HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

21 December 2023

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Managing cyber risk associated with third-party service providers

I am writing to share with the industry a set of sound practices for managing cyber risk associated with the use of third-party service providers.

As digitalisation of banking services advances, authorized institutions (AIs) are increasingly leveraging technology and third-party services to drive business growth and enhance operational efficiency. Meanwhile, greater reliance on third-party services has heightened AIs' exposure to cyber risk as threat actors target the weakest link in the supply chain of digital banking services. In fact, there was a rise in both the number and sophistication of supply chain attacks that impacted a multitude of global institutions over the past year. Against this backdrop, the HKMA has undertaken a round of thematic examinations focused on AIs' management of cyber risk associated with the use of third party services, and would like to share with the industry the sound practices observed.

Sound practices

As stated in various Supervisory Policy Manual modules of the HKMA (including "TM-G-1 General Principles for Technology Risk Management" and "OR-2 Operational Resilience"), AIs are required to put in place effective cyber defence covering their own operations as well as linkages with third-party service providers. The below sound practices, identified from the thematic examinations, provide guidance on how AIs may comply with this requirement.

- **Ensure sufficient emphasis on cyber risk associated with third-parties in risk governance framework** – The board of directors and senior management of AIs should ensure that their institution's governance framework for third-party risk management and cybersecurity place sufficient emphasis on cyber risk associated with the use of third-party services and products. The governance framework should enable the AI to effectively identify, assess and manage cyber risk associated with different types of third-party relationships under a range of possible scenarios (e.g. data breaches or operational disruptions at the service providers, or security compromise of third-party services or products).

- **Holistically identify, assess and mitigate cyber risk throughout the third-party management lifecycle** – As part of their third-party risk management processes, AIs should holistically identify, assess and mitigate cyber risk associated with third-parties before onboarding, and conduct regular reviews thereafter. This should include identifying cyber risk resulting from the actual operational set-up (e.g. third-parties' access to AIs' internal systems, data exchange and network connection with AIs), assessing the cyber resilience of third-parties and ensuring adequate security measures are in place to mitigate the relevant risks. These security measures should be supported by proper contractual agreements, with effectiveness evaluated periodically throughout the third-party management lifecycle.

- **Assess supply chain risks associated with third-parties supporting critical operations** – In light of the emerging threat of supply chain attacks, AIs should critically assess the supply chain risks arising from third-parties supporting critical operations by conducting additional due diligence in areas such as dependencies on fourth-parties and end-to-end data processing. AIs are advised to understand the service providers' secure software development practices and consider conducting additional security assurance reviews for higher-risk software acquisitions.

- **Expand cyber threat intelligence monitoring to cover key third-parties and actively share intelligence with peer institutions** – In addition to monitoring cyber threats intelligence related to their own environment, AIs should stay vigilant to cyber threats that target key technologies and third-party services used by them to enable timely impact assessment and the taking of containment actions. AIs should also actively exchange intelligence via the Cyber Intelligence Sharing Platform (CISP) with peer institutions in a bid to strengthen the industry's collective preparedness against supply chain attacks.

- **Strengthen the preparedness for supply chain attacks with scenario-based response strategies and regular drills** – Since supply chain attacks are difficult to prevent in advance, AIs should formulate scenario-based incident response strategies taking into account common risk scenarios and lessons learnt from previous supply chain incidents. AIs should also establish effective response protocols with third-parties supporting critical operations and conduct regular drills to validate and refine the established protocols.

- **Continuously enhance cyber defence capabilities through adopting the latest international standards, practices and technologies** – In light of the growing complexity of third-party relationships and evolving cyber threat landscape, AIs should regularly review and enhance their layers of cyber defence with reference to latest international standards and sound practices. In particular, AIs are encouraged to adopt regulatory technologies to refine, automate and streamline third-party risk management controls and uplift their cyber defence capabilities. Reference may be made to the HKMA's Regtech adoption guidance.

More details of the above best practices can be found in the **Annex**. AIs are expected to review their existing controls to manage cyber risk associated with third-parties against the above guidance. Where gaps are identified, AIs should seriously consider applying the sound practices in a manner commensurate with their cyber risk exposures and the level of reliance on third-parties. The HKMA will continue to keep abreast of the international and industry developments in third-party cyber risk management, and provide further guidance to the industry as appropriate.

Should your institution have any questions about this circular, please feel free to contact Mr Edmund To on 2878 1105 or Ms Angel Tse on 2597 0433.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Encl.