Guidelines of Certification Application for ECF on Cybersecurity (Core Level)

Introduction

This document is developed to provide more specific guidelines for the certification application for ECF on Cybersecurity (Core Level). It includes information related to (A) Eligibility Criteria, (B) Application Procedure and (C) Recertification Arrangement for the application.

A. Eligibility Criteria

1. Relevant Practitioner

The Enhanced Competency Framework (ECF) on Cybersecurity (Core Level) is targeted at "Relevant Practitioners (RPs)", including new entrants and existing practitioners, engaged by an **Authorized Institution (AI)**[1] to perform cybersecurity roles in banking industry. It is intended that the ECF on Cybersecurity (Core Level) applies to staff performing cybersecurity roles with key tasks listed in the below table.

Key Roles/ Responsibilities	
Role 1: IT Security Operations and Delivery	
Operational Tasks	**Technical Tasks**
1. Implement and enforce the bank's IT security policies. 2. Responsible for the day-to-day security operation of the bank including access control configuration, reviewing programme changes requests, reviewing IT incidents, security reporting and etc. 3. Implement cybersecurity monitoring framework. 4. Collect data on cybersecurity related risk, attacks, breaches and incidents, including external data and statistics as appropriate. 5. Investigate security incidents by gathering evidence and reviewing system logs/ audit trails. 6. Provide operational support to systems and network teams regarding security related matters.	1. Monitor network traffic through implemented security tools to proactively identify indicators of compromise (e.g. Host based IDS/ IPS, network based IDS/ IPS, firewall logs, application logs). 2. Perform maintenance and operation support for security devices such as firewall, IPS/ IDS, VPN, anti-virus and encryption services. 3. Participate in developing, tuning and implementing threat detection analytics.

[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.

Guidelines of Certification Application for ECF on Cybersecurity (Core Level)

Key Roles/ Responsibilities
Role 2: IT Risk Management and Control
1. Assist management in developing processes and controls to manage IT risks and control issues. 2. Assist in communicating the risk management standards, policies and procedures to stakeholders. 3. Apply processes to ensure that IT operational and control risks are at an acceptable level within the risk thresholds of the bank, by evaluating the adequacy of risk management controls. 4. Analyse and report to management, and investigate into any non-compliance of risk management policies and protocols.
Role 3: IT Audit
1. Assist in the execution of audits in compliance with audit standards. 2. Assist in the fieldwork and conducting tests. 3. Assist in evaluating data collected from tests. 4. Document the audit, test and assessment process and results. 5. Ensure appropriate audit follow-up actions are carried out promptly.

Please refer to HKMA's circular on "Enhanced Competency Framework on Cybersecurity" dated 10 Jan 2019 for more details.

2. Other Certification Requirements

RPs are also required to fulfil the following requirements:

- Completed the training programme and passed the examination for the Core Level; and
- Currently performing cybersecurity function (e.g. IT Security Operations and Delivery, IT Risk Management and Control, IT audit)

Guidelines of Certification Application for ECF on Cybersecurity (Core Level)

B. Application Procedure

1. Please follow the application procedure as below:

(a) Complete all the necessary fields in the relevant Certification Application Form for ECF on Cybersecurity, including applicant's signature and HR endorsement in relevant sections.

- For Core Level: CSP-G-023

(b) Obtain endorsement from the Human Resources Department (HR) of the concerned Authorized Institution(s) with signature of Head of HR or equivalent and company chop on the HR Verification Annex (Core Level) of the above Application Form. **Applications can only be accepted with HR endorsement included.**

If required, the HKIB may request applicants to provide employment records or additional information to substantiate their applications.

(c) Read Privacy Policy Statement set out on the HKIB's website before submitting applications.

(d) Send the completed Application Forms with HR department's endorsement, relevant supporting documents (e.g. copy of your HKID / Passport, copies of the examination result for Advanced Certificate for ECF on Cybersecurity) and payment evidence to the HKIB.

2. Fee Payable

- A **Non-refundable** fee is required for **ACsP** certification application.
- For details, please refer to the Fee Table of the Grandfathering and/or Certification Application of respective ECF which is available on the HKIB's website.

3. Payment Method

(a) Paid by Employer

(b) A crossed cheque or e-cheque made payable to "**The Hong Kong Institute of Bankers**" (Post dated cheques will not be accepted).

(c) Credit card (Visa or Mastercard)

Guidelines of Certification Application for ECF on Cybersecurity (Core Level)

4. Submission of Application

Please complete and submit the **SIGNED** application form together with the required documents via email to cert.gf@hkib.org or by post/ in person to The Hong Kong Institute of Bankers (HKIB) at the following address:

"Certification Application for ECF on Cybersecurity (Core Level)"
Department of Professional Assessment and Certification
The Hong Kong Institute of Bankers
3/F Guangdong Investment Tower
148 Connaught Road Central, Hong Kong

Note: Please ensure sufficient postage is provided when sending out the required documents.

5. Approval and Election

(a) The certification processing time, including the election process done by the HKIB committee members, will require **approximately 2 months**.

(b) Upon the successful completion of the certification process, **ACsP** holders will be registered as **Certified Individuals (CI)** and be included in a public register on the HKIB's website. The HKIB will also grant the holder a professional membership. **ACsP** Professional Qualification holders are then entitled to print the Professional Qualification on their business cards and curriculum vitae to signify their professional excellence.

(c) Besides, the professional qualification holders' names will also be presented on the HKIB website and published in the Institute's journal "Banking Today" and Annual Report.

C. Recertification Arrangement

1. Subject to the HKIB membership governance, if the applicant wants to maintain his/her **ACsP** professional qualification, he/she is required to renew his/her certification annually and to maintain a valid membership status with HKIB. The applicant must also be an RP who has met the annual **Continuing Professional Development (CPD)** requirement and pay the annual renewal of certificate fee.

2. **ACsP** holders are bound by the prevailing rules and regulations of the HKIB. They must abide by the HKIB's rules and regulations as per the HKIB Members' Handbook. **ACsP** holders are required to notify the HKIB of any material changes in their applications for certification, including their contact details. The HKIB may investigate the statements **ACsP** holders have made with respect to their applications, and that they may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in their applications.

3. To maintain ongoing professionalism and standards, **ACsP** holders are required to undertake a minimum of **20 CPD hours** each year, and a minimum of **120 CPD hours** over every 3 years period.

4. The renewal of **ACsP** certification is subject to fulfilment of the annual CPD requirements starting from the calendar year (**from 1 January to 31 December**) following the year of certification.

5. The CPD requirements are waived in the first calendar year (**ending 31 December**) of certification.

   For the avoidance of doubt, RPs who are captured under multiple ECFs are only required to fulfil the CPD hours for one of his/her certifications per year (i.e. whichever is greater).

--END--