

Cybersecurity Fortification Initiative (CFI) 2.0

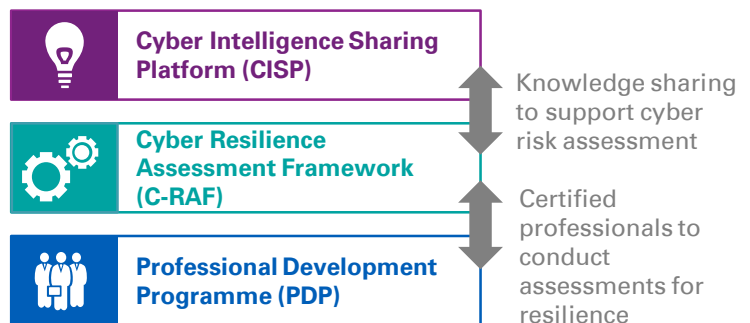
Further enhancements to strengthen the cyber resilience of Hong Kong's Banking industry

Enhanced cybersecurity framework

In light of the continuous and fast-paced developments in cybersecurity and technology, as well as the presence of increasingly dynamic and complex cyber threats, the Hong Kong Monetary Authority (HKMA) has conducted a review of its Cybersecurity Fortification Initiative (CFI) to improve the cybersecurity of the banking systems.

An enhanced scheme, CFI 2.0, has now been introduced, with a structured implementation timeline starting in mid-2021 and continuing through 2023. We have summarised the changes below:








The HKMA's Cybersecurity Fortification Initiative








Cyber Resilience Assessment Framework (C-RAF)	<ul style="list-style-type: none"> Allow flexibility to leverage group or headquarters' assessment results, subject to conditions Assessment should be generally conducted every three years 					
	<table border="1"> <thead> <tr> <th>Inherent Risk Assessment</th> <th>Maturity Assessment</th> <th>iCAST</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> An "upward override" mechanism Refined calculation approach for Inherent Risk Level Refinement of indicator criteria and its definition </td> <td> <ul style="list-style-type: none"> Outline Objectives of the Control Principles Introduce new and enhanced Control Principles </td> <td> <ul style="list-style-type: none"> More elaborated guidance on the expectations to avoid misunderstanding Flexibility in leveraging generic Threat Landscape Report Blue Team Requirements </td> </tr> </tbody> </table>		Inherent Risk Assessment	Maturity Assessment	iCAST	<ul style="list-style-type: none"> An "upward override" mechanism Refined calculation approach for Inherent Risk Level Refinement of indicator criteria and its definition
Inherent Risk Assessment	Maturity Assessment	iCAST				
<ul style="list-style-type: none"> An "upward override" mechanism Refined calculation approach for Inherent Risk Level Refinement of indicator criteria and its definition 	<ul style="list-style-type: none"> Outline Objectives of the Control Principles Introduce new and enhanced Control Principles 	<ul style="list-style-type: none"> More elaborated guidance on the expectations to avoid misunderstanding Flexibility in leveraging generic Threat Landscape Report Blue Team Requirements 				
Cyber Intelligence Sharing Platform (CISP)	<ul style="list-style-type: none"> Recommend the development of a Target Operating Model to improve the user-friendliness of CISP by outlining the governance, roles and responsibilities of users Expand the CISP membership to on-board members of the Deposit-taking Companies ("DTC") Association and other financial sectors 					
Professional Development Programme (PDP)	<ul style="list-style-type: none"> Update and expand the list of acceptable / equivalent cyber professional qualifications 					

CFI 2.0 changes at a glance

The CFI 2.0 changes affect all areas of cybersecurity coverage. The following are some of the key changes that are to be implemented across the seven domains of the C-RAF:

Governance 	<ul style="list-style-type: none"> Defines new requirements for key cybersecurity management roles. These include separate reporting lines for key roles - Chief Information Security Officer and Head of Technology Risk - to oversee, coordinate and govern enterprise-wide cybersecurity
Identification 	<ul style="list-style-type: none"> While a structured cyber risk management framework has always been a requirement, CFI 2.0 requires a new structure for the framework. This needs to cover risk identification; registering, assessment and treatment of threats; ongoing monitoring; and review and reporting
Protection 	<ul style="list-style-type: none"> Enhances requirements for sufficient controls to respond to different kinds of threats, including new physical, remote, wireless and mobile access Establishes new requirements for infrastructure protection controls, including virtualisation security and Internet of Things (IoT) security, given their wider adoption in the industry Firms will now need to have DevOps activities and processes to align with their System Development Life Cycle (SDLC) - including IT service management processes and agile software development if these are used within SDLC New requirements on testing of Application Programming interfaces (APIs) against known types of cyberattacks
Detection 	<ul style="list-style-type: none"> New requirement on continuous detection and endpoint behavioral detection Clarity on the need of security audit log retention for incident response investigation
Response and recovery 	<ul style="list-style-type: none"> More clarity in the definition of accountability and responsibilities to ensure appropriate stakeholders are engaged in the event of a cyber incident New established processes to identify qualified third-party cyber incident response and recover experts and establish a retainer agreement New requirement for management framework for dealing with Cyber forensics The need to have a continuous improvement processes for cyber incident response and recovery capabilities
Situational awareness 	<ul style="list-style-type: none"> New requirement on how to effectively share threat intelligence internally and externally
Third party risk management 	<ul style="list-style-type: none"> Clear responsibilities are now defined in the understanding of how you are connected to external networks or information systems More clarity on the need to have a structured process to perform due diligence and regularly perform security assessments or audit of the service providers

How KPMG can help

C-RAF based assessment	Formulation of improvement roadmap	Boardroom strategy workshop	Threat intelligence framework	Training programme management
<ul style="list-style-type: none"> 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 (iCAST) 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Boardroom awareness training to improve awareness and understanding of key risks Assist in establishing a governance structure and process on management oversight 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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
Technology Consulting
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Brian Cheung
Director
Technology Consulting
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

John Chiu
Associate Director
Technology Consulting
KPMG China
T: +852 2847 5096
E: john.chiu@kpmg.com

Kenneth Kwan
Associate Director
Technology Consulting
KPMG China
T: +852 2685 7390
E: kenneth.kwan@kpmg.com

kpmg.com/cn

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG Advisory (Hong Kong) Limited, a Hong Kong limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in Hong Kong, China.