HONG KONG MONETARY AUTHORITY
香港金融管理局

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

保險業監管局
Insurance Authority

強制性公積金計劃管理局
MANDATORY PROVIDENT FUND SCHEMES AUTHORITY

29 July 2026

Ref: HKMA/B1/15C
SFO/IS/028/2026
INS/TEC/10/48
SU/CTR/2026/002

To: Chief Executives of all Authorized Institutions and Stored Value Facility Licensees
Chief Executive Officer of the Hong Kong Interbank Clearing Limited
Officers of all Designated Retail Payment Systems
Responsible Officers of all Licensed Corporations
Chief Executives of all Authorized Insurers
Chief Executives of all MPF Approved Trustees

Joint Circular on the Cross-Sectoral Cyber Mapping Exercise

The Hong Kong Monetary Authority ("HKMA"), the Securities and Futures Commission ("SFC"), the Insurance Authority ("IA"), and the Mandatory Provident Fund Schemes Authority ("MPFA") (collectively referred to as "the Authorities") issue this joint circular to advise the industry on the outcomes of the first production run of the cross-sectoral Cyber Mapping exercise.

Background

Against a backdrop of rapid digitalisation, the global financial system has become more interconnected. Financial institutions ("FIs") now increasingly rely on a complex network of shared technologies, infrastructures and third-party service providers. While these developments support innovation and efficiency, they also raise the risks of a single point of failure and that a cyber incident targeting one common party (e.g. a technology service provider) could propagate across the broader financial system.

While the Authorities have continually driven cyber resilience enhancements in their respective sectors, the "borderless" nature of cyber threats required an ecosystem response. In light of this, the Authorities collaborated to take forward

a Cyber Mapping exercise with the support of the Financial Services and the Treasury Bureau ("FSTB"). This initiative was aligned with the International Monetary Fund ("IMF")'s analytic framework [1], and informed by a recommendation given under the Financial Sector Assessment Program ("FSAP"), aiming to develop a Cyber Map to enhance the Authorities' understanding of cyber risk concentration and interdependencies within the financial system in Hong Kong.

Key takeaways from first production run

The first production run of the Cyber Mapping exercise was completed in March 2026. It delivered a Cyber Map that allowed the Authorities to visualise, for the first time, how over 50 participating FIs across the banking, retail payment, securities and capital markets, mandatory provident fund and insurance sectors are connected at both business and technology levels.

The Authorities have drawn three key takeaways from the Cyber Map:

1. **There are no new and major "unknown-unknown" sources of systemic cyber risk.** Specifically, the Cyber Map reaffirmed that the largest nodes in the Hong Kong financial system are those FIs, financial market infrastructures, and major technology service providers (e.g. cloud service providers, data centre operators) and data service providers already known to support critical business and technology functions.

2. **That said, a deeper analysis of specific business processes and information and communication technology ("ICT") arrangements revealed that certain third-party service providers playing critical roles within their areas of expertise might warrant increased supervisory attention moving forward.** In particular, similar adoption patterns were observed in participating FIs' use of network infrastructure appliances and cybersecurity solutions that support security event monitoring and privileged access management. Certain recurring specialist vendors were also observed in select payment processing and customer communication workflows. While this takeaway does not mean that the providers identified are unsafe, or that a systemic issue already exists, it does support the case for early, and forward-looking supervisory monitoring.

[1] Please see the IMF's Paper on "Cybersecurity Risk Supervision" (24 September 2019) and "Good Practices in Cyber Risk Regulation and Supervision" (5 January 2026)

3. **Cyber Mapping is a useful risk management tool for the Authorities and potentially FIs in the future.** In addition to enabling the visual depiction of potential systemic cyber risks, the dashboard-based design of the Cyber Map allows the Authorities to dynamically filter outcomes based on a scenario at hand and turn complex data sets into actionable insights. These capabilities are particularly useful in supporting more precise third-party risk supervision and triaging of and response to incidents. Building on this experience, there may be potential, in the future, to extend the Cyber Map's dashboard capabilities to FIs (for data relevant to them) to support their own risk management and incident handling.

While the Cyber Map did not reveal any immediate sources of systemic cyber risk outside the Authorities' current supervisory radar, it reaffirmed that the financial sector is highly interconnected, and that these connections are becoming increasingly complex as the technology landscape and role of third parties continues to evolve. This underscores the importance of the Authorities' ongoing portfolios of work to enhance cyber resilience, including that focusing on strengthening FIs' capabilities across the full cyber risk management lifecycle.

Going forward, the Authorities will adopt the Cyber Map to complement their day-to-day supervisory work, especially in the areas of third-party risk and incident management. Where warranted, the Authorities will also leverage relevant insights distilled from the Cyber Map and take forward additional cross-sectoral collaboration as needed, such as conducting drill exercises, thematic reviews, and developing additional contingency arrangements. For the technical details of the Cyber Map – including underlying data collection methodology – please see the Technical Note attached at **Annex**. The Authorities will, where appropriate, also share insights and supervisory feedback specific to the FIs that participated in the first production run on a bilateral and confidential basis.

