香港銀行學會
The Hong Kong Institute of Bankers

Advanced Certificate for ECF on Cybersecurity

<QF Level 4> *

Programme Handbook

(Syllabus, Regulations and General Information)

* This is a Specification of Competency Standards (SCS) based programme. The qualification is accredited by the Hong Kong Council for Accreditation of Academic and Vocational Qualifications (HKCAAVQ) with validity period from 15 Nov 2018 to 14 Feb 2022. (QR registration no. 18/000829/L4)

CSP-G-002
Last updated: 1 February, 2019

Table of Contents

1. Introduction

Given the growing number of cyber attacks 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 wants to complete the ECF on Cybersecurity training and examination with the intent of obtaining the Professional Designation of “Associate Cybersecurity Professional (ACsP)” which offered by HKIB and recognized by HKMA.

For more details, please refer to the HKMA’s Guide to ECF on Cybersecurity at http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf and the HKIB website at https://www.hkib.org/en/training-examinations/ecf/cybersecurity .

2. Background

A. 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.

B. Qualification Structure

The competency standards of the ECF on Cybersecurity comprise two levels: Core Level and Professional Level.

Core Level – This level is applicable for entry-level staff with less than 5 years of relevant work experience in the cybersecurity function;

Professional Level – This level is applicable for staff with 5 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

The coverage and competency requirements in the syllabus of the ECF on Cybersecurity are referenced to the Hong Kong Qualifications Framework (QF), with the Core Level being pitched at QF Level 4 and the Professional Level at QF Level 5. For details of QF, please refer to QF website at www.hkqf.gov.hk.

C. 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:

(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 in HKMA's Guide to ECF on Cybersecurity at http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf

D. Certification and Public Register

A relevant practitioner who has relevant work experience in cybersecurity, completed the "Advanced Certificate for ECF on Cybersecurity" training and passed the relevant examination are eligible to be certified as **ACsP**.

[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.

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

E. Annual renewal of certification and CPD Requirements

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

As a general guideline, Relevant Practitioners are expected to maintain a minimum of 20 CPD hours each year and a minimum of 120 CPD hours over every 3 years period.

No CPD is required in the year when the ACsP Certification is granted. The CPD requirement starts in the following calendar year.

F. Grandfathering

Grandfathering arrangement is not applicable for the ECF on Cybersecurity.

3. Programme Overview

3.1 Entry Requirements

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

- A Bachelor's Degree in any discipline awarded by a recognised university or equivalent; OR
- An Associate Degree (AD) / Higher Diploma (HD) in a banking and finance, computer studies/science, information systems/technology discipline or equivalent; OR
- Relevant professional qualifications; OR
- Mature applicants with either
  - At least five years of work experience in banking and finance, information systems/technology or equivalent; OR
  - Two years of work experience in banking and finance, information systems/ technology with a recommendation from the employer. Note
- Registered HKIB student members or post-secondary full-time students of the stated Diploma or Degree programmes.

Note: The recommended staff member should have the knowledge and skills to complete the training activities and achieve the intended learning outcomes. The employer should make the recommendation based on the competency of the potential learner. For example, in addition to 2 years of banking and finance experience, the recommended staff member also possesses other relevant traits and skills such as exhibiting a strong work ethic or transferable skills that the employer finds desirable. The recommendation may also include comments on the career advancement prospects of the staff member.

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 Learning 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.
- Conduct IT audits and security testing to assess cybersecurity risk protection.

3.4 Learning Hours

The programme design is adopted a blended learning approach. Learners are advised to spend not less than 200 Notional Learning Hours (equivalent to 20 QF credit). Notional 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 “Advanced Certificate for ECF on Cybersecurity” 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 “Advanced Certificate for ECF on Cybersecurity” training and obtained a pass at the relevant examination are encouraged to join the CB (Stage I) Programme.

For more details, please refer to the HKIB website at www.hkib.org/en/training-examinations/certified-banker .

3.6 Qualifications Framework

HKIB's "Advanced Certificate for ECF on Cybersecurity" has been officially accredited at Level 4 within the Qualifications Framework (QF) by the Hong Kong Council for Accreditation of Academic and Vocational Qualifications (HKCAAVQ). (QR registration number: 18/000829/L4)

This is a Specification of Competency Standards (SCS) based programme. Upon completion of this Advanced Certificate, graduates have the competencies to take up job positions in IT security operations and delivery, IT risk management and control and IT audit.

