HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B9/166C

19 December 2016

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Enhanced Competency Framework on Cybersecurity

I am writing to introduce the launch of the Enhanced Competency Framework (ECF) on Cybersecurity.

Authorized institutions (AIs) have increased their reliance on technologies and online channels to deliver innovative banking services to their customers. The level of cyber resilience, which contributes to the operational resilience, is becoming a decisive factor in the overall resilience of the systems and operating environment of AIs. Given the growing number of cyber attacks to financial institutions in recent years, it is essential to improve AIs' preparedness and capability to defend for such attacks.

In this connection, the Hong Kong Monetary Authority (HKMA) and the banking industry have worked together to develop an industry-wide ECF on Cybersecurity for the banking sector. This framework enables cybersecurity talent development and facilitates the building of professional competencies and capabilities of those staff engaged in cybersecurity duties.

In addition, the Guide to ECF on Cybersecurity is attached to this letter. The Guide aims to provide details of the scope of application, qualification structure, recognised certificates and continuing professional development requirements to equip relevant staff with the right skills, knowledge and behaviour. As the Supervisory Policy Manual module CG-6 "Competence and Ethnical Behaviour" has already emphasised the importance of ensuring continuing competence of AIs' staff members, AIs are therefore encouraged to make use of the ECF on Cybersecurity to raise and maintain professional competence of their cybersecurity practitioners.

Separately, AIs are advised to keep records of the relevant training and qualifications. The HKMA will assess the progress of implementation of the ECF on Cybersecurity by AIs and AIs' effort in enhancing staff competence in this area during its on-going supervisory process.

In the meantime, if you have any enquiries relating to this circular, please contact Mr Josiah Lam on 2878 1425 or Mr Wilson Pang on 2878 1249.

Yours faithfully,

Arthur Yuen
Deputy Chief Executive

Encl.

c.c. FSTB (Attn: Ms Eureka Cheung)

Guide to
Enhanced Competency Framework
on Cybersecurity

Hong Kong Monetary Authority

December 2016

Table of Contents

1. Introduction

1.1 Cybersecurity has become more important to the banking sector. According to research, in 2015, the global average annualised cost of cybercrimes amounted to HK$59.73 million (equivalent to US$7.7 million) per year.[1] The same research shows that the financial sector is experiencing the highest average annualised cost as compared with other industry segments in 2015. As internet and digital banking services have become more common, the modern bank is now under an unprecedented spectrum of attacks which are copious in numbers and sophisticated in complexity. To build the required resilience against these cyber threats, there is a need for banks to formulate new and dynamic system designs that will provide a rapid response to such attacks.

1.2 In Hong Kong, the cyber security landscape has changed drastically over the last decade. Cyber threats in Hong Kong continue to rise in numbers: in 2015, the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") handled almost 5,000 cyber-attack incidents, representing a 43% increase in cyber-attacks year on year.[2] According to police statistics, financial losses due to cybercrime cases amounted to HK$1.8 billion in Hong Kong during 2015.[3]

[1] Ponemon Institute LLC (sponsored by Hewlett Packard Enterprise). "2015 Cost of Cyber Crime Study: Global". Publication date: October 2015. Retrieved on 27 July 2016 from https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

[2] Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT). "HKPC Warns of Growing Cyber Attacks that Harvest Credentials for Profit". HKCERT Press Centre. Publication date: 27 January 2016. Retrieved on 22 July, 2016 from https://www.hkcert.org/my_url/en/blog/16012701

[3] Questex Asia Ltd. "Cyber Security Summit launches at Science Park". Computer World Hong Kong Publication date: 17 May 2016; SCMP. "Hackers have their sights on Hong Kong, cyber security experts warn". Publication date: 14 May 2016. Retrieved on 27 July 2016 from http://www.scmp.com/news/hong-kong/economy/article/1944676/hackers-have-their-sights-hong-kong-cyber-security-experts

1.3 With respect to the banking sector in Hong Kong, the city is one of the most popular targets for banking malware attacks.[4] The Hong Kong Institute of Bankers ("HKIB") is quoted as stating that "the banking sector is 300% more likely to face cyber-attacks than any other sector".[5] In light of the heightened cyber risk in the banking sector, the Hong Kong banking industry recognises the vital importance of protecting banks and its customers from cyber-attacks, and in upholding Hong Kong's position as a leading international financial centre.