Further work

Noting the Cyber Map's strong value proposition, the Authorities intend to make the Cyber Mapping exercise a recurring fixture. Efforts are underway to consolidate the experience gained and feedback received throughout the first production run to enhance the exercise methodology, refine the data scope, expand the participant coverage, and develop permanent and sustainable infrastructure. During development, the Authorities will continue to be guided by the overarching principles applied to the first production run, including that of only collecting data necessary for producing an effective Cyber Map, and

placing top priority on ensuring data security. Based on current estimates, the Authorities expect to commence the next Cyber Mapping exercise in 2027/2028. More details will be shared with the industry well in advance.

The Authorities are fully committed to strengthening the resilience of the financial system. We appreciate the support from FIs that participated in the first production run and look forward to continued collaboration with the broader industry.

Carmen Chu
Executive Director
(Banking Supervision)
Hong Kong Monetary Authority

Eric Yip
Executive Director of Intermediaries
Securities and Futures Commission

Clement Lau
Executive Director
Policy and Legislation
Insurance Authority

Kenneth Chan
Executive Director (Members and Supervision)
Mandatory Provident Fund Schemes Authority

Annex

Technical Note on Cross-Sectoral Cyber Mapping Exercise

Purpose of Note

- This Technical Note sets out how the Authorities developed the inaugural Cyber Map, including the underlying data collection methodology, and approach adopted to visualise the data in dashboard format.

Developing the inaugural Cyber Map

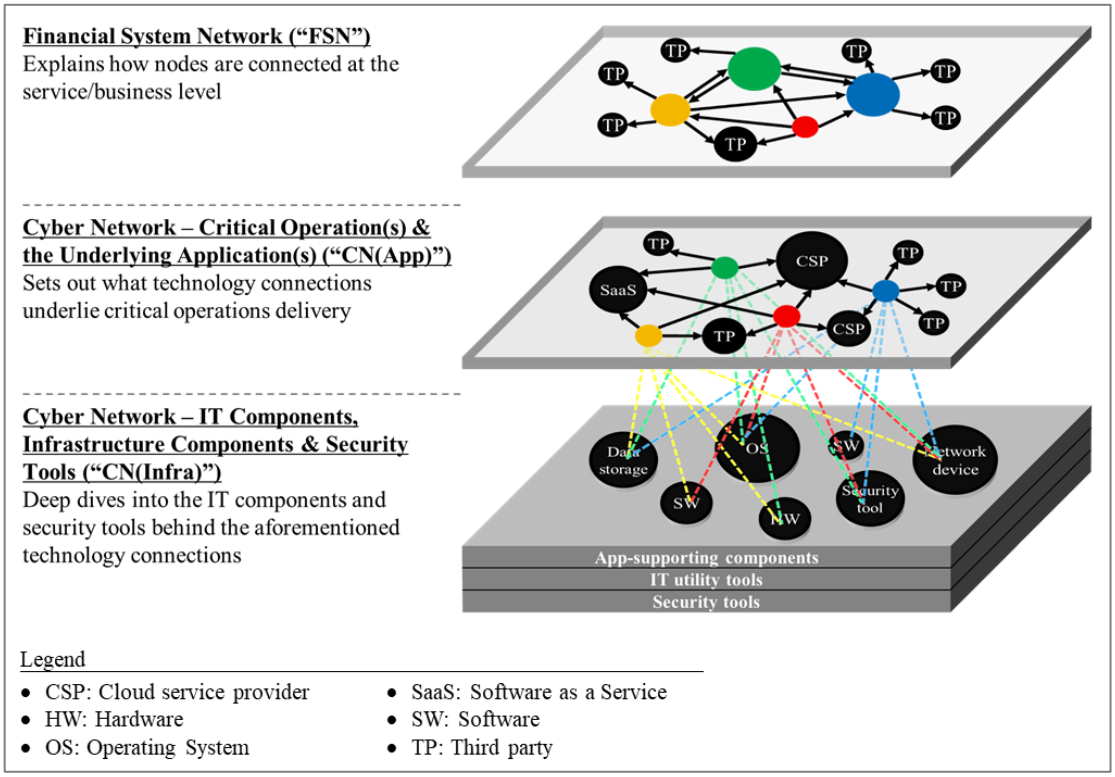
Exercise methodology

- The Cyber Mapping exercise had two key objectives, namely to: (i) help the Authorities better understand potential cyber risk concentration and interdependencies within the financial system in Hong Kong; and (ii) enable more targeted supervision and incident response by unlocking more precise mapping of third-party dependencies and potential spillover pathways.

- To achieve these dual objectives, the Authorities needed to design a unique data collection methodology that could map/track the inter-relationships between participating FIs' business and technological connections. Only through such a structure could the Authorities examine how a cyber incident could affect a FI's critical operations, spread across connected entities, and ultimately impact business service delivery at a more systemic scale. After establishing this baseline methodology, the Authorities also needed to determine the specific data fields that could adequately capture and represent these business and technological connections. This required careful balancing to ensure that the Authorities collected all information reasonably necessary to construct a useful Cyber Map, while not subjecting participating FIs to excessive reporting requirements.