Please refer to website of HKQF and HKCAAVQ for details of SCS.

4. Learning Support

✚ *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.

✚ *Market Information Updates*

HKIB regularly organizes training courses, seminars and luncheon talks on current issues and developments in financial markets that candidates may find essential, helpful and relevant to their learning.

✚ *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.

An new e-learning course on “Cybersecurity Essentials” will be 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 will be available soon in the HKIB e-learning portal.

For more details, please refer to HKIB website at
https://secure.kesdee.com/ksdlms/?Partner=HKIB

5. Programme Syllabus

A. Syllabus

Chapter 1: Technical Foundation of Cybersecurity	
1	**Foundation of a Network** - OSI and TCP/IP Model - LAN and WAN Technologies and Devices - An Overview of Internet Architecture - Intrusion Detection System and Intrusion Prevention System - Common Network Protocols - DMZ and Network Segmentation - Wireless Network Infrastructure
2	**IT Security Principles** - Confidentiality, Integrity, Availability - Accountability, Non-repudiation - Types of Security Controls - Least Privilege - Separation of Duties - IT Asset Management
3	**Foundation of Access Control** - Access Control Concepts - Identification, Authentication, Authorisation - Identity Management - Common Access Control Implementation
4	**Overview of Cryptography** - Hashing - Salting - Symmetric/Asymmetric Encryption - Digital Signatures - Merkle Tree - Cryptographic Key Management

5	**Foundation of Cloud Computing** - Virtualisation - Infrastructure as a Service, Software as a Service and Platform as a Service - Public Cloud and Private Cloud - Data Governance on Cloud Computing - Jurisdiction Concerns
6	**Open Banking with the API Framework** - The Readiness of Open API Adoption
Chapter 2: Bank IT Security Controls	
1	**International Standards and Regulatory Requirements** - ISO 27001 Principles and Process - ISO 27001 Control Objectives - The HKMA’s Technology Risk Management Policies and Guidelines - Other International Standards
2	**Network Security Administration** - Understanding Wireless Security - Protecting the Network Infrastructure - Protecting the Network Management Platform - Network Vulnerability Management
3	**System Security Administration** - Database Security - System Hardening - Patch Management - Sandboxing - Application Whitelisting - Virtual Desktop
Chapter 3: Cybersecurity Monitoring	

1	**Threats, Malware and Malicious Activities** - Threats - Malware - Rootkits - Botnets - APT - DDoS
2	**Malware Infection Vectors** - Social Engineering - Spam, Phishing, Spear-phishing - Social Networking - Physical Media - Software Vulnerability - Watering Hole Attack
3	**Network and System Monitoring** - Log Files and Log Management - Security Events, Detection Mechanisms and Logs - Monitoring Tools - Wireless Attack Monitoring
4	**Network Attack Pattern Analysis** - SIEM Architecture and Components - Correlation Rule - Detection of Malicious Activities
Chapter 4: Security Incident Response	
1	**Security Incident Response Process** - Containment - Eradication - Recovery - Improvement - ISO 27043 Incident Investigation Principles and Processes

2	**Digital Evidence** - First Responder - Evidence Handling - Preservation of the Scene - Chain of Custody - Evidence Related to Network Events
3	**Security Incident Communication** - Internal Communication and Preparation of Management Reports - Structured Threat Information Expression (STIX) - Communication between Banks and Other Parties
Chapter 5: IT Risk Management and Control	
1	**Risk Management Process** - Risk Management Concepts - Risk Assessment - Risk Treatment (Accept, Transfer, Mitigate, Avoid)
2	**Risk Monitoring and Compliance Checking** - Risk Visibility - Risk Register and Risk Dashboard - Compliance Self-assessments
3	**Risk Acceptance** - Risk Ownership - Risk Acceptance Process
4	**Security and Risk Awareness Training**
Chapter 6: IT Audit	
1	**Principles of IT Audit** - Audit Team Functions - Independence - Audit Trail - IT Audit

2	**Security and Compliance Control Testing** - Document Review - Sampling - Walkthrough and Control Verification - Control Effectiveness Testing
3	**Audit Reports and Follow Up**
Chapter 7: Security Testing	
1	**Penetration Test Process** - Preparation - Vulnerability Scanning and Assessment - Network-layer Penetration Test - Application-layer Penetration Test
2	**Red Team Approach** - Red Team Testing Approach - Assume Breach

B. Recommended Readings

Essential Readings

HKIB Study Guide – Advanced Certificate for ECF on Cybersecurity (2018).