1.4 Against this backdrop, the Hong Kong Monetary Authority ("HKMA") has considered the necessity of placing cybersecurity at the forefront of its fintech agenda. In May 2016, the HKMA announced the Cybersecurity Fortification Initiative ("CFI") with the purpose of enhancing the resilience of Hong Kong banks to cyber-attacks under a three-pronged approach. CFI includes introducing a common risk-based assessment framework for Hong Kong banks, a professional training and certification programme that aims to increase the supply of qualified professionals, and a cyber-intelligence sharing platform.

1.5 In parallel with the CFI's professional training and development programme, the HKMA is now launching a module on cybersecurity under the Enhanced Competency Framework (ECF) for banking practitioners. The goal is to introduce an industry-wide competency framework for the banking sector that enables talent development, and facilitates the building of professional competencies and capabilities of those working in cybersecurity. In view of the evolving cybersecurity risks, it is imperative that banks should start enhancing their cybersecurity cultures by equipping staff with the right skills, the right knowledge and the right behaviour.

2. <u>Objectives</u>

2.1 The ECF on Cybersecurity (hereinafter referred to as "ECF-C") is a non-statutory framework which sets out the common core competences required of

[4] Kaspersky Lab. "Kaspersky Security Bulletin 2015", p.51. Retrieved on 22 July 2016 from https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf

[5] SCMP. "On the defence: Hong Kong Monetary Authority to boost cybersecurity for city's banking system". Publication date: 18 May 2016. Retrieve on 27 July 2016 from http://www.scmp.com/news/hong-kong/economy/article/1946686/defence-hong-kong-monetary-authority-boost-cybersecurity

cybersecurity practitioners in the Hong Kong banking industry. The objectives of the ECF-C are twofold:

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

(b) to raise and maintain the professional competence of cybersecurity practitioners in the banking industry.

2.2 Although the ECF-C is not a mandatory licensing regime, authorised institutions (“AIs”) are encouraged to adopt the ECF-C. This includes:

(a) to serve as a benchmark to determine the level of competence required and to assess the ongoing competence of individual employees;

(b) to support relevant employees to attend training programmes and examinations that meet the ECF-C benchmark;

(c) to support the continuing professional development of individual employees; and

(d) to specify the ECF-C as one of the criteria for recruitment purposes.

3. Scope of application

3.1 The ECF-C is aimed at persons (referred as ‘Relevant Practitioners’) engaged by AIs undertaking cybersecurity roles. Under the ECF-C, a ‘Relevant Practitioner’ is defined as:

“a new entrant or an existing practitioner engaged by an authorised institution to perform in roles ensuring operational cyber resilience”.

3.2 For avoidance of doubt, the following categories of staff are excluded from the definition of ‘Relevant Practitioners’:

(a) Those who are not required to perform the three key roles specified under the ECF-C (i.e. IT Security Operations and Delivery, IT Risk Management and Control, and IT Audit); and

(b) Those who performing key roles solely in the information technology operating function of an AI, such as system developers, system operators, helpdesk operators, and IT support.

3.3 AIs have the responsibility to ensure Relevant Practitioners performing duties in overseas branches and subsidiaries should be competent and have the capability as required under the ECF-C. However, we understand that the qualifications held by the staff outside Hong Kong may be different from the required qualifications set out in ECF-C. To allow flexibility to implement the ECF-C, AIs may exercise sound judgment on evaluating if those staff in overseas branches and subsidiaries possess equivalent qualifications that are:

(a) formally recognised by the list of certificates under ECF-C (see Section 5.1); and/or

(b) similar to the list of certificates under the ECF-C (see Section 5.1), in which the ‘similarity’ criterion should be determined based on the following three factors:

i. recognition of the qualification by the local industry;
ii. technical qualification of the certificates; and
iii. ethical requirement of the qualification.

4. <u>Qualification structure</u>

4.1 The qualification structure of the ECF-C comprises the following two levels based on the year of work experience of Relevant Practitioners in performing the tasks as specified in Annex 1:

(a) Core Level - This level is applicable for entry-level staff with less than 5 years of relevant work experience in the cybersecurity function.

(b) Professional Level - This level is applicable for staff with 5 and above years of relevant work experience in the cybersecurity function.

4.2 The qualification structure is driven by the key roles based upon the three lines of defence concept under cyber risk governance (hereinafter referred to as the “key roles”):

(i) first line of defence: IT Security Operations and Delivery

(ii) second line of defence: IT Risk Management and Control

(iii) third line of defence: IT Audit

Details of the roles and qualification requirements can be found in Annex 2.

