13 March 2020

Wilson Pang
Senior Manager, Fintech Facilitation Office
Hong Kong Monetary Authority

PwC CFI review team

ASIFMA Response to HKMA Soft Consultation on CFI2.0

Dear,

Thanks very much for giving us the opportunity to provide comments on certain sections of the draft revision of the HKMA Cybersecurity Fortification Initiative (CFI). On behalf of our members, we are pleased to provide in what follows our feedback on section 4 (and Appendix 3) and section 5 of the consultation paper covering cybersecurity qualifications and professional development programmes. We hope that we will have the opportunity to also review the other sections in due course and when they are ready for consultation, but in the meantime, we have also taken the liberty to share some thoughts on other sections of the CFI.

1) Chapter 4, consultation question *Q17. Do you have any comments on the recommended additions and revisions to the list of equivalent qualifications? Refer to the detailed recommendations in paragraph 4.2.2 as well as to the Mapping of CREST Certifications to Equivalent Qualifications in Appendix 3.*

- We suggest that the HKMA clarify that the possession of one of the listed equivalent qualifications will suffice to qualify for each role.
- In general, the list of certifications specified are considered relevant to the skills required to conduct the Inherent/Maturity Assessment and iCAST. However, there are professionals who have the required expertise and experience but do not possess the certifications listed. We feel that the list of certification can be taken as an recommendation / reference for the industry but it should not be a mandatory requirement as long as the firm have assessed their expertise and experience before conducting the assessments and simulation tests.
- It would also be good to understand whether HKMA has a view on whether these qualifications are sufficiently available in Hong Kong.
- For the iCAST Manager and iCAST Specialist, GPEN and GXPN, and OSCE and OSEE respectively are listed in conjunction, while it could be argued that only possessing GXPN or OSCE suffices as well. The rationale is that GPEN and GXPN have significant overlap, and the body of knowledge for OSCE and OSEE is roughly the same. The rationale for listing similar certifications in conjunction is unclear, and it raises the question whether other common combinations with the same body of knowledge (e.g. OSCP and GXPN) suffice. We suggest that the list is simplified to only list individual certifications, e.g. as follows (changes in red):

iCAST Role	**Equivalent Qualifications**
C-RAF Assessor	CISA, CISSP, CISM, CRISC, CSX-P, CISP-HK, CEH
iCAST Manager	CCASP-CSAM, GXPN, OSCE

iCAST Specialist	CCASP-CSAS, GXPN, OSCE, OSCP, eCPTX, eWPTX, CRTE

- We also suggest that the list of Equivalent Qualifications for the iCAST Threat Intelligence Specialist is expanded with the following well-recognised threat intelligence certifications:
    - EC-Council Certified Threat Intelligence Analyst Qualification (CTIA) (https://www.eccouncil.org/programs/certified-threat-intelligence-analyst-ctia/);
    - Treadstone 71 Certified Cyber Intelligence Professional (https://www.treadstone71.com/cyber-intelligence-training/23-training/313-intelligence-roadmap)

2) Chapter 4, consultation question *Q18. Do you have any comments on the recommended frequency for reviewing and updating the list of equivalent qualifications? Refer to the detailed recommendations in paragraph 4.2.3.*

-Members agree that three years is a good frequency but given that developments are happening at a fast pace, we would recommend changing the frequency to a minimum of three years, which would allow an earlier reassessment as needed or appropriate.

3) Chapter 4, consultation question *Q19. Do you agree with the HKMA's view that there are sufficient channels for cybersecurity professionals to develop their technical skills to a level enabling them to obtain the relevant certifications or equivalent qualifications? Refer to the detailed recommendations in paragraphs 4.3.1, 4.3.2, and 4.3.3.*

- Having competent people in cybersecurity roles is crucial, but obtaining certification is only one of the channels to evaluate ongoing competencies and qualification to undertake the relevant roles & responsibilities. There are a range of other activities, including recruitment strategy, internal training, knowledge sharing, external training and events, etc., which can provide continuous talent nurturing.
- We would like to highlight that there are insufficient channels to attain the OSEE certification. This certification is only offered as part of classroom training at Black Hat USA in Las Vegas, NV (once a year with very limited seats; it is always immediately sold out), or alternatively via Offensive Security In-House Training, which in our members' experience requires a minimum of 15 participants at a significant expense when logistic are included. See the Offensive Security website as well: https://www.offensive-security.com/awe-osee/. We therefore suggest to withdraw OSEE from the list of Equivalent Qualifications, based on the insight that there are insufficient channels to attain this certification.
- iCAST manager certificates are extremely difficult and costly to obtain for internal staff. In fact, we understand that there is only one training and certification agent in Hong Kong and the cost of the training is high. For that reason, we would also challenge the statement that *"there are sufficient channels for cybersecurity professionals".* Many AIs therefore use external suppliers outside of Hong Kong. We recommend the HKMA to develop that talent pool locally. For example, we recommend that more can be done in schools and universities to build the pipeline, and to guide students in these fields (e.g. mentor/menteeship programs). Another suggestion would be to incorporate some of the subjects of the qualifications in certain university courses so that students can get certain exemptions from some of the qualifications.