Supplementary Readings

1. Josiah Dykstra (2015). Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems, "O'Reilly Media, Inc."
2. Vacca, J. (Ed.). (2013). Computer and Information Security Handbook, Second Edition. Morgan Kaufmann.
3. 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
4. Cole, E. (2013). Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Syngress Publishing.
5. Michael S. Collins (2016) Network Security Through Data Analysis: Building Situational Awareness, 2nd Edition. "O'Reilly Media, Inc."

6. Federal Office for Information Security. (n.d.). A Penetration Testing Model. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf
7. Hong Kong Monetary Authority. (2016). Cyber Resilience Assessment Framework. Retrieved from http://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf
8. HKCERT https://www.hkcert.org/faq
9. CIS – Center of Internet security https://www.cisecurity.org/cybersecurity-best-practices
10. GovCERT https://www.govcert.gov.hk/en/index.html
11. Cybersechub https://www.cybersechub.hk/en/home/cert
12. HK Police CSTCB https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/index.html
13. HKIB e-learning course: Cybersecurity Essentials https://secure.kesdee.com/ksdlms/?Partner=HKIB

Further Readings

For Chapter 1:

1. Schneier, B. (1993). Applied Cryptography. John Wiley & Sons Inc.
2. Jonathan Katz, Yehuda Lindell, CRC Press. (2007). Introduction to Modern Cryptography: Principles and Protocols
3. Kavis, M. J. (2014). Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Wiley.

For Chapter 2:

1. BackTrack 5 Wireless Penetration Testing by V. Ramachandran, published in September 2011 by Packet Publishing
2. Australian Signals Directorate. (2018). Protect: Implementing Application Whitelisting. Retrieved from https://www.asd.gov.au/publications/protect/application_whitelisting.htm
3. Vacca , J. (Ed.). (2013). Computer and Information Security Handbook, Second Edition . Morgan Kaufmann.

For Chapter 3:

1. The Art of Deception: Controlling the Human Element of Security by Kevin D. Mitnick and William L. Simon, published in 2002 by John Wiley & Sons.

2. Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization by Eric Cole, published in 2013 by Syngress Publishing.
3. Applied Network Security Monitoring: Collection, Detection, and Analysis, by Chris Sanders and Jason Smith, published in 2014 by Syngress Publishing.

For Chapter 4:

1. Schultz, E. E. J., & Shumway, R. (2001). Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Sams Publishing.
2. 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.
3. Anatomy of a Breach, Microsoft. (2016)

For Chapter 5:

1. Hoo, K. J. (2000). How Much Is Enough? A Risk-Management Approach to Computer Security. US: Consortium for Research on Information Security and Policy.
2. General Principles for Technology Risk Management. (2003). HK: HKMA.
3. Joint Task Force Transformation Initiative (Ed.). (2012). Guide for Conducting Risk Assessments. HK: National Institute of Standards and Technology (NIST).
4. COBIT 5, ISACA
5. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
6. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems requirements
7. Trull, J. C. C. (2016, October 16). Use Security Education and Awareness Programs to Your Advantage. Available from: https://cloudblogs.microsoft.com/microsoftsecure/2016/10/26/use-security-education-and-awareness-programs-to-your-advantage/

For Chapter 6:

1. Leveraging COSO across the Three Lines of Defense. The Institute of Internal Auditors (2015).
2. Moeller, R. (Ed.). (2010). IT Audit, Control, and Security. Wiley.
3. National Institute of Standards and Technology. (2018). Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework

For Chapter 7:

1. Scarfone, K., Souppaya, M., Orebaugh, Angela, & Cody, A. (2008). Technical Guide to Information Security Testing and Assessment. NIST.
2. Shrestha, N. (2012). Security Assessment via Penetration Testing: A Network and System Administrator’s Approach. UNIVERSITY OF OSLO.

