

Received on:

Acknowledged on:

Application no:

Certification Application Form for Associate Cybersecurity Professional (ACSP)

Important notes:

1. The application is only for the **Relevant Practitioner** engaged by an Authorized Institutions (AIs) at the time of application **ONLY**.
2. Read carefully the “Guidelines of Certification Application for Associate Cybersecurity Professional (ACSP)” (CSP-G-017) **BEFORE** completing this application form.
3. Only **completed application form** with all valid supporting documents, including the HR verification forms, will be processed.

Section A: Personal Particulars¹

Title: <input type="checkbox"/> Mr <input type="checkbox"/> Ms <input type="checkbox"/> Dr <input type="checkbox"/> Prof		HKIB Member: <input type="checkbox"/> Yes _____ <input type="checkbox"/> No <i>(Membership No.)</i>	
Name in English ² : <i>(Surname) (Given Name)</i>		Name in Chinese ² :	
HKID/ Passport Number:		Date of Birth: <i>(DD/ MM/ YYYY)</i>	
Contact information			
(Primary) Email Address ³ :		Mobile Phone Number:	
(Secondary) Email Address:			
Correspondence Address:			
Employment information			
Name of Current Employer:		Office Telephone Number:	
Position/ Job Title:		Department:	
Office Address ⁴ :			
Academic and Professional Qualification			
Highest Academic Qualification Obtained:	University/ Tertiary Institution:	Received on:	Date (of Award) only
Other Professional Qualifications:	Professional Bodies:	Acknowledged on:	Application no:

1. Put a “✓” in the appropriate box(es)
2. Information as shown on identity document
3. All the HKIB communication will be sent to the Primary Email Address (Personal email preferred).
4. Provide if not the same as the correspondence address above.

Section B: Application Type

ACSP Certification Application

Eligibility:

- Completed ECF on Cybersecurity (Core Level) trainings and passed the examinations for the Advanced Certificate for ECF on Cybersecurity; and
- Currently performing cybersecurity function (e.g. IT Security Operations and Delivery, IT Risk Management and Control, IT audit); and
- Employed by an AI at the time of application.

Section C: Declaration related to Disciplinary Actions, Investigations for Non-compliance and Financial Status

Put a “✓” in the appropriate box(es). If you have answered “Yes” to any of the questions, provide details by attaching all relevant documents relating to the matter(s).

1. Have you ever been reprimanded, censured, disciplined by any professional or regulatory authority?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Have you ever had a record of non-compliance with any non-statutory codes, or been censured, disciplined, or disqualified by any professional or regulatory body in relation to your profession?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Have you ever been investigated about offences involving fraud or dishonesty or adjudged by a court to be criminally or civilly liable for fraud, dishonesty, or misfeasance?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Have you ever been refused or restricted from the right to carry on any profession for which a specific license, registration, or other authorisation is required by law?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Have you ever been adjudged bankrupt, or served with a bankruptcy petition?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Section E: Privacy Policy Statement

It is our policy to meet fully the requirements of the Personal Data (Privacy) Ordinance. HKIB recognises the sensitive and highly confidential nature of much of the personal data of which it handles, and maintains a high level of security in its work. HKIB does its best to ensure compliance with the Ordinance by providing guidelines to and monitoring the compliance of the relevant parties.

For more details, please refer to this [Privacy Policy Statement](#) or contact us at the address and telephone number below:

The Hong Kong Institute of Bankers
3/F Guangdong Investment Tower
148 Connaught Road Central, Hong Kong

Tel: (852) 2153 7800

Fax: (852) 2544 9946

Email: cs@hkib.org

- The HKIB would like to provide the latest information to you via weekly eNews. If you do not wish to receive it, please tick the box.***

FOR INSTITUTE USE ONLY		
Received by:	(Staff Name)	(Date)
_____	_____	_____
Assessed by:	(Staff Name)	(Date)
_____	_____	_____
<input type="checkbox"/> Approved / <input type="checkbox"/> Rejected by:	(Staff Name)	(Date)
_____	_____	_____
Remarks:	_____	

Section F: Acknowledgement and Declaration

- I declare that all information I have provided in this form is true and correct.
- I understand that the fees paid are non-refundable and non-transferable.
- I authorise the HKIB to obtain the relevant authorities to release, any information about my qualifications and/ or employment as required for my application.
- I acknowledge that the HKIB has the right to withdraw approval of grandfathering and/or certification status if I do not meet the requirements. I understand and agree that the HKIB may investigate the statements I have made with respect to this application, and that I may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in this application.
- I confirm that I have read and understood the [Privacy Policy Statement](http://www.hkib.org) set out on the HKIB website at <http://www.hkib.org>, and consent to the terms set out therein. I also understand that the Institute will use the information provided and personal data collected for administration and communication purposes.
- I have read and agreed to comply with the “Guidelines of Certification Application for Associate Cybersecurity Professional (ACsP)” (CSP-G-017).

