Cybersecurity Fortification Initiative (CFI)

A framework initiated by the HKMA to strengthen cybersecurity

Hong Kong's cybersecurity framework

In light of increasing cyber threats, regulators across the globe are focusing their efforts on improving the cybersecurity of banking systems. The Hong Kong Monetary Authority (HKMA) announced the launch of the 'Cybersecurity Fortification Initiative' (CFI), a new scheme designed to enhance the resilience of Hong Kong banks to cyber attacks. The CFI consists of three pillars:

1. Cyber Resilience Assessment Framework – a risk-based approach for banks to assess and benchmark resilience against cyber attacks,
2. Cyber Intelligence Sharing Platform – a platform for banks to share intelligence and to collaborate on cyber attacks,
3. Professional Development Programme – a training programme designed to increase the number of qualified cybersecurity professionals.

The HKMA's Cybersecurity Fortification Initiative

- **Cyber Intelligence Sharing Platform**
- **Cyber Resilience Assessment Framework (C-RAF)**
- **Professional Development Programme**

Knowledge sharing to support cyber risk assessment

Certified professionals to conduct assessments for resilience

Cyber Resilience Assessment Framework

- Establish a common risk-based framework for banks to assess their own risk profiles and determine the level of defense and resilience required.
- Banks under the first phase of implementation should have completed both the Inherent Risk Assessment and the Maturity Assessment by the end of September 2017 while the remaining banks are expected to complete the assessments by the end of 2018.

Inherent Risk Assessment	Maturity Assessment	Improvement Plan
• Identify the risk exposure level across five areas (technology, delivery channels, product and technology services, organisational characteristics and track records on cyber threats) • Determine the required maturity levels	• Assess the maturity levels across seven key areas (governance, identification, protection, detection, response and recovery, situational awareness and third party risk management) • Determine the current maturity levels	• Perform gap analysis (required level vs current level) • Identify areas for improvement and increase the maturity level

Intelligence-led attack simulation testing (iCAST)

- This is a test of the Bank's cyber resilience by simulating real-life cyber attacks from adversaries, making use of relevant cyber intelligence. Banks with an inherent risk level assessed to be "medium" or "high" are expected to conduct the iCAST within a reasonable time.

Cyber Intelligence Sharing Platform

- Establish a secure platform to facilitate sharing of cyber threat intelligence among banks in order to enhance collaboration and improve the industry's resilience to cyber attacks
- Allow banks to make use of intelligence information in order to strengthen cyber resilience and take timely action against any attacks

Professional Development Programme

- Increase the number of qualified cybersecurity professionals capable of carrying out effective cyber risk assessment and cyber-related security testing
- Establish a new certification scheme for individuals and service providers that are responsible for testing cyber systems and providing intelligence updates

Common challenges in the banking industry

Some of the common challenges faced by Banks in complying with C-RAF requirements are:

Governance	• Lack of formal cyber risk appetite statement, cybersecurity programme and strategy • Insufficient updates and reporting on cybersecurity risks to management • Staff with cybersecurity responsibilities do not have the requisite qualifications to conduct the necessary tasks of the position
Identification	• An inventory of the IT assets (including hardware, software, data, and systems hosted internally and externally) is not maintained and updated
Protection	• Lack of comprehensive patch management programme (e.g. including patch criticality classification, covering non-Windows operating systems, etc.) • Insufficient hardening standards for operating systems and network devices • Lack of formal process on escalation of high-risk issues to senior management
Detection	• Incomplete system and application coverage of log monitoring and analysis across the environment • Lack of monitoring and detection of unauthorised software
Response and recovery	• Lack of policies and processes on controls for digital forensics • Security investigations, forensic analysis and remediation are not performed by qualified staff or third parties • Lack of communication plan for cyber incidents
Situational awareness	• Lack of threat and vulnerability information sharing process
Third party risk management	• Lack of process to maintain and update the list of third parties, that are network-connected, and process, store or transmit Bank's sensitive or critical data • Cybersecurity assessments of third parties are not in place, regularly updated and reviewed

How KPMG can help

C-RAF based assessment	Formulation of improvement roadmap	Boardroom strategy workshop	Threat intelligence framework	Training programme management
• Assist in determining the inherent risk and provide risk ratings. • Assess current maturity levels and perform gap analysis against what is required. • Perform iCAST.	• Assist in developing an improvement plan and provide a roadmap, taking business priorities into consideration. • Provide assistance in overall project management during the implementation of the roadmap.	• Boardroom awareness training to improve awareness and understanding of key risks. • Assist in establishing a governance structure and process on management oversight.	• Establish a threat intelligence framework covering the analysis process, incident response, intelligence sharing approach, system integration approach and the roles and responsibilities across business units.	• Assist in developing a training programme for management in order to continuously track and monitor staff development. • Assist in developing a programme to raise awareness of cyber risks

Contact us

Henry Shek
Partner, IT Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Brian Cheung
Associate Director,
IT Advisory
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

kpmg.com/cn