6. Training Application

A. Training Schedule

For the latest information about the training application period and class schedules, please contact HKIB staff or refer to HKIB website at https://www.hkib.org/en/training-examinations/ecf/cybersecurity/schedule

B. Training Duration

The training is set out as follows:

Training Mode	Lecture
Training Duration*	15 Hours

**15 hours are set as the standard training duration for the whole programme. If you have any special request and situation for a different training duration, please contact HKIB staff for special arrangement.*

C. Training Application

- Applicants can obtain an application form: (i) from HKIB website; or (ii) in person from the counter of HKIB Head Office during office hours.

Application Requirements:

- The information provided for the training enrolment must be true and clear.
- Completed application forms can be returned by fax or email, by hand or by registered mail (to avoid loss in transit) on or before the corresponding application deadline. Attention should be paid to the application deadline. Postal applicants are reminded to allow sufficient time for mailing or a late entry fee is charged.
- Inaccurate or incomplete applications may not be accepted even if the applicant has paid the training fee.
- Each applicant should submit only ONE application form for each programme.

- HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received an application form, NO alterations to the training arrangement are allowed.
- HKIB reserves the right to change training dates and application deadlines at any time.
- Applicants are advised to retain a copy of the completed application form for their own records.

D. Training Fee and Payment

Training	15 Hours
Fee	HK$ 3,600 (Study Guide Inclusive)

- Applicants should pay the training fee as follows:

  (a) By cheque (post-dated cheques are not accepted), attached to the application form. Cheques/E-cheques should be made payable to "The Hong Kong Institute of Bankers"; **OR**

  (b) By credit card. Please provide your credit card information on the application form.
- Application forms without payment instructions are **NOT** 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 payment.
- Confirmation of training application is sent to applicants via email at least **7 days** prior to the training date.
- **Late entries**: Late entries are accepted up to 7 days after stipulated application deadlines. A late entry fee of HK$200 (in addition to the module entry fee) applies.
- HKIB reserves the right to adjust training application, study guide and/or administration surcharge fees (if applicable), at any time.

7. Examination Application and Regulations

A. Examination Mode and Format

The examination mode and format are as follows:

<table>
<tr><td><b>Examination Mode</b></td><td colspan="2">Paper-based Examination</td></tr>
<tr><td><b>Examination Duration</b></td><td colspan="2">2.5 Hours</td></tr>
<tr><td><b>Question Type</b></td><td colspan="2">Multiple-choice Type Questions (MCQs)</td></tr>
<tr><td><b>No. of Questions</b></td><td colspan="2">80 MCQs</td></tr>
<tr><td><b>Pass Mark</b></td><td colspan="2">70%</td></tr>
<tr><td rowspan="7"><b>Grading</b></td><td>Pass with Distinction</td><td>Above 90%</td></tr>
<tr><td>Pass with Credit</td><td>80% - 90%</td></tr>
<tr><td>Pass</td><td>70% - 79%</td></tr>
<tr><td>Fail A</td><td>60% - 69%</td></tr>
<tr><td>Fail B</td><td>50% - 59%</td></tr>
<tr><td>Fail C</td><td>Below 50%</td></tr>
<tr><td>Absent</td><td></td></tr>
</table>

.

B. .Examination Timetable

- For latest information about the examination application period and examination dates, please contact HKIB staff or refer to HKIB website at https://www.hkib.org/en/training-examinations/ecf/cybersecurity/schedule .

C. 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 obtain an application form: (i) from HKIB website; or (ii) in person from the counter of HKIB Head Office during office hours.
- The information provided on the application form must be true and clear. Applicants should submit a completed and signed application form, together with the appropriate examination fee, to HKIB Head Office on or before the corresponding application deadline.
- Application forms can be returned by fax or via email, by hand or by registered mail (to avoid loss in transit). Attention should be paid to the application deadline. Postal applicants are reminded to allow sufficient time for mailing or a late entry fee is charged.
- **Late entries** are accepted up to 14 days after the stipulated application deadlines. A late entry fee of HK$200 (in addition to the module entry fee) applies.
- Inaccurate or incomplete applications may not be accepted even if the applicant has paid the examination fee.
- Each applicant should submit only ONE application form for each examination.
- 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 the application form, NO alterations to the examinations and examination arrangements are allowed.
- HKIB reserves the right to change examination dates and application deadlines at any time.
- Applicants are advised to retain a copy of the completed application form for their own records.

