



Advanced Certificate for ECF on Cybersecurity

QF Level 4

(QR registration no. 18/000829/L4) #



Scan our QR code to
visit our website



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.

Enhanced Competency Framework for Banking Practitioners

With an aim to support capacity building and talent development for banking professionals, the Hong Kong Monetary Authority (HKMA) works together with the banking industry to introduce an industry-wide competency framework - Enhanced Competency Framework (ECF) for banking practitioners.

Under the industry-wide ECF for banking practitioners, the ECF on Cybersecurity was introduced which enables cybersecurity talent development and facilitates the building of professional competencies and capabilities of those staff engaged in cybersecurity related duties currently or in future.

Qualifications Framework by HKCAAVQ

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)

The Programme is a Specification of Competency Standards (SCS) based programme. The learning content is encompassing all relevant Units of Competency (UoC) drawn from the SCS of banking industry.

Becoming an Associate Cybersecurity Professional (ACsP)

(1) Training Programme and Examination

To earn the certification of Associate Cybersecurity Professional (ACsP), candidates must successfully complete the programme "Advanced Certificate for ECF on Cybersecurity". They must first complete the training sessions, and proceed to the examination afterward. After passing the examination, they will be awarded the "Advanced Certificate for ECF on Cybersecurity".

(2) Certified Individual (CI)

It is mandatory for all individuals to maintain a valid membership status with HKIB if the applicants want to apply for and maintain the ACsP designation. ACsP Certification Holders will be registered as CI and included in a public register on the HKIB website. The CI Register posted on the HKIB website enables the public recognition of ACsP Certification Holders.

(3) Continuing Professional Development (CPD)

All ACsP Certification Holders are required to comply with annual Continuing Professional Development (CPD) Scheme. ACsP Certification Holder is required to undertake a minimum of 20 CPD hours each year and a minimum of 120 CPD hours over every 3 years period.

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.

Learning Outcomes

Upon completion of the programme, candidates 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.

Programme Outlines

- Enhance learners' comprehension of fundamental concepts, principles and theories in networking and cybersecurity which allow participants to apply in personal and work environment
- Acquire the knowledge of different aspects of cybersecurity:
 - Technical Foundation of Cybersecurity
 - Bank IT Security Controls
 - Cybersecurity Monitoring
 - Security Incident Response
 - IT Risk Management and Control
 - IT Audit
 - Security Testing
- Participants shall be able to identify potential security threats and apply early intervention to common cyber security problems

Target Participants

Entry-level relevant practitioners who perform the relevant tasks in cybersecurity function

Entry Requirements

The programme is open to members / non-members of HKIB. Candidates must fulfill 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 5 years of work experience in banking and finance, information systems / technology or equivalent; OR
 - 2 years of work experience in banking and finance, information systems / technology with a recommendation from the employer.
- Registered HKIB student members or post-secondary full-time students of the stated Diploma or Degree programmes

Certification

The Relevant Practitioners in Cybersecurity sectors of the banking industry will be certified as an Associate Cybersecurity Professional (ACSP) at Core Level when they have successfully:

- completed the training programme; AND
- passed the examination

Medium of Programme

- Training is delivered through classroom and self-study in either Cantonese or English supplemented with English materials.
- All the examination questions are set in **English** only.

Learning Mode

Tuition (15 Hours)

Application

Email : application@hkib.org

In person/ Mail : 3/F Guangdong Investment Tower,
148 Connaught Road Central, Hong Kong

Please visit the HKIB website for application details.

General Enquiries

Tel : (852) 2153 7800

Email : ecf.cybersecurity@hkib.org

Website : www.hkib.org

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

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.