Document Checklist

To facilitate the application process, please check the following items before submitting to the HKIB. Failure to submit the documents may cause delays or termination of application. Please “✓” the appropriate box(es).

- All necessary fields on this application form filled in including your signature
- Completed form(s) of HR Verification Annex fulfilling the requirements as stipulated for certification application
- Certified true copies of your HKID/Passport ⁵
- Payment or evidence of payment enclosed (e.g. cheque or completed Credit Card Payment Instructions)

5. Submitted copies of documents to the HKIB must be certified as true copies of the originals by:

- The HKIB staff; or
- HR/authorised staff of current employer (Authorized Institution); or
- A recognized certified public accountant/lawyer/notary public; or
- Associateship/Fellowship of Chartered Governance Hong Kong.

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).

Signature of Applicant

(Name: _____)

Date

THIS PAGE IS INTENTIONALLY LEFT BLANK

**Certification Application Form
for Associate Cybersecurity Professional (ACsP)**

HR Department Verification Form on Employment Information for Cybersecurity Practitioner

Important notes:

1. A completed Certification Application Form for ACsP should contain p.1-5 plus this **HR Verification Annex (ACsP)** form(s) (p.AC1-AC3).
2. Fill in **ONE set of HR Verification Annex form for CURRENT relevant position/functional title** in your application.
You can make extra copies of this blank form for use.
3. All information filled in including company chop must be true and original.
4. Use BLOCK LETTERS to complete this form.

Employment Information	
Name of the applicant:	
HKID/Passport number:	
Current Position/Functional title:	
Name of Current employer:	
Business division/department:	
Employment period of the <u>Current</u> position /functional title: <i>(DD/MM/YYYY)</i>	From: To:
Key roles/responsibilities in relation to the <u>stated</u> position/functional title: <i>(Tick the appropriate box(es); Application will be processed based on the role(s) ticked)</i>	<input type="checkbox"/> Role 1 – IT Security Operations and Delivery <i>(fill in p.AC2)</i> <input type="checkbox"/> Role 2 – IT Risk Management and Control <i>(fill in p.AC2)</i> <input type="checkbox"/> Role 3 – IT Audit <i>(fill in p.AC3)</i>
Total number of years and months of carrying “Role 1”, “Role 2” or “Role 3” function in the <u>stated</u> position	_____years _____months
Work Location	<input type="checkbox"/> Hong Kong <input type="checkbox"/> Others, please specify: _____

Applicant please self-declares by ticking the appropriate “Key Roles/Responsibilities” in relation to your position/functional title stated on **p.AC1 of HR Verification Annex (ACsP)** form.

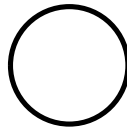
Key Roles/ Responsibilities	Please “√” where appropriate
<input type="checkbox"/> Role 1 – IT Security Operations and Delivery	
<input type="checkbox"/> Operational Tasks:	
1. Implement and enforce the bank’s IT security policies	
2. Responsible for the day-to-day security operation of the bank including access control configuration, reviewing program 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 appreciate	
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	
<input type="checkbox"/> Technical Tasks:	
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	
<input type="checkbox"/> 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	

Applicant please self-declares by ticking the appropriate “Key Roles/Responsibilities” in relation to your position/functional title stated on **p.AC1 of HR Verification Annex (ACsP)** form.

Key Roles/ Responsibilities	Please “✓” where appropriate
<input type="checkbox"/> 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	

Verification by HR Department

The Employment Information provided by the applicant in this form has been verified to be consistent with the information on the applicant that is retained by the HR department of the applicant’s employer (where the organisation has a record of this information).



Signature & Company Chop

Date

Name: _____

Department: _____

Position: _____

THIS PAGE IS INTENTIONALLY LEFT BLANK

Authorisation for Disclosure of Personal Information to a Third Party

I, _____, (*name of applicant*) hereby authorise
The Hong Kong Institute of Bankers (HKIB) to disclose my results and progress of the
“Grandfathering/Examination/Certification/Exemption results for ECF on Cybersecurity” to
_____ (*applicant’s bank name*) for HR and Internal Record.

Signature

HKIB Membership No./HKID No.*

Date

Contact Phone No.

**The HKIB Membership No./HKID No. is needed to verify your identity. We may also need to contact you concerning the authorisation.*

Important notes:

1. Personal information includes but is not limited to grandfathering/examination/certification/exemption results of a module/designation and award(s) achieved.
2. Original copy of this signed authorisation form must be submitted to the HKIB. Electronic or photocopied signatures are not acceptable.
3. Applicant may rescind or amend consent in writing to the HKIB at any time, except where action has been taken in reliance on this authorisation.