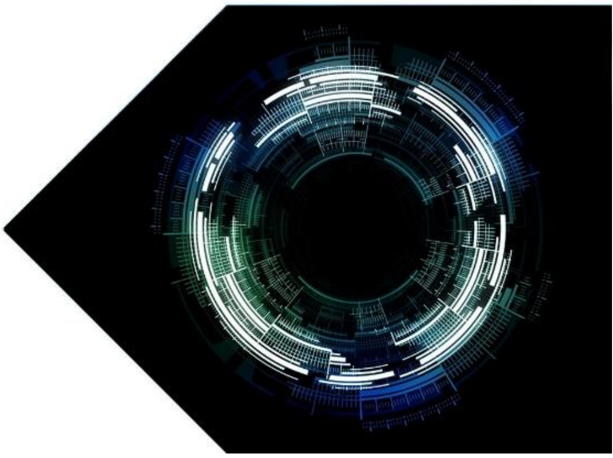
Governance, Risk & Internal Audit

CYBERSECURITY FORTIFICATION INITIATIVE 2.0



In December 2016, Cybersecurity Fortification Initiative (CFI) had been introduced by the Hong Kong Monetary Authority (HKMA) for the enhancement of cyber resilience of Hong Kong's banking systems. While the initiative made great progress in past years, HKMA announced the implementation of CFI 2.0 after receiving feedbacks from the industries and expertise.

The CFI 2.0 has come into effect on 1 January 2021. The three pillars (i) the Cyber Resilience Assessment Framework (C-RAF); (ii) the Professional Development Programme (PDP); and (iii) the Cyber Intelligence Sharing Platform (CISP) were enhanced to cater to latest technology.

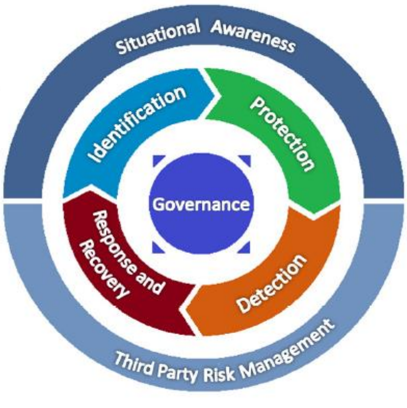
Three pillars of the CFI programme

Cyber Resilience Assessment Framework (C-RAF)

C-RAF is a common risk-based framework for Authorised Institutions (AIs) to assess their own risk profiles and determine the level of defense and resilience required. The assessment comprises 3 stages:

Inherent Risk Assessment – An AI is required to assess its level of inherent cybersecurity risk and categorise it into "low", medium" or "high" in accordance with the outcome of the assessment. A typical inherent risk profile comprises the following categories taking into account various business and operational aspects of the AI:

- Technologies and Connection Types
- Delivery Channels
- Products and Technology Services
- Organisational Characteristics
- Tracked Records of Cyber Threats



7 domains of the maturity assessment

Maturity Assessment – AI then determines the maturity level within each of the seven domains and assesses 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.

New changes
The CFI 2.0 introduced the latest 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).

In order to simplify the assessment process, the new programme allows more flexibility for AIs to leverage the results of similar cyber resilience assessments performed by their banking groups or headquarters.

Intelligence-led Cyber Attack Simulation Testing (iCAST) – 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.

New changes
There is a new requirement related to establishing both red and blue team exercises to provide a holistic security solutions ensuring strong defences while keeping in view of evolving threats. Red teams simulate attacks against blue teams to test the effectiveness of the network's security. In CFI 2.0, new Blue team requirements will come effective to measure the effectiveness of detection, response and recovery functions of AIs. Red team is no longer the only required entity for the simulated attacks. Blue team is encouraged to coordinate with Red team for the more advanced cyber resilience.

Professional Development Programme (PDP)

Local certification scheme and training programme – It aims to train and nurture cybersecurity practitioners to increase the supply of qualified professionals in Hong Kong.

New changes
In the revised CFI, HKMA updates and expands the list of acceptable cyber professional qualifications for conducting C-RAF assessments, including new iCAST threat intelligence qualifications.

Notably, EC-Council's Certified Ethical Hacker (CEH) will become the equivalent qualifications for C-RAF Assessor. Offensive Security Certified Professional (OSCP) Certification will be added for the iCAST Penetration testers.