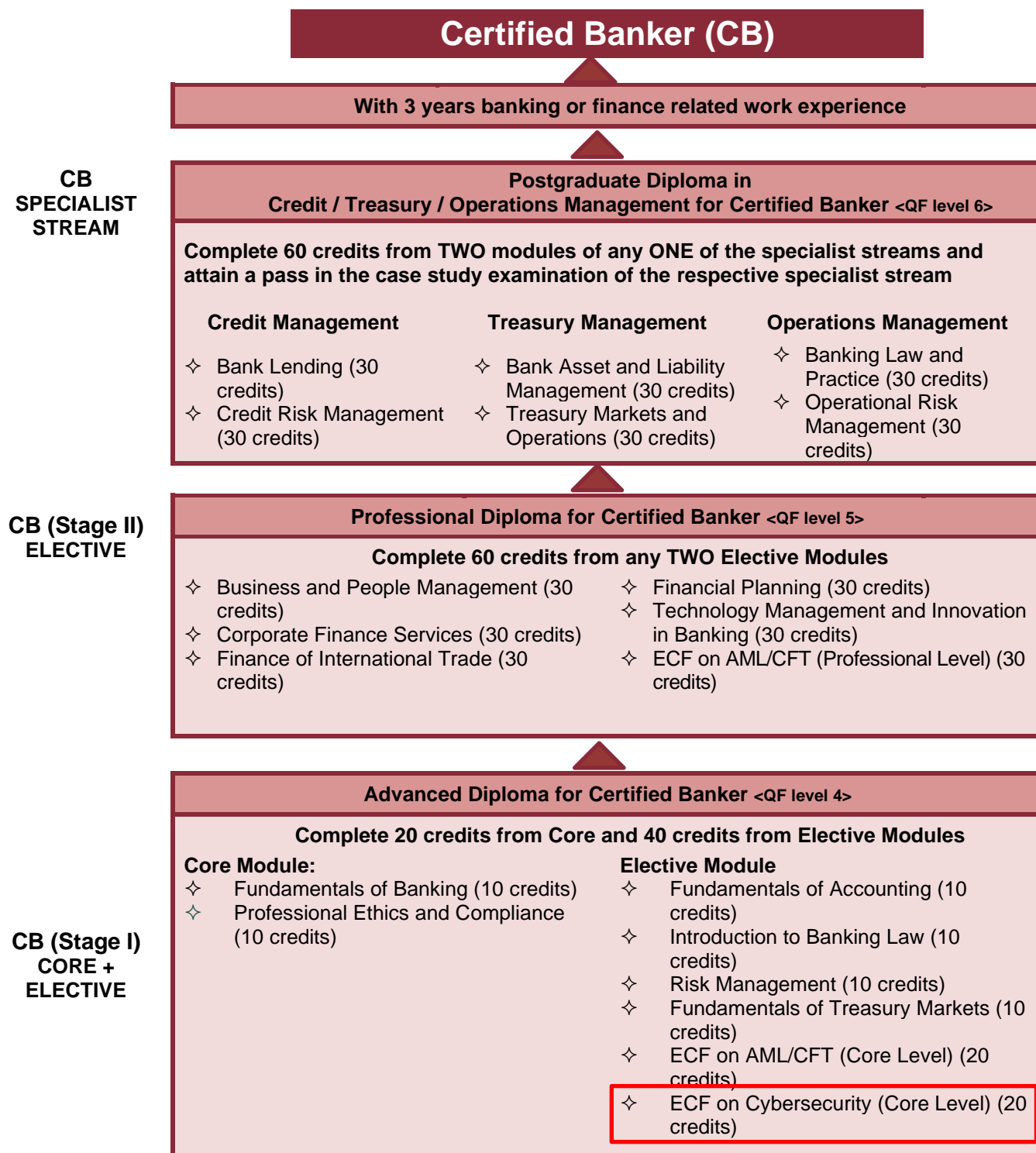
Copyright of HKIB - All rights reserved

CSP-G-004

Last updated: 1 April 2020

Integration of ECF in Certified Banker (CB)

Certified Banker (CB) is a professional banking qualification programme developed and offered by HKIB. This common qualification benchmark 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” and obtained a pass at the relevant examination are eligible to articulate to study for CB (Stage I) programme. Candidates can then apply for an exemption for the elective module “ECF on Cybersecurity” of the CB (Stage I) programme.



For more details, please visit: <https://www.hkib.org/page/73>