4) Chapter 4, consultation question *Q20. Do you have any comments on the three-year review exercise to evaluate the local talent stockpile and identify supplementary initiatives to reduce the local cybersecurity talent gap? Refer to the detailed recommendation in paragraph 4.4.1.*

- We find it difficult to comment on the proposed three-year review exercise to evaluate the local talent stockpile and identify supplementary initiatives to reduce the local cybersecurity talent gap, as no details have been provided with respect to the intended approach or implementation. We recognize the need to evaluate the local talent stockpile and identify supplementary initiatives to reduce the local cybersecurity talent gap. However, we would suggest that HKMA clarifies the intended approach to conduct this periodic exercise.
- We also recommend that any initiatives to build the local cybersecurity talent pool should be a continuous, year-round approach to employee development that is based on regular check-ins, real-time feedback and coaching.
- We suggest that regulators and/or industry bodies in HK assess whether inspiration can be drawn from Singapore's IMDA Talent Programmes (https://www.imda.gov.sg/imtalent/programmes), specifically CITREP+ (https://www.imda.gov.sg/imtalent/programmes/citrep-plus), and local grant schemes such as Singapore's Cybersecurity Capability Grant (https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Fact-Sheet-on-FSTI-CCG.pdf?la=en&hash=A8972BEDA02FCD535151B960D72058CF5E63F7FC)

5) Chapter 5: Qualification requirements:

- Under iCAST Specialist in section 5.2.3 we would welcome clarification on whether it should be attack vectors or objectives.

6) Timeline

Considering the fact that the first batch of AIs completed the C-RAF 1.0 assessment between September 2017 to June 2018 and given the current Covid-19 situation, we suggest the HKMA considers a grace period to implement and complete CRAF v2.0 assessment if it will be finalized by 1Q2020. For example, under a three-year cycle, the first batch of AIs will need to complete the C-RAF assessment as early as Q4 2020 which is a challenging timeline for AIs to meet.

8) International equivalence

As discussed during our August 2019 meeting, would like to stress the need for international policy harmonisation and reiterate our suggestions around international equivalence. Currently there is overlap for firms where they need to comply with different assessments in different jurisdictions. We would like the HKMA to consider a substituted compliance/deference regime for firms so that they do not need to repeat overlapping assessments in different locations. For CRAF specifically, there should be consideration on the applicability of the C-RAF maturity assessment if the AI demonstrates that it is conducting similar security assessments according to industry standards – e.g. NIST, FFIEC, etc. Many of the C-RAF controls overlap with other industry standards, which adds duplication of work for many of the AIs. The majority of the cyber controls are operated globally, and such controls have been evaluated and even assessed by independent party.

Specifically, we recommend that the Financial Sector Profile (FSP) as one of the frameworks financial institutions could leverage. Overall, we also encourage HKMA to consider referencing the FSP in addition to NIST Cybersecurity Framework as the FSP is based off of NIST Cybersecurity Framework (NIST CSF) and tailors the controls specifically to the Financial Sector. As IOSCO pointed out in its June 2019 Cyber Task Force Report, the Profile "is a customization of the NIST Cybersecurity Framework that financial institutions can use for internal and external cyber risk management assessment and as evidence for compliance, encompassing relations between Cyber frameworks, including Core Standards. Further, the tool encompasses all three of the Core Standards of this report, as well as others."

In the U.S. the Federal Financial Institutions Examination Council (FFIEC), constituting the Federal Reserve Service (FRB), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and others, also issued a public statement emphasizing the benefits of using a standardized approach to assess and improve cybersecurity preparedness, and cited the Cybersecurity Assessment Tool (CAT), the NIST CSF, and the Financial Sector Profile as such frameworks.

Other statements of Regulatory Support of the FSP include :

- **Federal Reserve Board:** "… we'll welcome any financial institution to provide information to us using the structure and taxonomy of the Profile, we see that as a boon for harmonization."
- **SEC:** "…to the extent that we can rationalize and cut down on that duplication, allowing those scarce resources to start driving toward protecting the enterprise, I think we're in a good space."
- **OCC:** "If the industry moves to use this cybersecurity profile, that is what we will base our assessments on….".

We hope you find the above feedback helpful and we would be happy to address any questions you might have. Please contact Laurence Van der Loo on lvanderloo@asifma.org. We also very much look forward to the opportunity to comment on the other sections of the consultation paper.

Yours sincerely,

Mark Austen
Chief Executive Officer,
Asia Securities Industry & Financial Markets Association