4.3 Relevant Practitioners are considered as qualified under the ECF-C if they are in possession of one or more of the certificates listed under the ECF-C (refer to Section 5.1). Relevant process flow is illustrated in Annex 3.

4.4 It is quite common for some smaller banks to have employees assuming multiple job roles. In such a situation, if the staff concerned took charge of any cybersecurity roles in the three lines of defence, no matter in a part time or full time basis, he or she should be considered as a Relevant Practitioner.

5. Recognised certificates

Under the ECF-C, the list of recognised certificates is as follows:

	First Line of Defence	**Second Line of Defence**	**Third Line of Defence**
RECOGNISED CERTIFICATES	**IT Security Operations and Delivery**	**IT Risk Management and Control**	**IT Audit**
Core Level			
CSX Fundamentals Certificate	✓	✓	✓
CSX Practitioner Certificate (CSX-P)	✓	✓	✓
GIAC Information Security Professional (GIAC GISP)	✓	✓	
GIAC Security Essentials (GSEC)	✓	✓	✓
ISC^2 Systems Security Certified Practitioner (SSCP)	✓		

Professional Level			
CSX Specialist Certificate (CSX-S)	✓	✓	✓
CSX Expert Certificate (CSX-E)	✓	✓	✓
ISACA Certified Information Systems Auditor (CISA)	✓	✓	✓
ISACA Certified Information Security Manager (CISM)	✓	✓	✓
ISACA Certified in Risk and Information Systems Control (CRISC)		✓	
ISACA Certified in the Governance of Enterprise IT (CGEIT)		✓	
ISC² Certified Information Systems Security Professional (CISSP)	✓	✓	✓
ISC² Certified Cloud Security Professional (CCSP)	✓	✓	

6. Training programmes and examinations

6.1 Relevant Practitioners can meet the ECF-C certification requirements by obtaining the relevant qualifications.

7. Continuing Professional Development (CPD) requirements

7.1 The aim of the CPD arrangement is to ensure that Relevant Practitioners maintain their competency levels by updating their existing knowledge base and skill set, particularly in light of the constantly evolving cybersecurity regulatory environment and the fast-paced change in trends.

7.2 Relevant Practitioners who have successfully obtained the qualifications listed under Section 5.1 should fulfil the CPD requirement of the relevant certification scheme. 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.

8. Grandfathering

8.1 Grandfathering arrangements are not applicable under the ECF-C.

9. Maintenance of relevant records

9.1 As a matter of good practice, AIs are encouraged to maintain up-to-date records on relevant practitioners within the organisation who meet the Core / Professional Level of qualification as set out in this guide.

Annex 1 –Example of key tasks for roles under ECF-C

I) Core Level

Role 1: IT Security Operations and Delivery		
Core Level		
Key tasks	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 change 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.	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.

II) Professional Level

Role 1: IT Security Operations and Delivery		
Professional Level		
Key tasks	Operational Security Tasks 1. Define cybersecurity requirements as a subset of general information security requirements. 2. Implement cybersecurity control mechanisms which are consistent with the bank's risk strategy. 3. Implement general IT risk and control mechanism such as access controls, program change / development controls and IT operations controls. 4. Manage information systems security operations, including security operations performance. 5. Define appropriate framework for cybersecurity monitoring (including monitoring requirements, indicators, datasets, collection and analytical methods). 6. Analyse cybersecurity incidents and make recommendations on remediation actions. 7. Implement corrective action plans to address process and control deficiencies identified by the second and third line of defence.	Technical Tasks 1. Plan and design security architectures and implement different security solutions to safeguard the bank's network and systems. 2. Research security standards, security systems and authentication protocols. 3. Develop technical requirements and controls for network, system and data security. 4. Provide technical guidance to the systems and network team regarding security configurations. 5. Perform risk analyses on existing security infrastructure and implement security enhancements. 6. Implement systems and procedures to enable digital forensics capabilities.

I) Core Level

Role 2: IT Risk Management and Control	
Core Level	
Key tasks	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.