D. Examination Fee and Payment

First attempt	HK$1,020
Re-attempt	HK$1,020

- Applicants should pay the examination fee:

  (a) By cheque (post-dated cheques are not accepted), attached to the application form. Cheques / E-cheques should be made payable to "The Hong Kong Institute of Bankers"; **OR**

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

- Application forms without payment instruction are **NOT** 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.
- Acknowledgement of the examination application is sent to candidates via email within **7 working days** of receipt of application form. Candidates who fail to receive an acknowledgement within this time should inform the Institute immediately.
- HKIB reserves the right to adjust the examination, study guide and/or administration surcharge fees (if applicable), at any time.

E. *Examination Attendance Notice*

- Examination Attendance Notices (Attendance Notices) are sent to candidates via **email ONLY** approximately **2 weeks** before the examination. Candidates must inform the Institute if they have not received it **1 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.

F. 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 1 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.

G. 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.

H. 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.

I. Examination Results

- Candidates receive a result slip by post 2-4 weeks after the examination date.
- Results are not revealed by telephone, fax or email.
- Candidates may check their examination results online through the HKIB online platform. Candidates receive email notification once the examination results are available. The online examination results are removed 1 month after they are released.

- 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.
- Candidates may request rechecking or remarking of their examination scripts (not applicable to MCQ examinations) within 1 month of the issue of examination results, by submitting a written request. An administrative fee may apply. Please contact HKIB staff for details.

J. 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.

8. Certification Application Process

A. *Certification Application*

A Relevant Practitioner in cybersecurity functions of the banking industry who has completed the "Advanced Certificate for ECF on Cybersecurity" training and obtained a pass at the examination may apply for ACsP Certification with HKIB professional membership.

The applicants are required to submit a completed Application Form for ACsP Certification together with the relevant supporting documents and payment of the required Certification Fee to HKIB. The application form for ACsP Certification can be obtained from the HKIB website or HKIB Head Office.

ACsP holders will be registered as Certified Individuals (CI) and included in the public register on HKIB website. Upon successful application for certification with HKIB, HKIB will also grant the certificate holders a HKIB professional membership.

B. *Certification Fee and Payment*

- The application fee for Certification in various categories are as follows: *(Valid until 31 December 2019)*

Certification	1st year certification - Non-HKIB member: HK$1,600 - HKIB student member: HK$1,600 - HKIB ordinary member: HK$550 - HKIB professional member: **Waived** - HKIB Senior member: HK$1,400
Certification Renewal	Annual Fee - Certification: HK$1,600 - Re-registration Fee for Default Member: HK$2,000

- Applicants should pay the Certification Fee:

- By cheque (post-dated cheques are not accepted), attached to the application form. Cheques / E-cheques should be made payable to "The Hong Kong Institute of Bankers"; **OR**
- By credit card. Please provide your credit card information on the application form.

- 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, re-certification and/or administration surcharge fees (if applicable), at any time.

C. 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.

Certification holders would be bounded by the prevailing rules and regulations of HKIB. They are abide by HKIB's rules and regulations in HKIB Members' Handbook. Certification holders are required to notify HKIB of any material changes to responses to any of the questions in application of the certification, including their contact details. HKIB may investigate the statements certification holders have made with respect to applications,

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

Certifier must **sign** and **date** the copy document (printing his/her **name** clearly in capitals underneath) and clearly indicate his/her **position** on it. Certifier must state that it is a true copy of the original (or words to similar effect) and that they may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in their applications.

Certification holders have the responsibility to notify HKIB of any material changes to responses to personal information required, including contact details. The HKIB may investigate the statements the applicant makes with respect to certification application, and that the applicant may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in certification application.

D. Membership Reinstatement

Members who have not paid the annual subscription fees when fall due shall be considered as default members, and are not entitled to use any HKIB designations, and must not claim themselves as members of the Institute.

Default members who reinstate their membership with HKIB are required to pay the current year's subscription plus a re-registration fee. Once the membership s 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, candidates should visit HKIB website at www.hkib.org for announcements about the latest arrangements, and should pay attention to radio/ television broadcasts about weather conditions.