- To ensure the exercise was well designed, the Authorities consulted with experts from the IMF and peer financial regulators, and also conducted a pilot run with selected FIs to reaffirm the reasonableness of the methodology and proposed data fields. Based on the constructive feedback provided by the industry and relevant experts, a three-layered structure that mapped financial services, critical operations and supporting applications, and the underlying IT infrastructure components was developed, as illustrated in **Diagram 1**.

Diagram 1: Cyber Map's three-layered data collection methodology



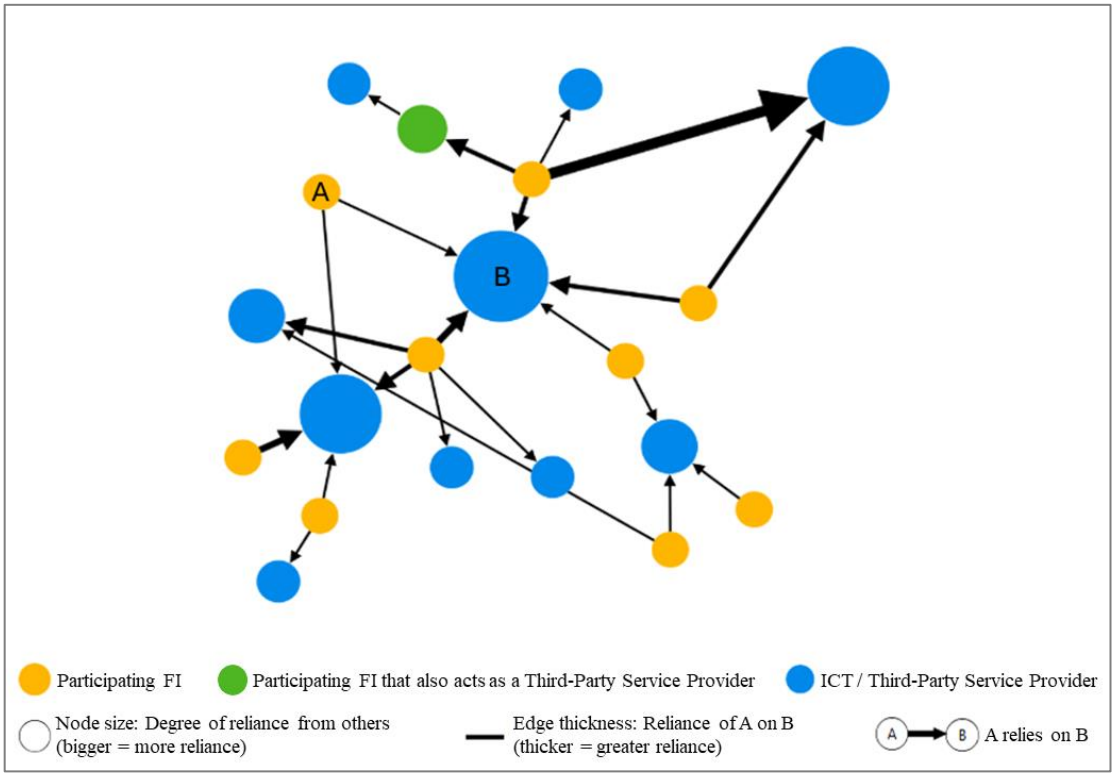
Constructing the inaugural Cyber Map

- Based on the finalised data collection methodology, the Authorities started collecting data from around 50 participating FIs in late 2025. To ensure the resulting Cyber Map would be reasonably representative and insightful, these FIs were selected from across the banking, retail payment, securities and capital markets, mandatory provident fund, and insurance sectors, taking into account factors including their market presence, systemic importance, cyber risk profile, as well as perceived interconnectedness. The data collection process was highly collaborative and involved extensive engagement with each FI, as well as iterative data cleansing. Ultimately, some 2,900 dependencies were captured in the inaugural Cyber Map, and used to develop the first visual representation of how FIs in Hong Kong are connected at both the business and technology levels.

- The Cyber Map was "charted" leveraging a dashboard-based, network visualisation solution. To facilitate intuitive analysis, the map design and associated legend were carefully constructed. Specifically, based on the relationship data collected from participating FIs, the map depicts each entity as a "node" and illustrates the relationships between different entities using lines of varying thickness, direction and colour.

- Where one entity (e.g. entity A) relies on another (e.g. entity B), the line would point <u>from</u> entity A to entity B, and also be thicker or thinner subject to the materiality of the dependency assessed (e.g. from a data transmission, system hosting perspective). Nodes are also colour-coded by entity type, e.g. participating FI, ICT service provider, etc. Finally, the size of a "node" indicates the degree to which the entity is relied on by others (**<u>Diagram 2</u>**). The Authorities further incorporated customised filtering options to allow quick categorisation of the full data set and targeted analysis based on the scenario under review.

<u>Diagram 2: Illustrative example of how network relationships are represented in the Cyber Map</u>



The Hong Kong Monetary Authority
The Securities and Futures Commission
The Insurance Authority
The Mandatory Provident Fund Schemes Authority

29 July 2026