collected by the invigilators before the end of the examination, if necessary.
- Candidates should arrive at the examination venue at least 15 minutes before the start. Candidates must not enter the examination room until instructed to do so.
- Candidates are not allowed to sit for the examination if they are unable to present Attendance Notice/ valid identification document, or if the identification document does not contain a clear and current photograph of the candidate.
- All examinations begin at the time stated on the Attendance Notice. Latecomers may be admitted during the first 30 minutes of the examination, but extra time will not be given to compensate for any time lost.
- Smoking, eating and drinking are not allowed in the examination room. All mobile phones and other electronic devices must be switched off.
- All bags, books and other personal belongings must be placed in a location advised by the invigilator, before the examination begins.
- If you need to go to the toilet during the examination, you should seek permission from an invigilator. An invigilator will accompany you and you must NOT carry any mobile phones, other electronic devices, question books, answer sheets or other papers to the toilet.
- No other aids, such as books, dictionaries, computers (e.g. notebooks, PC tablets) or papers are permitted in the examination. No draft paper is provided during the examination. Rough workings or notes should be made on the question book and will not be marked.
- The packets of question papers are opened in the presence of the candidates before the start of the examination. Candidates should remain silent and are not allowed to communicate with other

candidate during the examination. Candidates interfering with the proper conduct of the examinations are warned by the invigilator or expelled from the examination room in a serious case. Under such circumstances, a report is submitted to HKIB to consider whether disciplinary action should be taken. Disciplinary action includes, but is not limited to, candidate disqualification.

- Candidates cannot leave the examination room during the first 45 minutes and the last 15 minutes of an examination. Candidates who decide to leave early must notify the invigilator as quietly as possible, and are not allowed to re-enter the examination room.
- Candidates must stop writing when instructed to do so by the invigilator.
- Candidates must not detach any part of their answer sheet, or remove their answer sheet, wholly or partly, from the examination room.
- Candidates are not allowed to communicate with other candidates during an examination. They are also prohibited from communicating with third parties outside the examination room by using any electronic device. The invigilator has the right to expel candidates from the examination room if their behaviour interferes with the proper conduct of the examination. Any candidate attempting to copy from another candidate's script or any other source is disqualified.
- If any candidate infringes any of the above regulations, he/she is liable to disciplinary actions, including disqualification.

7.12 Examination Misconduct Handling

This section sets out the standards of conduct expected from candidates during HKIB examinations and the procedures for handling alleged misconduct.

1. Any infringement of these guidelines may result in disciplinary action, including disqualification.
2. Candidates who contravene the proper conduct of the examination will be warned by the invigilator or, in serious cases, expelled from the examination room. In such instances, a report will be submitted to HKIB for consideration of disciplinary action. Disciplinary measures may include, but are not limited to, disqualification of the candidate.
3. Candidates are strictly prohibited from communicating with other candidates during the examination. They must also refrain from contacting any third parties outside the examination room through any electronic device. The invigilator reserves the right to remove any candidate whose behaviour disrupts the proper conduct of the examination. Any candidate found attempting to copy from another candidate's script or conduct any other form of plagiarism or collusion will be disqualified.
4. Examples of misconduct during examination include:
    a. Improper communication or contact with other candidates
    b. Use of unauthorised electronic or communication devices
    c. Sharing, photographing, or otherwise capturing examination content

d. Suspicious or disruptive behaviour (e.g., repeated eye movements suggesting copying)
e. Possession of prohibited materials
f. Causing unnecessary disturbance in the examination room
g. Engaging in cheating, contract cheating or collusion

5. In determining whether misconduct has occurred, HKIB may consider the candidate's possible motive, any attempt to engage in misconduct, or any conduct that constitutes misconduct.
6. In the event of suspected misconduct by examination candidates, HKIB will implement a thorough and robust investigation process. If it is determined that misconduct has occurred, HKIB will notify the relevant candidate in writing.
7. As part of the appeal process for HKIB's decision, the candidate will have the opportunity to submit a written representation, including any mitigating factors, within 30 calendar days after providing intention notification to HKIB, providing any additional information or documentation as appropriate. If deemed necessary, HKIB may convene a disciplinary hearing panel, comprising members of HKIB Committees and attended by the candidate, to determine a final decision on the matter. During the hearing, the candidate will be given the opportunity to present additional information verbally. The candidate will receive the written final decision within 5 business days after the disciplinary hearing panel hearing.
8. Candidate behaviour considered to constitute misconduct during the examination will be classified into three levels of severity:

    Level 1: Individual dishonest behaviour without question leakage

    Examples:

    i. Continuing to write after the "time's up" announcement
    ii. Attempting to copy from another candidate

    Level 2: Individual dishonest behaviour with question leakage

    Examples:

    i. Attempting to communicate with a third party during the exam
    ii. Taking photos or recordings of the question paper

    Level 3: Group dishonest behaviour with question leakage

    Example:

    i. Sharing or coordinating answers among a group of candidates who are in the examination room

9. The reference starting points for penalties arising from candidate misconduct, corresponding to the three levels of severity, are as follows:

a. Level 1: Suspension from enrolling in HKIB Professional Qualifications Examinations for a period of 1 year; together with mandatory participation in a “remediation programme” as specified by HKIB.
b. Level 2: Suspension from enrolling in HKIB Professional Qualifications Examinations for a period of 3 years; together with mandatory participation in a “remediation programme” as specified by HKIB.
c. Level 3: Suspension from enrolling in HKIB Professional Qualifications Examinations, and exclusion from admission as a member and/or as a professional qualification holder, for a period of five years; together with mandatory participation in a “remediation programme” as specified by the HKIB.

10. The remediation programme will require mandatory participation in designated training courses provided by HKIB, focusing on professional ethics and compliance.
11. The decision of the disciplinary hearing panel is final.
12. HKIB will record all misconduct cases in the candidate’s personal records maintained by it.

8. Certification Application and Renewal Process

8.1 Certification Application

A Relevant Practitioner in cybersecurity functions of the banking industry who has completed the ECF on Cybersecurity (Core Level) Programme and obtained a pass at the examination may apply for ACsP Certification with HKIB professional membership.

Applicants are required to submit a completed Certification Application Form to HKIB together with the relevant supporting documents and payment of the required certification fee. The Certification Application form can be obtained from HKIB website.

Certification holders are registered as Certified Individuals (CI) and included in the public register on HKIB website. Upon successful application for the above certification, professional membership is also granted by HKIB.

8.2 Certification Renewal

Certification of ACsP is subject to annual renewal by HKIB.

PQ holders are required to comply the annual Continuing Professional Development (CPD) scheme requirements in order to renew their Certification.

For Core Level qualification, the requirement is a minimum of 20 verifiable CPD hours each calendar year and a minimum of 120 verifiable CPD hours over every 3 years period.

PQ holders are required to renew their certification registration annually by 31 December. Renewal email will be sent to members before renewal deadline. PQ holders who do not pay the certification renewal fee on or before 31 January of each calendar year are treated as Default Members.

8.3 Certification Fee, Certification Renewal Fee and Payment

- The application fee for Certification in various categories are as follows: (Valid until 31 December 2026)

Certification	First year certification - Non-HKIB Member: HKD2,230 - Current HKIB Ordinary Member (a) Complimentary: HKD2,230 / 970* - Current HKIB Professional Member: Waived

Certification Renewal	Annual Certification Renewal - Current HKIB Professional Member: HKD2,230 - Reinstatement fee for default member: HKD2,000

* Members who have paid the HKD1,260 Ordinary Membership fee for the current membership year are required to pay only the difference of HKD970 to complete their certification application.

- Applicants should pay the Certification Fee and Certification Renewal Fee as follows:

  (a) By Employer.

  (b) By credit card. Please provide your credit card information on the application form.

  (c) By FPS payment. Please provide your FPS payment receipt.

- Application forms without payment instruction will **NOT** be processed.
- **NO** fees are refunded or transferred under any circumstances.
- Applicants are advised to keep a record of their payment.
- HKIB reserves the right to adjust the certification, certification renewal and/or administration surcharge fees (if applicable), at any time.

8.4 Certification and HKIB Membership Regulations

It is mandatory for all individuals to maintain a valid membership status with HKIB if the applicants want to apply for and maintain the certification and be subject to HKIB membership governance.

Once an application is processed, the membership subscription and registration fees are non-refundable and non-transferable.

