This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To set out the overall policy and approach of the Hong Kong Monetary Authority (HKMA) for supervising authorized institutions' (AIs') management of cyber risks and for strengthening the cyber resilience of the banking sector.

Classification

A statutory guideline issued by the MA under the Banking Ordinance §7(3)

Previous guidelines superseded

Circular on "Cybersecurity Risk Management" dated 15 September 2015.

Application

To all AIs

Structure

1. Introduction
   - 1.1. Background
   - 1.2. Application
2. HKMA's policy on cyber risk supervision and roles of AIs
3. Supervisory processes
   - 3.1. Risk-based approach

3.2. Assessing cyber risks of individual AIs

3.3. Assessing systemic cyber risks

3.4. Providing supervisory guidance

3.5. Implementing the Cyber Resilience Assessment Framework (C-RAF) to strengthen AIs' cyber defence maturity

3.6. Conducting supervisory reviews

4. Strengthening the banking sector's incident response and recovery capabilities

5. Implementing infrastructure for information sharing

6. Industry engagement and feedback

7. Domestic and international co-operation

7.1. Domestic collaboration on cyber risk management

7.2. International co-operation on sound practices and information exchange

1. Introduction

1.1 Background

1.1.1 Growing level of digitalisation and technological adoption across the globe have brought both new opportunities and risks. In an increasingly technology-dependent and interconnected ecosystem, cyber threats have emerged as a growing concern for the banking and financial sector. The HKMA attaches great importance in strengthening the cyber resilience of AIs in Hong Kong, noting that a significant cyber incident can fuel broader risk implications for the overall stability of the financial system.

1.1.2 The borderless and evolving nature of cyber threats highlights the importance of cross-jurisdictional and cross-sectoral collaboration. Internationally, the HKMA participates in relevant standard-setting bodies and forums, including the Financial Stability Board (FSB) and the Basel Committee on Banking Supervision (BCBS), and joins hands with other financial authorities in addressing cyber risks that might threaten global financial stability.

1.1.3 Domestically, the HKMA collaborates closely with other relevant Government policy bureaux, law enforcement agencies, financial regulators and market participants in improving AIs' resilience to cyber threats, given the interconnectedness of different sectors in the financial system, and potential systemic impact of a severe cyber incident.

1.2 Application

1.2.1 This Module sets out the HKMA's overall policy and supervisory approach on AIs for managing cyber risks, which is premised on a risk-based, forward-looking and collaborative approach. It should be read in conjunction with other related Supervisory Policy Manual (SPM) modules, assessment frameworks and guidance relevant to cyber risk management or

cybersecurity issued by the HKMA from time to time.

2. HKMA's policy on cyber risk supervision and roles of AIs

2.1 The HKMA adopts a risk-based approach to cyber risk supervision. The policy objective is to enhance the cyber resilience of the Hong Kong banking sector by guiding AIs in managing cyber risks and fostering relevant industry-wide initiatives.

2.2 Under this policy, AIs are required to develop robust technology and cyber risk management frameworks that are proportionate to the nature, scale and complexity of their operations. This principle is consistent with those set out in other SPM modules including Module IC-1 "General Risk Management Controls" and Module TM-G-1 "General Principles for Technology Risk Management".

2.3 It is acknowledged that while cyber risks cannot be completely eliminated, AIs should attain a level of resilience commensurate with their cyber risk exposure, and be prepared to effectively respond and recover from severe but plausible cyber incidents.

2.4 AIs are responsible for designing and implementing effective systems and safeguards to manage cyber risks. They should also promptly report significant cyber incidents to the HKMA and, where appropriate, relevant authorities [1] in accordance with prevailing legal and regulatory obligations.

2.5 AIs are expected to support collaboration with other market participants, industry associations, the HKMA and other financial regulators, and relevant authorities to address systemic cyber risks, and thus contributing to the overall stability of the financial system.

