KPMG

Cybersecurity Fortification Initiative (CFI)

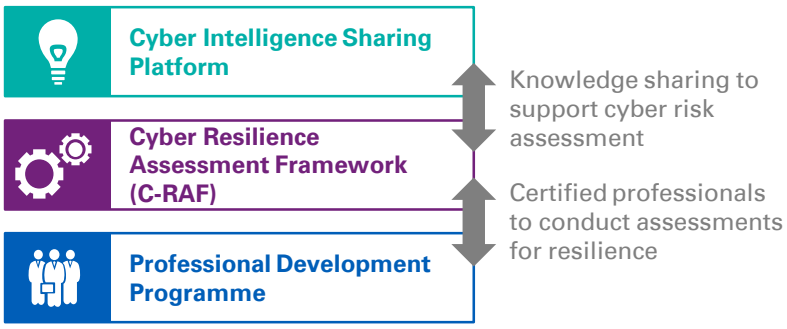
A new framework initiated by the HKMA to strengthen cybersecurity

Hong Kong's new 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) recently 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 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.

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

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

How to prepare yourself

As the Cyber Resilience Assessment Framework (C-RAF) is under consultation for a period of three months, banks can use this opportunity to participate and provide feedback. Banks should also start to prepare to implement the CFI.

Cyber Resilience Assessment Framework (C-RAF)

- What cybersecurity information is available to the board and senior management when making appropriate C-RAF risk decisions?
- How do you ensure that the board and senior management are regularly involved in managing cybersecurity risks and resource allocation?
- How do you integrate C-RAF within the existing risk management framework?
- Who is responsible for assessing risk and conducting maturity assessments?
- How can you develop an improvement plan and continue to monitor its progression?
- How can banks conduct simulation based tests for cyber attacks?

Cyber Intelligence Sharing Platform

- Do you have a management framework for dealing with threat intelligence?
- Have you defined the roles and responsibilities across different departments, the process for dealing with any threats and the communication channels to senior management?
- How can you integrate threat intelligence with existing processes such as intrusion detection, incident response, crisis management, simulation based testing?
- What are the existing protocols for sharing threat intelligence?

Professional Development Programme

- Do you have adequate resources across your main three lines of defence? Do they have the necessary cybersecurity management skills?
- What is your existing programme for talent management?
- How do you track the skills and resources of your employees?
- How do you promote organisational awareness on cybersecurity?

How KPMG China 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 cyber attack simulation exercises.	• 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

Kelvin Leung
Director, IT Advisory
KPMG China
T: +852 2847 5052
E: kk.leung@kpmg.com

Alvin Li
Associate Director,
IT Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

Matrix Chau
Associate Director,
IT Advisory
KPMG China
T: +852 2685 7521
E: matrix.chau@kpmg.com

kpmg.com/cn