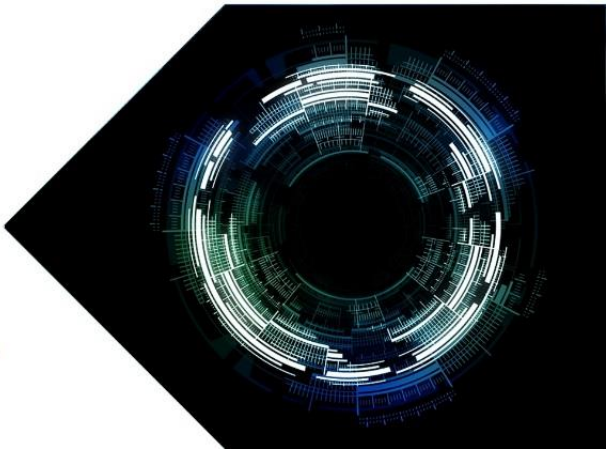
MOORE

Governance, Risk & Internal Audit

IMPLEMENTATION OF HKMA CYBERSECURITY FORTIFICATION INITIATIVE



In December 2016, the Hong Kong Monetary Authority (HKMA) announced the implementation details of the Cybersecurity Fortification Initiative (CFI) which aims to further enhance the cyber resilience of the banking sector in Hong Kong. The CFI programme consists of three pillars: the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Programme (PDP), and the Cyber Intelligence Sharing Platform (CISP).

Three pillars of the CFI programme

Cyber Resilience Assessment Framework (C-RAF)

C-RAF is a common risk-based framework for 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

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.

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.

7 domains of the maturity assessment

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.

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.

Implementation timeline

Considering the availability of qualified assessors and overseas experience, the HKMA had adopted a phased approach to implement the C-RAF assessments. Around 30 AIs including all major retail banks, selected global banks and a few smaller AIs were selected for the first phase to complete the C-RAF assessment.

C-RAF assessment stages	First phase (targeted 30 AIs)	Second phase (remaining AIs)
Inherent Risk Assessment	By September 2017	By December 2018
Maturity Assessment	By September 2017	By December 2018
iCAST	By June 2018	To be determined by the HKMA based on the assessment results

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 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 and perform real-life cyber attacks simulation to assess the resilience against cyber threats.

Why work with us

- Our team includes professionals with substantial knowledge and 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 developed a mature cybersecurity review methodology and approach which addresses the regulator’s expectations and concerns.

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

MOORE

www.moore.hk