II) Professional Level

Role 2: IT Risk Management and Control	
Professional Level	
Key tasks	1. Design, develop and update IT risk management framework, policies and controls taking into consideration the bank's strategy, current/future regulatory requirements and emerging risk scenarios. Communicate IT risk management standards, policies and procedures to stakeholders of bank. 2. Assess the potential cybersecurity impact of emerging technologies and innovations, and include known risk and issues. 3. Identify control weaknesses in cybersecurity from a risk-based perspective. 4. Define monitoring requirements and indicators for measuring the higher level risk position. 5. Monitor, review and update IT risk profile and controls on a regular basis. 6. Ensure IT security/risk compliance within the AI.

I) Core Level

Role 3: IT Audit	
Core Level	
Key tasks	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.

II) Professional Level

Role 3: IT Audit	
Professional Level	
Key tasks	1. Plan audits to assess the controls, reliability and integrity of IT environment and systems. 2. Execute a risk-based audit strategy in compliance with auditing standards. 3. Perform inherent risk and maturity level assessments. 4. Assess the inherent risk and maturity assessment results and review improvement plans for identified gaps. 5. Communicate audit and assessment results and recommendations to stakeholders. 6. Evaluate IT plans, strategies, policies and procedures to ensure adequate management oversight. 7. Assess the adequacy and effectiveness of controls on an ongoing basis.

Annex 2 –Key roles, qualifications and CPD requirements under ECF – C Competency Framework

I) Core Level

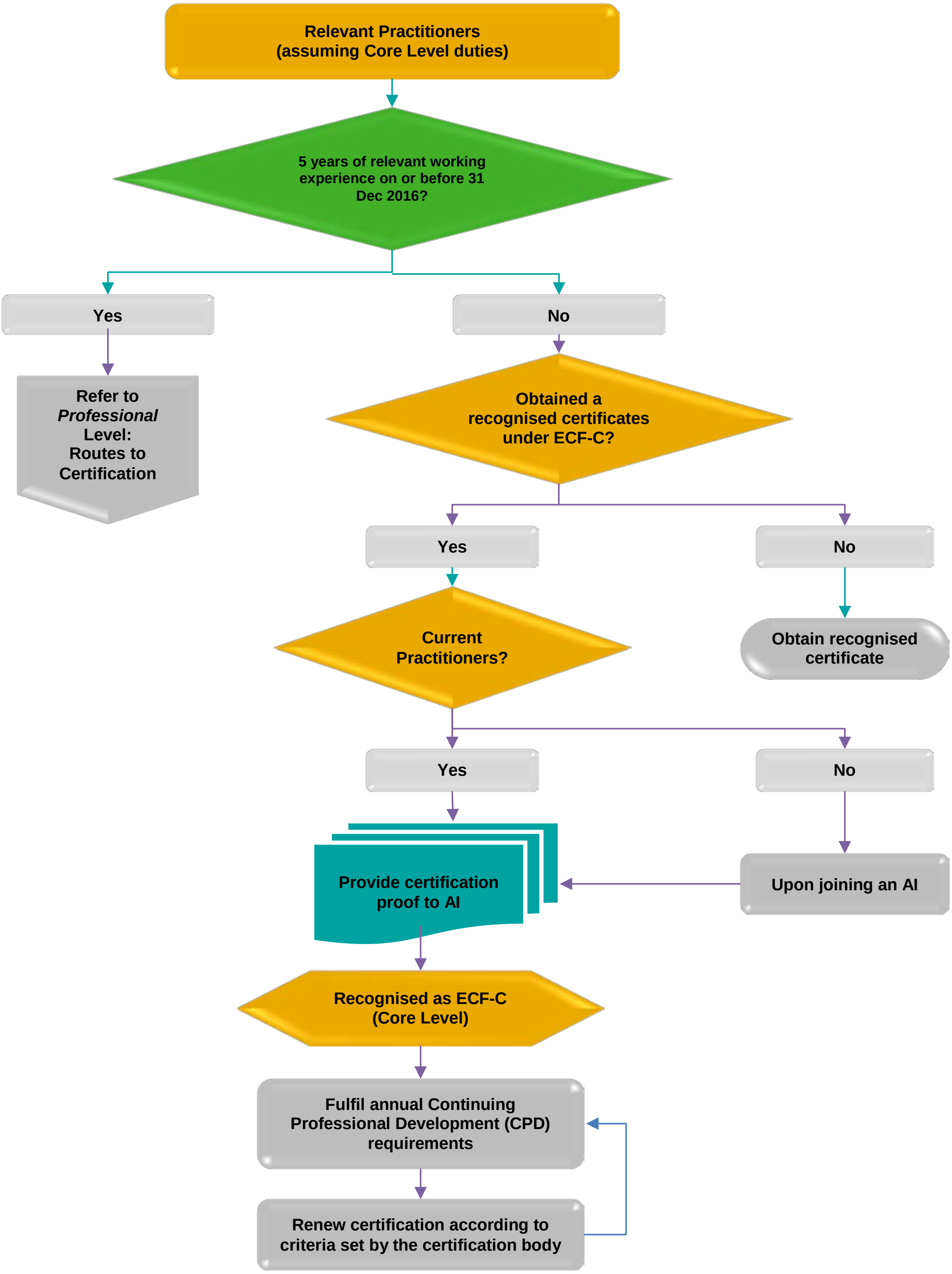
	Role 1	**Role 2**	**Role 3**
	IT Security Operations and Delivery	**IT Risk Management and Control**	**IT Audit**
	Core Level For entry-level staff with less than 5 years of relevant work experience in cybersecurity		
Role description	Apply daily administrative operational processes	Assist in development and communication of control processes	Conduct and document audits
Qualifications (certificates recognised)	• CSX Fundamentals Certificate • CSX Practitioner Certificate (CSX-P) • GIAC Information Security Professional (GIAC GISP) • GIAC Security Essentials (GSEC) • ISC² Systems Security Certified Practitioner (SSCP)	• CSX Fundamentals Certificate • CSX Practitioner Certificate (CSX-P) • GIAC Information Security Professional (GIAC GISP) • GIAC Security Essentials (GSEC)	• CSX Fundamentals Certificate • CSX Practitioner Certificate (CSX-P) • GIAC Security Essentials (GSEC)
CPD requirements	Minimum 20 CPD hours each year; and minimum 120 CPD hours over every 3 years period	Minimum 20 CPD hours each year; and minimum 120 CPD hours over every 3 years period	Minimum 20 CPD hours each year; and minimum 120 CPD hours over every 3 years period

