Our Ref.: B1/15C

1 June 2026

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

<u>Operational Resilience: Sustaining and Uplifting</u>

I am writing to share the Hong Kong Monetary Authority (HKMA)'s expectations for Authorized Institutions (AIs) following the conclusion of the "1+3 year"[1] operational resilience journey set out in Supervisory Policy Manual (SPM) module OR-2 on Operational Resilience.

Based on the results of a recent survey conducted by the HKMA, all AIs have achieved operational resilience by end-May 2026 as planned. Each AI has systematically completed the steps of developing a robust operational resilience framework, identifying its critical operations and corresponding tolerances for disruption, conducting mapping and scenario testing to further its understanding of interconnections/dependencies, as well as remediating potential vulnerabilities. We are particularly encouraged that AIs have made extensive use of the supervisory resources provided by the HKMA, including good practice guides, as well as industry sharing sessions and drills simulating a major cross-sectoral disruption[2].

/…page 2

[1] SPM module OR-2 required AIs to develop an operational resilience framework no later than 1 year after 31 May 2022, and to fully implement the framework and achieve operational resilience no later than 31 May 2026.

[2] These included:
- Industry sharing sessions in November 2022 and December 2024 covering respectively, the topics of governance and the establishment of operational resilience parameters, and conducting mapping and scenario testing.
- Circulars setting out good practices for mapping and scenario testing (issued in January 2025) and addressing vulnerabilities (issued in April 2026).
- Support to the 2023 and 2025 editions of the Whole Industry Simulation Exercise which allowed participants to simulate their ability to respond to a supply chain attack and an extreme weather event respectively.

Going forward, AIs should continue to sustain and uplift their operational resilience as a matter of "business as usual", in the light of the changing operating landscape. While AIs may adopt different approaches according to individual circumstances, the HKMA reminds AIs of the following core "building blocks" of operational resilience:

- **"Tone from the top".** The Board and senior management should continue to lead by example and reinforce the importance of embedding operational resilience considerations across all processes. In particular, for those AIs that may have relied on project team-based structures during the "1+3 year" journey, proper transition to "business-as-usual" is required. To facilitate this, AIs should equip and empower all staff to take ownership and effectively discharge their duties on an ongoing basis. They should also provide training and guidance where necessary.

- **Continual review of operational resilience parameters.** AIs should regularly review[3] their list of critical operations, tolerances for disruption, and severe but plausible scenarios. The objective is to ensure that they properly reflect the AI's business profile, as well as prevailing risk landscape. Where appropriate, AIs should also challenge themselves in compressing tolerances for disruption to further minimise the potential impact of a disruption and aim to demonstrate tangible improvements in their operational resilience maturity.

- **Regularly refine mapping and scenario testing approaches.** AIs should strive to enhance the sophistication of their mapping, such as by deepening the granularity. As for scenario testing, scenarios of increasing severity and impact for testing may be developed. AIs should also consider, where possible, leveraging more technology elements for these processes to enhance their usability, such as to automate mapping so that new services or third-party service providers are automatically refreshed.

/…page 3

[3] SPM module OR-2 requires the Board to review: (i) the criteria for determining an AI's critical operations; (ii) the actual list of critical operations; and (iii) the tolerances for disruption set at least annually or when major operational changes occur. The continued relevance of the list of severe but plausible scenarios identified should be reviewed regularly by both the Board and senior management.

- **Proactively manage new risks and prioritise remediation efforts.** As the operating landscape evolves, new risks and vulnerabilities will inevitably emerge. For instance, Artificial Intelligence (A.I.) -empowered cyber risks could present step-changes in how AIs approach their cyber security as well as management of third-party service providers. AIs should have processes in place to stay abreast of major developments in a timely manner. There should also be a clear risk-based framework for determining the timeline and priority of remediations. The relevant risk management frameworks[4] and incident management programme should be enhanced to support the process as appropriate.

The HKMA will continue to monitor the post-OR-2 implementation progress of AIs and provide further guidance and support as necessary. Should your institution have any questions on the above, please contact us at operational.resilience@hkma.iclnet.hk.

Yours faithfully,

Carmen Chu
Executive Director (Banking Supervision)

[4] Including operational risk management, business continuity planning and testing, third-party dependency management, and information and communication technology (ICT) risk management, including cyber security.