HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

21 December 2016

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Cybersecurity Fortification Initiative

I am writing to inform you of the implementation details of the Cybersecurity Fortification Initiative (CFI) undertaken by the Hong Kong Monetary Authority (HKMA) in collaboration with the banking industry.

The CFI, announced by the HKMA in May 2016, consists of three pillars, namely (i) the Cyber Resilience Assessment Framework (C-RAF); (ii) the Professional Development Programme (PDP); and (iii) the Cyber Intelligence Sharing Platform (CISP).

The C-RAF is an assessment tool to help AIs evaluate their cyber resilience. The assessment comprises three stages:

(i) Inherent Risk Assessment – This facilitates an AI to assess its level of inherent cybersecurity risk and categorize it into "low", "medium" or "high" in accordance with the outcome of the assessment;

(ii) Maturity Assessment – This assists an AI in determining whether the actual level of its cyber resilience is commensurate with that of its inherent risk. Where material gaps are identified, the AI is expected to formulate a plan to enhance its maturity level; and

(iii) Intelligence-led Cyber Attack Simulation Testing (iCAST) – This is a test of the AI's cyber resilience by simulating real-life cyber attacks from adversaries, making use of relevant cyber intelligence. AIs with an inherent risk level assessed to be "medium" or "high" are expected to conduct the iCAST within a reasonable time.

The HKMA has taken on board many of the industry's comments received during the consultation in finalising the C-RAF. In terms of the implementation timeline, the industry has raised a practical issue concerning the availability of qualified assessors to undertake the assessment. Taking this concern into account and having regard to overseas experience, the HKMA will adopt a phased approach to implementation as follows:

(i) The first phase will cover around 30 AIs including all major retail banks, selected global banks and a few smaller AIs. The HKMA will inform these AIs individually;

(ii) The expected timeline for completing the C-RAF assessment under the first phase is:

- Inherent Risk Assessment and Maturity Assessment — End-September 2017
- iCAST (if applicable) — End-June 2018

(iii) Depending on industry feedback and the experience gathered from the first phase, the second phase will cover all the remaining AIs. They will be expected to complete the Inherent Risk Assessment and the Maturity Assessment by the end of 2018. The HKMA will take into account the assessment results of the second phase in determining a timeframe for the remaining AIs to complete the iCAST. Although AIs covered in the second phase are given a longer timeframe for implementation, they should familiarise themselves with the C-RAF and take steps to strengthen their cyber resilience at an early stage where necessary.

The PDP seeks to provide a local certification scheme and training programme for cybersecurity professionals. It was rolled out earlier this month. At the request of the industry, the HKMA has adopted a list of professional qualifications recommended by an expert panel comprising representatives from major IT professional associations, banks and universities. These professional qualifications are considered to be equivalent to the certification provided under the PDP. A person holding a PDP certification or an equivalent professional qualification may perform the assessments and tests in relation to the different roles defined under the C-RAF as set out in the **Annex**.

Finally, we are also pleased to report that the CISP, the third pillar of the CFI, is ready for access by banks this month.

Should you have any questions regarding the implementation schedule of the C-RAF, please feel free to contact Ms Teresa Chu on 2878-1563 or Mr Ivan Shek on 2878-8755. For other questions relating to the CFI, please contact Mr Josiah Lam at 2878-1425 or Mr. Wilson Pang at 2878-1249 of the Fintech Facilitation Office (FFO).

Yours faithfully,

Sunny Yung
Acting Executive Director (Banking Supervision)

Encl.

Annex

List of equivalent qualifications

1. C-RAF Assessor

- ISACA's *Certified Information Systems Auditor (CISA)*;
- (ISC)^2's *Certified Information Systems Security Professional (CISSP)*;
- ISACA's *Certified Information Security Manager (CISM)*;
- ISACA's *Certified in Risk and Information Systems Control (CRISC)*;
- ISACA's *Cybersecurity Fundamentals Certificate (CSX-F)* and *Cybersecurity Nexus Practitioner certification (CSX-P)*; or
- China Information Technology Security Evaluation Centre's *Certified Information Security Professional - Hong Kong (CISP - HK).*

2. iCAST Manager

- HKIB's *CCASP – Certified Simulated Attack Manager*[**];
- *CREST Certified Simulated Attack Manager*;
- *GIAC Penetration Tester (GPEN)* and *GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)*; or
- *Offensive Security Certified Expert (OSCE)* and *Offensive Security Exploitation Expert (OSEE).*

3. iCAST Specialist

- HKIB's *CCASP – Certified Simulated Attack Specialist*[**];
- *CREST Certified Simulated Attack Specialist*;
- *GIAC Penetration Tester (GPEN)* and *GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)*; or
- *Offensive Security Certified Expert (OSCE)* and *Offensive Security Exploitation Expert (OSEE).*

4. iCAST Tester

a. for professional who performs IT infrastructure testing

- HKIB's *CCASP – Certified Infrastructure Tester*[**];
- *CREST Certified Infrastructure Tester*;
- *GIAC Penetration Tester (GPEN)*; or
- *Offensive Security Certified Expert (OSCE).*

b. for professional who performs web application testing

- HKIB's *CCASP – Certified Web Applications Tester*[**];
- *CREST Certified Web Applications Tester*;
- *GIAC Web Application Penetration Tester (GWAPT)*; or
- *Offensive Security Web Expert (OSWE).*

[**] Certified Cyber Attack Simulation Professional (CCASP) is the new certification programme of Hong Kong Institute of Bankers (HKIB) provided under the PDP, which is supported by the Council of Registered Ethical Security Testers (CREST) International.