II) Professional Level

	Role 1	Role 2	Role 3
	IT Security Operations and Delivery	**IT Risk Management and Control**	**IT Audit**
	Professional Level For staff with 5 and above years of relevant work experience in cybersecurity		
Role description	Manage information systems security operations	Manage IT risk management and control procedures and policies	Plan and execute audit and assessments
Qualifications (certificates recognised)	• CSX Specialist Certificate (CSX-S) • CSX Expert Certificate (CSX-E) • ISACA Certified Information Systems Auditor (CISA) • ISACA Certified Information Security Manager (CISM) • ISC² Certified Information Systems Security Professional (CISSP) • ISC² Certified Cloud Security Professional (CCSP)	• CSX Specialist Certificate (CSX-S) • CSX Expert Certificate (CSX-E) • ISACA Certified Information Systems Auditor (CISA) • ISACA Certified Information Security Manager (CISM) • ISACA Certified in Risk and Information Systems Control (CRISC) • ISACA Certified in the Governance of Enterprise IT (CGEIT) • ISC² Certified Information Systems Security Professional (CISSP) • ISC² Certified Cloud Security Professional (CCSP)	• CSX Specialist Certificate (CSX-S) • CSX Expert Certificate (CSX-E) • ISACA Certified Information Systems Auditor (CISA) • ISACA Certified Information Security Manager (CISM) • ISC² Certified Information Systems Security Professional (CISSP)
CPD requirements	Minimum 20 CPD hours each year; and minimum 120 CPD hours over every 3 years period	Minimum 20 CPD hours each year; and minimum 120 CPD hours over every 3 years period	Minimum 20 CPD hours each year; and minimum 120 CPD hours over every 3 years period