- If the typhoon signal No. 8 or above, or black rainstorm signal is hoisted or still in force on the day of a training class, the arrangements below apply:

Signal in force	Training Class(es) cancelled
At 6:30am	Morning Session (8:30am – 2:00pm) is cancelled.
At 12:00noon	Afternoon Session (2:00pm – 6:00pm) is cancelled.
At 3:00pm	Evening Session (6:00pm – 10:00 pm) is cancelled.

- If the typhoon signal No. 8 or above, or brainstorm signal is hoisted or still in force on the day of an examination at the following times, the arrangements below will apply:

Signal in force	Examination cancelled
At 6:00am	Examination(s) (8:00am – 1:00pm) are cancelled.
At 10:00am	Examination(s) (1:00pm – 5:00pm) are cancelled.
At 2:00pm	Examination(s) (at 5:00pm or after) are cancelled.

- If typhoon signal No. 8 or above, or black rainstorm signal, is hoisted or still in force while the training class / examination is in progress, the training class / examination continues as scheduled.

- If a training class / examination is rescheduled, HKIB notifies candidates of the new training class / examination date and time by email within **1 week** of the originally scheduled date. Under such circumstances, candidates are not required to re-register for the training class / examination. Applications for a refund and/or transfer are NOT allowed.

- HKIB reserves the right to postpone, cancel and/or reschedule any training class/ examination.

9.2 Personal Data Protection Policy

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. For details, candidates can contact the Institute.

Candidates are advised to read the Personal Data Protection Policy at **Appendix** 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.

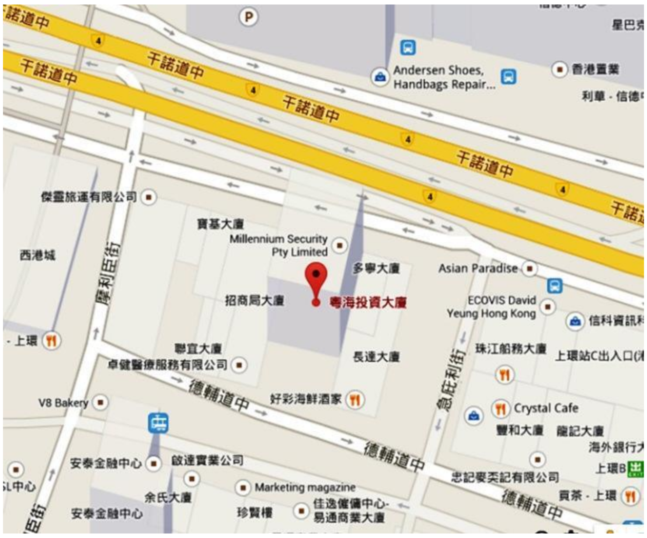
9.3 Addendums and Changes

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, Training and Programme Enquiries

Tel.: (852) 2153 7800 Facsimile: (852) 2544 9946
Email: hkib@hkib.org or ecf.cybersecurity@hkib.org

Membership Enquiries

Tel.: (852) 2153 7879 Email: membership@hkib.org

Examination Enquiries

Tel.: (852) 2153 7821 Email: exam@hkib.org

Office Service Hours

Monday – Friday: 09:00 - 18:00

Appendix: Personal Data Protection Policy

When HKIB collects information from participants in our activities, training and/or examinations ("Participants"), it is our policy to meet fully the requirements of the Ordinance, which regulates the treatment of personal data. Throughout this policy, the meaning of the term "personal data" is as defined in the Ordinance. In dealing with personal data, we ensure compliance by our staff with the standards of security and confidentially prescribed under the Ordinance.

1. All information of a personal nature obtained by HKIB is for the purposes of administering our services, which may include, but are not limited to: training, examinations and other activities organized wholly or in part by HKIB; conducting subsequent performance assessments; and handling related irregularities, if any.

   Personal data are supplied either by Participants themselves or from external sources, including, but not limited to: employers, service or learning providers, third parties who are otherwise affiliated to the service in which Participants are involved, and, who may provide HKIB with relevant information on their employees, members and/or students; and members of the public.