The name of the member to be entered on HKIB's records is that on the certification application form. This name, and the order and spelling in which it is presented, are used subsequently on all transcripts, pass lists, diplomas, and certificates except where a member has notified HKIB of any change. Such notification must be accompanied by a certified true copy[2] of documentary confirmation, e.g. Hong Kong Identity Card, birth certificate, statutory declaration, etc.

PQ holders are bounded by the prevailing rules and regulations of HKIB. They are abided by HKIB's rules and regulations in HKIB Members' Handbook. PQ holders are required to notify HKIB of any

[2] Submitted copies of documents to HKIB must be certified as true copies of the originals by:
- HKIB designated staff; or
- HR / authorized staff of current employer (Authorized Institution); or
- A recognised certified public accountant / lawyer / banker / notary public; or
- Hong Kong Institute of Chartered Secretaries (HKICS) member.

The certifier must sign and date the copy document (printing his/her name clearly in capital letters underneath) and clearly indicate his/her position on it. The certifier must state that it is a true copy of the original (or words to similar effect).

material changes to responses to any of the questions in application of the certification, including their contact details. HKIB may investigate the statements holders have made with respect to applications, and applicants may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in their applications.

8.5 Membership Reinstatement

Professional Members who have not paid the certification renewal fee when due shall be considered as default members and are not entitled to use any HKIB Professional Qualifications and neither may call themselves members of the Institute.

Default members who reinstate their membership with HKIB are required to pay the current year's certification renewal fee plus a reinstatement fee. Once the membership is reinstated, the member's examination record, if any, is reactivated.

9. General Information

9.1 Bad Weather Arrangements

In the event of bad weather on the training class/examination day, learners/candidates should pay attention to announcement made by the Hong Kong Observatory about weather conditions. They could also visit HKIB website for its announcements. For the respective individuals, they will be notified by SMS message about the latest arrangements.

Bad weather – Typhoon signal No. 8 or above, or the black rainstorm signal, or "extreme conditions" is hoisted.

For On-site Training

Signal in force	Bad Weather Arrangement
At or after 7am	Session starts from 9:00am to 2:00pm will be switched to virtual training class/event whenever possible.
At or after 12:00noon	Session starts from 2:00pm to 6:00pm will be switched to virtual training class/event whenever possible.
At or after 4:00pm	Session starts from 6:00pm to 10:00pm will be switched to virtual training class/event whenever possible.

For On-site Examination

Signal in force	Bad Weather Arrangement
At or after 7am	Session starts from 9:00am to 2:00pm will be rescheduled.
At or after 12:00noon	Session starts from 2:00pm to 6:00pm will be rescheduled.
At or after 4:00pm	Session starts from 6:00pm to 10:00pm will be rescheduled.

For Virtual Training / Remote Examination

Signal in force	Bad Weather Arrangement
At or after 7am	Session starts from 9:00am to 2:00pm will be continued as per schedule whenever possible.
At or after 12:00noon	Session starts from 2:00pm to 6:00pm will be continued as per schedule whenever possible.
At or after 4:00pm	Session starts from 6:00pm to 10:00pm will be continued as per schedule whenever possible.

9.2 Privacy Policy Statement

Personal data provided by the candidate are used for administrative and communicative purposes relating to training and examination. Failure to provide complete and accurate information may affect the provision of administrative services to the candidate. The Institute keeps the personal data provided confidential, but may need to disclose it to appropriate personnel in the Institute and other relevant parties engaging in the provision of examination services to the Institute. Candidates have the right to request access to and correction of their personal data in writing to HKIB by using HKIB's email address of cs@hkib.org.

Candidates are advised to read the Privacy Policy Statement at HKIB website to understand their rights and obligations in respect of the supply of personal data to HKIB and the ways in which HKIB may handle such data.

9.3 Addendums and Changes

HKIB reserves the right to make changes and additions to membership, training and examination regulations, enrolment / application procedures, information in this handbook and any related policies without prior notice. HKIB shall bear no responsibility for any loss to candidates caused by any change or addition made to the aforementioned items.

10. Contact Information

HKIB Head Office Address

3/F Guangdong Investment Tower, 148 Connaught Road Central, Hong Kong

General Enquiries

Tel.: (852) 2153 7800

Email: cs@hkib.org

Office Service Hours

Monday – Friday: 09:00 - 18:00 (except public holidays)