HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
G4/58C

2 June 2026

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Strengthening Cyber Resilience amid Artificial Intelligence-Empowered Cyber Threats

I am writing to remind Authorized Institutions (AIs) to stay vigilant amidst the evolving global cyber threat landscape, and especially the potential for cyber-attacks empowered by frontier Artificial Intelligence (A.I.) models.

The risks that A.I. could be leveraged for nefarious purposes are not new. Indeed, the Hong Kong Monetary Authority (HKMA) has long been working with AIs to counter different A.I.-assisted attacks, including those concerning phishing, malware and deepfakes[1]. However, the recent emergence of increasingly capable frontier A.I. models could mark a step change in the global cyber risk landscape. As highlighted by several A.I. firms and research institutes, these frontier A.I. models show capacity to independently identify and exploit zero-day vulnerabilities in critical software and infrastructures, and could commoditise the attack process by reducing the need for

[1] For instance, please see the HKMA's circular on "E-Banking Security ABCD" issued on 25 August 2025.

human expertise and involvement. This could result in faster, more frequent and increasingly sophisticated cyber-attacks.

Defenses will need to adapt accordingly. In particular, AIs are expected to:

- **Critically review and assess the sufficiency of their existing cyber defense controls:** In line with the HKMA's existing supervisory requirements[2], AIs already have multi-layered defenses against the zero-day vulnerabilities targeted by frontier A.I. models, including but not limited to defense-in-depth, zero trust architecture and appropriate patching protocols. In view of the evolving threat, AIs should assess whether current arrangements remain fit-for-purpose assuming the scale and speed of attacks will accelerate with frontier A.I.'s assistance. As part of this process, AIs should also assess the cyber resilience capabilities of their third-party service providers, which as common "nodes" supporting the ecosystem, are increasingly being targeted by threat actors and as potential points of entry to compromise AIs' systems and data, that is, supply chain attacks.

- **Uplift incident response and recovery capabilities:** As the velocity and intensity of cyber-attacks trend upwards, "breach" scenarios will become more probable. With this, AIs should critically review the readiness of their incident response and recovery processes, including but not limited to playbooks prepared for prominent cyber-attacks. Where appropriate, suitable scenario testing should be conducted, including as part of prevailing operational resilience programmes. AIs will also need to ensure that any third parties that they are dependent on during the response and recovery process are equipped and sufficiently resourced to step up in times of need.

[2] Including as set out in Supervisory Policy Manual (SPM) module TM-C-1 on "Supervisory Approach on Cyber Risk Management" and the Cyber Resilience Assessment Framework (C-RAF) 2.0.

- **Enhance data resilience to counter destructive cyber-attacks:** For AIs that have implemented a Secure Tertiary Data Backup (STDB) as recommended by the HKMA, they should review whether and how related arrangements could be improved to enhance response capacity in the event of a destructive attack. AIs that have yet to implement a STDB should also revisit the decision in the light of the evolved risk landscape.

While individual AIs are responsible for their own cyber resilience, the HKMA recognises the importance of ecosystem collaboration and empowerment in the fight against A.I.-driven threats. The HKMA will continue to actively support the industry through a series of targeted initiatives, including:

- **Establishment of Task Force on A.I.-Driven Cyber Risks:** This Task Force will serve as an official forum for key stakeholders in the financial and cyber risk ecosystem – including financial authorities, financial institutions, relevant government bureaux and departments and cyber experts – to stay connected on the latest intelligence around A.I.-driven risks and to discuss practical ecosystem responses. A key objective of the Task Force is to address potential information asymmetry that may arise as a result of rapid cross-jurisdictional developments. Key findings and takeaways will be shared with the broader industry in a timely manner.

- **Development of the Cyber Resilience Testing Framework (CRTF):** This new supervisory framework will provide AIs with a systematic way to stress test their ability to respond to and recover from actual "breach" situations. It augments and complements existing cyber initiatives by extending AIs' cyber resilience capabilities from detection and prevention-based to also oriented around response and recovery. A dedicated Industry Working Group formed under the Hong Kong Association of Banks (HKAB) is currently working with the HKMA on the Framework's development, and an initial test run with selected institutions is targeted for late 2026.

- **Supporting the effective implementation of the Protection of Critical Infrastructures (Computer Systems) Ordinance (PCICSO):** As a designated authority for the banking and financial services sector under the PCICSO, the Monetary Authority (MA) is charged with a number of responsibilities aimed at enhancing the cyber security of the critical computer systems (CCSs) operated by critical infrastructure operators (CI operators)[3]. To facilitate effective discharge of these duties, the MA has entered into a Memorandum of Understanding (MoU)[4] with the Commissioner of Critical Infrastructure (Computer-system Security) to ensure a coordinated approach to implementation work, and which prioritises reduced compliance burden for the industry where practicable. To better support AIs designated as CI operators (Designated AIs), the MA has also, pursuant to Section 8(1) of the PCICSO, issued a Sectoral Code of Practice (CoP) that provides practical guidance on how Designated AIs can comply with the category 1 and category 2 statutory obligations, including as far as practicable, by leveraging the HKMA's prevailing supervisory framework. The said Sectoral CoP has taken into account the outcomes of an extensive industry consultation and came into operation on 2 June 2026. It is available at the HKMA's website at https://brdr.hkma.gov.hk/eng/doc-ldg/current/20260527-25-EN.

[3] These include, amongst others, the duty to ascertain specified critical infrastructures (CIs) under the MA's purview, designate CI operators as well as their associated CCSs. The MA is also responsible for supervising such CI operators' compliance with the category 1 (organizational) and category 2 (preventive) obligations set out under the PCICSO. The Commissioner of Critical Infrastructure (Computer-system Security) is responsible for overseeing compliance with the category 3 (incident reporting and response) obligations.

[4] A copy of the MoU can be accessed at the HKMA's website at https://www.hkma.gov.hk/eng/key-functions/banking/banking-regulatory-and-supervisory-regime/supervisory-co-operation/.

The HKMA will continue to closely monitor global developments, engage with the industry and relevant ecosystem participants, and provide additional supervisory guidance and practical support as appropriate, to uplift the cyber resilience of the banking sector.

Should your institution have any questions about this circular, please contact us at bsd-tr-cs@hkma.gov.hk.

Yours faithfully,

Carmen Chu
Executive Director (Banking Supervision)

cc: FSTB (Attn: Mr Timothy Wong)
SB (Attn: Mr Francis Chan)