3. Supervisory processes

3.1 Risk-based approach

3.1.1 The HKMA adopts a risk-based approach in its

[1] Including the Office of the Privacy Commissioner for Personal Data (PCPD), the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force etc.

supervision of AIs' cyber risk management. In general, supervisory attention and resources of the HKMA are focused on AIs with higher cyber risks, as well as emerging risks that could pose serious threat to the stability of the banking system. As cyber threats may evolve rapidly and entail cross-jurisdictional implications, the HKMA conducts cyber risk supervision in a forward-looking and collaborative manner on par with international standards.

3.2 Assessing cyber risks of individual AIs

3.2.1 In evaluating cyber risks of individual AIs, the HKMA engages the industry through ongoing discussions and supervisory reviews (e.g. reviews of AIs' cyber resilience assessment results, onsite examinations, offsite reviews on AIs' management of cyber risks), and also takes into account AIs' track record on reporting, responding to, and recovering from cyber incidents. Based on the results of the supervisory activities, the HKMA periodically determines, and adjusts if appropriate, the priority and intensity of supervisory engagement with individual AIs.

3.2.2 As the cyber risk faced by an AI may evolve over time in the light of factors such as technological advancement, change in business models, or evolving tactics of threat actors, the HKMA places strong emphasis on ongoing risk assessment and agility in its supervisory activities.

3.3 Assessing systemic cyber risks

3.3.1 Given the borderless and potentially contagious nature of cyber incidents, the HKMA recognises that assessing cyber risks at an individual AI level might not sufficiently capture system-wide cyber risks. The HKMA therefore develops supervisory tools and programmes to facilitate the understanding and mapping of potential sources of systemic cyber risks within and beyond the banking sector, and to formulate appropriate initiatives to address the vulnerabilities

identified.

3.3.2 For example, in line with the sound supervisory practices for effective cybersecurity risk supervision published by the International Monetary Fund (IMF), the HKMA undertakes a cyber mapping exercise together with other domestic financial authorities to (i) map out the network interdependencies between key financial institutions, Financial Market Infrastructures (FMIs) and technology service providers, and (ii) identify potential concentration risks across the Hong Kong financial system. Based on the potential vulnerabilities identified from the exercise, the HKMA collaborates with other relevant Government policy bureaux, financial authorities, and market participants to address the associated systemic cyber risks.

3.4 Providing supervisory guidance

3.4.1 Cyber risk management interacts with general technology risk management and operational resilience, and relevant guiding principles are therefore not new to AIs. Relevant supervisory expectations are stipulated in SPM modules including but not limited to:

(a) TM-G-1 “General Principles for Technology Risk Management” sets out expectations on IT governance and technology risk management covering security controls;

(b) TM-E-1 “Risk Management of E-banking” provides guidance on risk management of e-banking services covering system and network security for Internet banking systems;

(c) OR-2 “Operational Resilience” provides guidance on the general principles that AIs are expected to consider when developing their operational resilience frameworks which include cyber security as one of the key elements; and

(d) SA-2 "Outsourcing" sets out the HKMA's supervisory approach on outsourcing covering general vendor management and measures to preserve confidentiality of customer data.

3.4.2 To complement existing supervisory guidelines, the HKMA issues circulars or other communications to the industry from time to time to provide additional guidance or insights on emerging cyber threats or issues.

3.5 Implementing the Cyber Resilience Assessment Framework (C-RAF) to strengthen AIs' cyber defence maturity

3.5.1 The Cyber Resilience Assessment Framework (C-RAF) introduced by the HKMA is an assessment tool that aims to facilitate AIs in effectively assessing their cyber risk profiles and benchmarking the level of defence and resilience required. The framework comprises:

(a) an inherent risk assessment based on risk factors such as AIs' business size, operational characteristics, technology profile and usage;

(b) a maturity assessment for AIs to assess whether their cybersecurity controls are commensurate with their inherent risk levels; and

(c) an Intelligence-led Cyber Attack Simulation Testing (iCAST) for AIs with "medium" or "high" inherent risk ratings to test their cyber resilience by simulating real-life cyber attacks.