Cyber Intelligence Sharing Platform (CISP)

An industry wide computer platform – sharing of cyber intelligence, alerts and solutions among banks in order to enhance collaboration and uplift cyber resilience.

New changes
Regarding CFI 2.0, it recommends the development of a target operating model to improve the user-friendliness of CISP by outlining the governance, roles and responsibilities of users.

It also expands the CISP membership to on-board members of the DTC Association and other financial sectors.

Implementation schedule/timeline

The revised scheme (CFI 2.0) has become effective on 1 January 2021. The HKMA will maintain the phased approach to the implementation of C-RAF 2.0 for three divided groups. Group 1 includes all major retail banks, selected foreign bank branches and new AIs which have never conducted the C-RAF assessments. Depending on the size, scale and risk profile, the rest will be covered in Group 2 or 3.

C-RAF assessment stages	Group 1	Group 2	Group 3
Inherent Risk Assessment	End-September 2021	End-June 2022	End-March 2023
Maturity Assessment	End-September 2021	End-June 2022	End-March 2023
iCAST (applicable to AIs with inherent risk level assessed to be "medium" or "high")	End-June 2022	End-March 2023	End-December 2023

What are the changes on the seven domains of C-RAF

Domain	Key changes
Governance	For the governance and coordination of enterprise cybersecurity, new requirements for key cybersecurity management roles have been defined.
Identification	With respect to Risk Management, covering the identification, assessment, treatment, monitoring and reporting, new requirements for a structured Cyber Risk Management Framework have been defined.
Protection	New requirements have been enhanced or established for the security controls of the following areas: • Physical and mobile access; • Virtualisation and Internet of Things (IoT); • Software Development Life Cycle (SDLC); • Application Programming interfaces (APIs) testing; and • VPN and Cloud platform.
Detection	Regarding detection controls, requirements have been reviewed, including: • Endpoint behavioural detection; and • Security audit log retention.
Response and Recovery	In response to cyber security incident, the following areas have been clarified and established: • Stakeholders' accountability and responsibility; • Identification of third-party response and recover experts; and • Continuous improvement processes.

Domain	Key changes
Situational Awareness	The effectiveness of threat intelligence sharing has been enhanced.
Third Party Risk Management	Enhancement of security controls regarding due diligence, security assessments and audit activities of the service providers.

How we can help

We have a highly experienced, global team to address your needs. We have expertise and strong security skills in threat and vulnerability management, cybercrime prevention, response and recovery, strategy and security design and implementation services. Our penetration testing capabilities help our clients to identify their information security risks, understand their impact on the business, and mitigate critical security risks before they lead to financial or reputation loss.

Inherent Risk Assessment	Maturity Assessment	Gap Analysis	iCAST support
• Determine cyber risk exposures based on a number of factors including technologies, delivery channels, products and technology services, organisational characteristics, tracked records of cyber threats. • Determine the required maturity levels based on the inherent risk rating (i.e. high, medium or low)	• Determine the actual maturity level via the revised controls in the seven domains (i.e. governance, identification, protection, detection, response and recovery, situational awareness, third-party risk management).	• Perform gap analysis between the actual and required maturity level. • Formulate plans to enhance cyber resilience and strengthen the maturity.	• For those inherent risk ratings ranked as “high” or “medium”, assist to conduct iCAST in both Red and Blue team’s perspective, and perform real-life cyber attacks simulation to assess the resilience against cyber threats.

Why Moore

- Our team includes professionals with substantial knowledge and extensive experience in cybersecurity, technology and operations, security and controls. This enables us to provide practical and tailored solutions to the wide range of challenges facing by AIs today.
- We have expertise in the risk assessment, methodology and management. We also have developed a mature cybersecurity review methodology and approach which addresses the regulator’s expectations and concerns. We are committed to providing relevant and valuable insights and opportunities based on our professionalism, accomplishment and networks inside and outside the business.

Patrick A. Rozario
Advisory Services Managing Director
T +852 2738 7769
E patrickrozario@moore.hk

Hermes Liang
Advisory Services Director
T +852 2738 7742
E hermesliang@moore.hk

We believe the information contained herein to be correct at the time of going to press, but we cannot accept any responsibility for any loss occasioned to any person as a result of action or refraining from action as a result of any item herein. Printed and published by © Moore Hong Kong, a member of Moore Global Network Limited, a worldwide network of independent firms. © 2021 Moore