Annex

Managing cyber risk associated with third-party service providers

The HKMA completed in 2023 a round of thematic examinations focused on AIs' third-party cyber risk management. This note shares the sound practices identified from the thematic examinations with a view to assisting authorized institutions (AIs) in strengthening their overall cyber resilience.

1. 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 set out structured and cohesive processes to identify, assess and manage cyber risk associated with different types of third-party relationships, including outsourcing and non-outsourcing arrangements as well as IT asset acquisitions. Well-defined risk parameters, such as the sensitivity and volume of data involved, the interconnectivity with other systems, and the complexity of the supply chain, should be developed. This would enable AIs to systematically assess and address the cyber risk implications of each third-party relationship under different scenarios (e.g. data breaches, operational disruptions, potential spill over damage in case of security compromise of third-party services or products).

2. 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 (such as sensitive data generation, exchange and storage, and access to and interaction with AIs' internal systems and/or systems of fourth-parties), assessing the cyber resilience of their third-party service providers, and ensuring adequate security measures (e.g. data encryption, access controls, network and service interface monitoring) are in place to mitigate the relevant risks. When conducting these reviews, AIs should follow a risk-based approach and should not rely solely on the general IT and security controls of the third-parties or external audit assurance reports. AIs should ensure that these control measures are properly implemented and proportionate to the underlying risks throughout the third-party management lifecycle. Where appropriate, these control measures should be set out in contractual agreements, with their effectiveness monitored through regular service meetings and periodic re-assessments.

3. Assess supply chain risks associated with third-parties supporting critical operations

In light of the emerging threat of supply chain attacks, it is important for AIs to conduct additional assessments of supply chain risks arising from third-parties which support AIs' critical operations or which can cause a higher security risk if the third-party

service or product is compromised. This would normally involve obtaining a better understanding of the third-parties' supply chains and conducting additional due diligence on areas such as dependencies on fourth-parties, use of open-source software and codes, end-to-end data processing and storage arrangements. The outcome of these reviews would enable AIs to assess third-party cyber risks more precisely and comprehensively, so as to determine the right level of ongoing monitoring required and facilitate effective responses to supply chain attacks targeting or affecting these third-parties. Further, to address the tactic of supply chain attacks through vulnerable commercial software, AIs should understand the secure software development practices of the software provider prior to acquiring mission critical system components. For cases assessed to be of high risk, AIs should consider conducting additional security assurance reviews (e.g. application security architecture review and penetration testing) prior to deploying the software in the production environment.

4. Expand cyber threat intelligence monitoring to cover key third-parties and actively share intelligence with peer institutions

Since supply chain attacks often involve exploiting zero-day vulnerabilities and can happen to any part of a supply chain, AIs should expand their cyber threat intelligence monitoring to include cyber threats that target key technologies and third-party services used by them. Through monitoring and responding to cyber threats relevant to their own environment and key third-parties, AIs would be able to enhance their capability in detecting potential supply chain attacks, thereby making timely impact assessments, incident response and the taking of containment actions possible. Furthermore, AIs should actively share supply chain threat intelligence with peer institutions via the Cyber Intelligence Sharing Platform (CISP) to strengthen the industry's collective preparedness against suspected or active supply chain attacks that may impact multiple institutions.

5. Strengthen the preparedness for supply chain attacks with scenario-based response strategies and regular drills

Given supply chain attacks are difficult to prevent in advance, it is important for AIs to strengthen their preparedness by developing scenario-based incident response strategies, taking into account common risk scenarios and lessons learnt from previous supply chain incidents. Moreover, AIs' incident response strategies should reflect the need to continuously assess the impact of a supply chain attack and revisit the appropriateness of their containment actions as the investigation progresses. Triggering criteria for more severe actions (e.g. fully disconnecting and isolating the affected systems) should be properly defined so as to contain the damages when remedial measures are not immediately available or feasible. In addition, AIs should establish effective protocols with third-parties supporting critical operations for vulnerability disclosure and cyber incident notification, and conduct regular cyber incident response drills involving these third-parties to validate and refine the established protocols.

6. 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 the evolving cyber threat landscape, AIs should regularly review and enhance their layers of cyber defence with reference to the latest international standards and sound practices such as micro-segmentation, behavioural-based abnormality detection and zero-trust architecture. Further, AIs are encouraged to adopt technologies to refine, automate and streamline their third-party risk management and cybersecurity controls. For example, AIs may leverage Regtech to develop a central repository, mapping their third-parties to their critical banking services and operations for third-party management and risk monitoring purposes. With the help of Regtech, AIs may also automate their security operations in areas such as configuration and patch management to ensure the identified security vulnerabilities are promptly mitigated. AIs may visit the HKMA's Regtech Knowledge Hub (to be upgraded to a Fintech Knowledge Hub) for the latest supervisory guidance.