3.5.2 AIs are required to conduct regular assessments under the C-RAF with a view to raising their cyber defence maturity to a level commensurate with the assessed risk exposures. The HKMA will engage the industry and update the C-RAF from time to time to keep pace with the evolving global and local cyber risk landscape as appropriate.

3.6 Conducting supervisory reviews

3.6.1 The HKMA conducts a range of supervisory work on AIs' cyber risk management and cybersecurity controls, including in the form of on-site examinations, reviews of AIs' C-RAF assessment results and other off-site reviews following a risk-based approach.

3.6.2 The HKMA engages with AIs' Board and/or senior management if relevant issues identified from the reviews warrant their attention, while common issues and best practices distilled from the supervisory reviews or other activities are shared with the industry where appropriate.

4. Strengthening the banking sector's incident response and recovery capabilities

4.1 Significant cyber incidents, if not properly managed, could potentially disrupt the financial system in Hong Kong and pose risks to financial stability. Therefore, the HKMA actively facilitates the development of the banking sector's capabilities on incident response and recovery.

4.2 Among others, the HKMA facilitates and participates in industry-led cyberattack simulations to enhance the sector's collective preparedness against cyber incidents. Through these drills, the HKMA, AIs and other industry players can strengthen ongoing collaboration, information sharing, and collective response to systemic cyber incidents impacting multiple sectors.

4.3 To mitigate the escalating risk of destructive cyber attacks (e.g. ransomware attacks) and to improve AIs' data resilience, the HKMA promotes AIs' adoption of the Secure Tertiary Data Backup (STDB) in order to recover and restore critical data promptly in the event that a cyberattack compromises both the production and backup environments of AIs.

5. Implementing infrastructure for information sharing

5.1 The sharing of cyber threat intelligence and incident-related information is widely recognised as an important element in monitoring cyber risks and raising collective defence. In this

connection, the HKMA launched the Cyber Intelligence Sharing Platform (CISP) under the Cybersecurity Fortification Initiative (CFI) to provide an effective infrastructure for AIs to exchange cyber intelligence in a timely and secure manner.

5.2 The HKMA collaborates with the Hong Kong Association of Banks (HKAB) to enhance cyber threat intelligence sharing within the banking sector and across financial sectors, including improvement of the CISP from time to time.

6. Industry engagement and feedback

6.1 The HKMA regularly engages the industry to share its supervisory feedback, ranging from good cyber risk management practices to areas of risk concerns, to facilitate AIs in strengthening their cyber resilience. The HKMA also periodically engages AIs and industry associations to understand the practical challenges in managing cyber risks, and to exchange views on emerging topics.

6.2 These interactions serve as a useful communication channel for the HKMA to keep abreast of the industry's developments in the cyber risk space, seek collaboration opportunities, clarify supervisory expectations, and help formulate supervisory focuses and activities as appropriate.

7. Domestic and international co-operation

7.1 Domestic collaboration on cyber risk management

7.1.1 The HKMA is committed to addressing the systemic implications of cyber threats through ecosystem-wide collaboration. This includes supporting ongoing efforts of relevant authorities and other market participants in fortifying Hong Kong's overall defence against cyber attacks. In this regard, the HKMA seeks to:

a) ensure its supervisory regime is congruent with the overall cybersecurity strategy and statutory framework of the Government;

b) collaborate with relevant Government policy

bureaux and sectoral authorities to identify and address vulnerabilities in the broader cyber ecosystem to facilitate the ongoing provision of essential financial services by AIs; and

c) enhance the collective response to systemic cyber incidents through appropriate reporting and information sharing mechanisms among relevant authorities and stakeholders.

7.2 International co-operation on sound practices and information exchange

7.2.1 As a member of the FSB and BCBS, the HKMA supports the work of international bodies through taking part in formulating policy standards that contribute to effective cyber risk supervision by financial authorities, as well as promoting sound cyber risk management practices to financial institutions. These international standards and practices are integrated into the local supervisory regime as appropriate.

7.2.2 The HKMA exchanges information and shares intelligence with overseas financial authorities as necessary and permissible under collaborative arrangements, and actively participates in the global cyber intelligence sharing community.

———————————