   After the data obtained from Participants have been captured, processed and checked, hard copies – for example, of Participants' information checklists or Attendance Notices – may be produced for all HKIB services in order to ensure accuracy of the data. Some data may also be used for the following purposes during registration and/or payment:

   - To verify Participants' identities;
   - To fulfill Participants' specific requests, applications or enrolments relating to our services;
   - To administer and deliver information about the service;
   - To maintain and process examination marks and results, if any;
   - To process and handle Participants' complaints, enquiries, feedback or irregularities, if any;
   - To maintain Participants' records;
   - To conduct research or statistical analysis;
   - To release information to relevant third parties on whose behalf HKIB administers, conducts or organised services, and to any third party that HKIB engages to administer and/or conduct services for and on behalf of HKIB;
   - To promote and provide various HKIB member services to Participants;
   - To serve other purposes as permitted by law; and

- To serve any other purposes as may be agreed between Participants and HKIB.

2. HKIB keeps personal data of Participants' confidential. Nevertheless, as part of its operations, HKIB may compare, transfer or exchange their data with the data already in HKIB's possession, or obtained hereafter by HKIB, for these or any other purposes.

3. HKIB is also professionally obliged to process the personal data fairly, confidentially and lawfully.

4. The provision of personal data or any information is voluntary. However, failure to provide the requested personal data may result in HKIB being unable to process Participants' requests, perform its statutory functions or deliver its services to Participants.

5. HKIB may contact a Participant if we require confirmation of his/her identity, or further information about the data requested that may assist HKIB to locate his/her personal data before complying with his/her request.

6. HKIB uses the data only for specifically or directly related purposes, as outlined on its enrolment / application form and the accompanying explanatory notes, if any. No exception to this rule is permitted without the express permission of HKIB.

7. HKIB recognises the sensitive and highly confidential nature of much of the personal data it handles, and maintains a high level of security in its work. HKIB has well-established guidelines and procedures for maintaining the security of all personal data, both as hard copies and in computer-readable form.

8. HKIB will do its best to ensure compliance with the Ordinance by providing guidelines and monitoring the compliance of the relevant parties. However, HKIB cannot control how third parties use Participants' personal information and assumes no responsibility for privacy protection provided by such third parties.

9. The means of Participants' communications with HKIB, including online, email, text message (SMS), and HKIB's customer hotline, may be recorded and retained for training and record-keeping purposes. Records may be used to monitor the quality of the assistance given and to verify the matters discussed.

Personal data protection in regions outside Hong Kong is subject to the requirements of these jurisdictions.

Responsibility and Rights of Candidates

Participants are required to keep HKIB informed of any changes in their personal data once they have enrolled as Participants for services offered by HKIB or for an examination, and until such time as the service is completed or Participants have completed the examination. HKIB has well-established procedures to verify and process the amendment of Participants' particulars. After the data obtained from the enrolment / application forms have been captured, processed and checked, hard copies – for example, of Participants' information checklists or Attendance Notices – may be produced for all services offered by HKIB in order to ensure accuracy of personal data.

Under the Ordinance participants have the right to request access to, or correction of any data provided by them as per the manner and limitations prescribed therein. As the Ordinance allows, HKIB has the right to charge a reasonable fee for processing request for data access.

Participants who request access to data or correction of their data should do so in writing to HKIB. Participants should also write to HKIB if they do not want to receive any information on services offered by HKIB.

Data Retention

Unless otherwise agreed, hard copies of all documents containing Participants' personal data they have provided to HKIB become the property of HKIB. HKIB destroys all documents it holds in accordance with its internal policy and applicable laws.

Personal data are retained only for such period as may be necessary for carrying out the purposes stated in this policy or as otherwise specified at the time of collection. In some circumstances, HKIB may retain certain records for other legitimate reasons, including to resolve disputes, cross-check against future examination application, if applicable, and to comply with other reporting and retention obligations.

Transfer of Personal Data Outside of Hong Kong

At times it may be necessary and prudent for HKIB to transfer certain personal data to places outside Hong Kong SAR, in order to carry out the purposes, for which the personal data were collected. Where such a transfer is performed, it is done in compliance with the requirements of the Ordinance.

Amendments

HKIB reserves the right to change or modify its privacy policy at any time without prior notice. Any such change or modification shall be effective immediately upon posting of the changes and modification on this website.

Enquiries

All access/ correction requests and any enquiries about this privacy policy statement should be directed to HKIB at the address and telephone numbers below:

The Hong Kong Institute of Bankers
3/F Guangdong Investment Tower
148 Connaught Road Central
Hong Kong
Tel.: (852) 2153 7800
Facsimile: (852) 2544 9946
Email: hkib@hkib.org