Annex

Cybersecurity Fortification Initiative 2.0

The HKMA has conducted a holistic review of the Cybersecurity Fortification Initiative (CFI) taking into account i) the experience gained in the past few years; ii) feedback of authorized institutions (AIs) obtained via an industry survey and interviews with selected institutions; and iii) overseas developments and new practices. The HKMA then issued a consultation paper in January 2020 putting forward a set of recommendations to enhance the three pillars of the CFI. Two workshops were conducted with members of the Hong Kong Association of Banks (HKAB), one in March and another in June, to discuss the industry feedback received during the consultation.

A revised CFI, or CFI 2.0, is subsequently developed, having regard to the findings of the review. The revised framework aims to simplify the assessment process while maintaining effective control standards that are commensurate with latest technology trends. Substantial efforts will be made to expand the talent supply and encourage cyber threat intelligence sharing across the industry. Details of the major enhancements are set out below.

C-RAF 2.0 – Risk assessment

- Introduction of new and enhanced control principles reflecting recent international sound practices in cyber incident response and recovery, as well as latest technology trends (e.g. cloud technology and virtualisation security);
- Introduction of Blue team requirements for iCAST to measure the effectiveness of detection, response and recovery functions of AIs;
- Allowing more flexibility for AIs to leverage the results of similar cyber resilience assessments performed by their banking groups or headquarters;

PDP –Talent Development

- Updating and expanding the list of acceptable cyber professional qualifications for conducting C-RAF assessments, including new iCAST threat intelligence qualifications (see below Table); and

CISP – Information Sharing

- Recommending the development of a target operating model to improve the user-friendliness of CISP by outlining the governance, roles and responsibilities of users;
- Expanding the CISP membership to on-board members of the DTC Association and other financial sectors.

List of equivalent qualifications

iCAST Role	CREST Certification	Equivalent Qualifications
C-RAF Assessor	N/A	• 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) • China Information Technology Security Evaluation Centre's Certified Information Security Professional – Hong Kong (CISP-HK) • EC-Council's Certified Ethical Hacker (CEH) *
iCAST Manager	CREST Certified Simulated Attack Manager (CCSAM)	• HKIB's CCASP – Certified Simulated Attack Manager • GIAC Penetration Tester (GPEN) and GIAC Exploit Research and Advanced Penetration Tester (GXPN) • Offensive Security Certified Expert (OSCE) and Offensive Security Exploitation Expert (OSEE)
iCAST Threat Intelligence Specialist	CREST Certified Threat Intelligence Manager (CCTIM) * CREST Registered Threat Intelligence Analyst (CRTIA) *	• HKIB's CCASP – Certified Simulated Attack Manager • GIAC Penetration Tester (GPEN) • GIAC Exploit Research and Advanced Penetration Tester (GXPN) • OSCE • OSEE • GIAC Cyber Threat Intelligence (GCTI) * • McAfee Institute's Certified Cyber Intelligence Professional (CCIP) *
iCAST Specialist	CREST Certified Simulated Attack Specialist (CCSAS)	• HKIB's CCASP – Certified Simulated Attack Specialist • GPEN and GXPN • OSCE and OSEE • eLearnSecurity Certified Penetration Tester eXtreme (eCPTX) * • eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) * • PentesterAcademy's Certified Red Teaming Expert (CRTE) *
iCAST Tester (IT infrastructure testing)	CREST Certified Infrastructure Tester (CCT Infra)	• HKIB's CCASP – Certified Infrastructure Tester • GPEN • OSCE • OSCP * • eLearnSecurity Certified Professional Penetration Tester (eCPPT) * • eLearnSecurity Web Application Penetration Tester (eWPT) * • PentesterAcademy's Certified Red Teaming Professional (CRTP) * • ISACA's CSX Penetration Testing Overview (CPTO) Certificate *

iCAST Role	CREST Certification	Equivalent Qualifications
iCAST Tester (web application testing)	CREST Certified Web Applications Tester (CCT Web App)	• HKIB's CCASP – Certified Web Applications Tester • GIAC Web Application Penetration Tester (GWAPT) • Offensive Security Web Expert (OSWE) • OSCP * • eLearnSecurity Certified Professional Penetration Tester (eCPPT) * • eLearnSecurity Web Application Penetration Tester (eWPT) * • PentesterAcademy's Certified Red Teaming Professional (CRTP) * • ISACA's CPTO Certificate *

_____

Additions to the equivalent qualifications are marked with an asterisk (*).