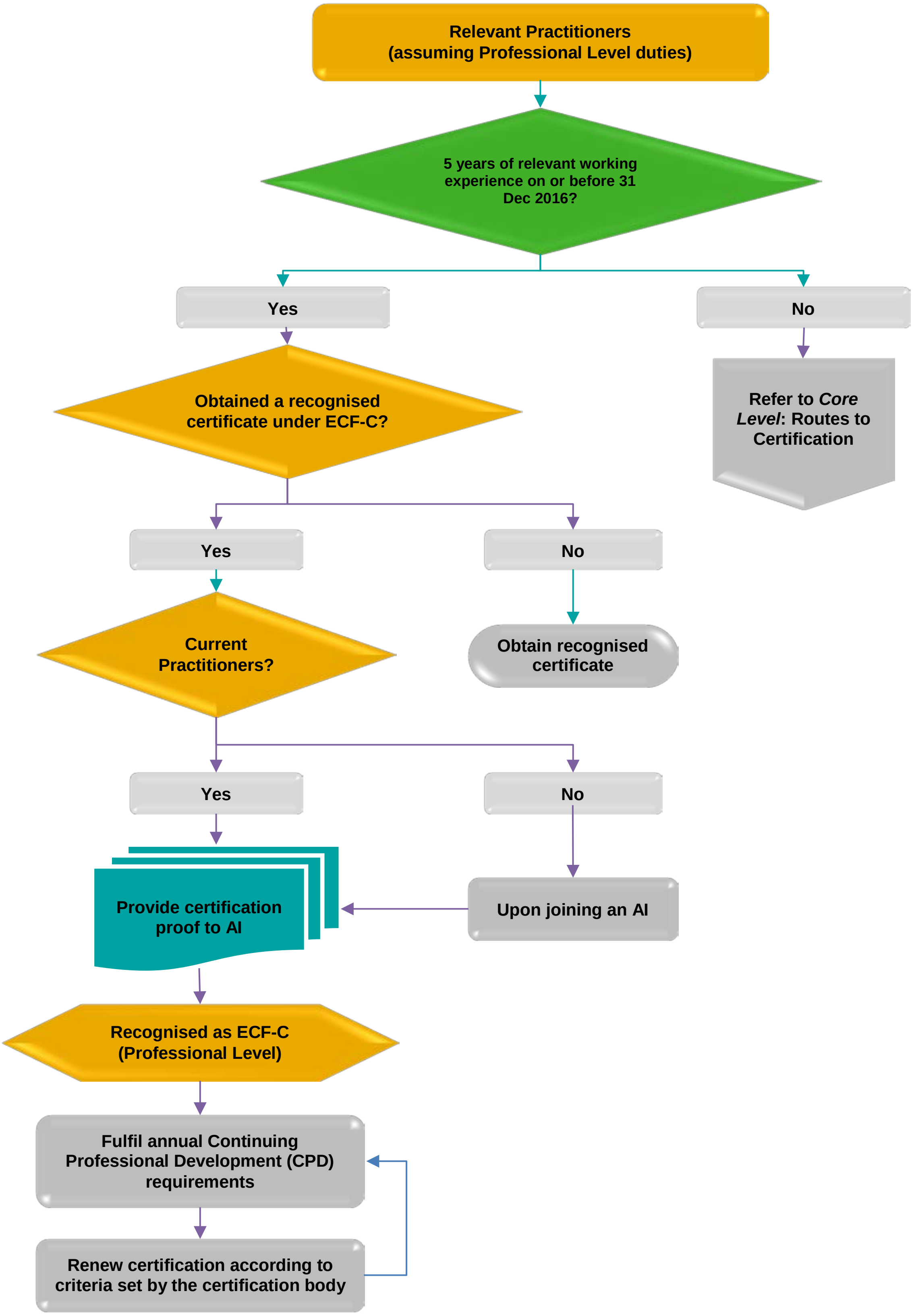
Annex 3 - Routes to certification

ECF on Cybersecurity Core Level:


Relevant Practitioners
(assuming Core Level duties)
5 years of relevant working experience on or before 31 Dec 2016?
Yes
No
Refer to *Professional* Level: Routes to Certification
Obtained a recognised certificates under ECF-C?
Yes
No
Current Practitioners?
Obtain recognised certificate
Yes
No
Provide certification proof to AI
Upon joining an AI
Recognised as ECF-C (Core Level)
Fulfil annual Continuing Professional Development (CPD) requirements
Renew certification according to criteria set by the certification body

*For Relevant Practitioners performing duties in overseas branches and subsidiaries, please refer to Section 3.3.

ECF on Cybersecurity Professional Level:


Relevant Practitioners
(assuming Professional Level duties)
5 years of relevant working experience on or before 31 Dec 2016?
Yes
No
Obtained a recognised certificate under ECF-C?
Refer to *Core Level*: Routes to Certification
Yes
No
Current Practitioners?
Obtain recognised certificate
Yes
No
Provide certification proof to AI
Upon joining an AI
Recognised as ECF-C (Professional Level)
Fulfil annual Continuing Professional Development (CPD) requirements
Renew certification according to criteria set by the certification body

*For Relevant Practitioners performing duties in overseas branches and subsidiaries, please refer to Section 3.3.