HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C

1 April 2026

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Good practices for addressing vulnerabilities related to operational resilience

I am writing to share a set of good risk management practices as observed from our ongoing supervision and engagement with the industry. These will provide practical reference for Authorized Institutions (AIs) to address vulnerabilities related to operational resilience.

In line with the Supervisory Policy Manual (SPM) module OR-2 on Operational Resilience, all AIs are noted to have made substantial progress in developing and implementing related frameworks. The Hong Kong Monetary Authority (HKMA) has closely engaged with AIs, including through regular surveys, the review of self-assessments and independent validations, bilateral consultative sessions, as well as supported industry events like the Whole Industry Simulation Exercise (WISE) 2025. While the initial efforts centred on refining mapping and scenario testing approaches, AIs' attentions have naturally re-focused during the "last mile". These included evaluating the outcomes of these earlier exercises, and assessing whether there are residual risks or vulnerabilities that require enhanced risk management to secure full operational resilience by no later than 31 May 2026.

The HKMA notes that AIs have been proactive throughout this journey. Major AIs have implemented targeted enhancements to risk management areas with closer nexus to technology enablement, including information and communication technology (ICT) risk, cyber security risk, third-party dependency management as well as business continuity planning (BCP) and testing and incident management, with a view to better "future proof" their operational resilience frameworks.

/… page 2

In particular, good industry practices with details are set out in the **Annex**, covering the following aspects:

- **ICT risk management** – Incorporating "resilience by design" principles within ICT risk management, including by eliminating single points of failure within the technology environment, enhancing the resilience and recovery of key ICT supporting assets, and updating ICT risk management frameworks using a "resilience-first" mindset.

- **Cyber security risk management** – Enhancing risk management capabilities across the full cyber risk management lifecycle, leveraging both individual capabilities and broader ecosystem collaboration.

- **Third-party dependency management** – Incorporating operational resilience considerations within the third-party risk management framework (TPRMF), including from governance, contractual arrangements, risk assessment and monitoring controls, as well as exit management perspectives.

- **BCP and testing and incident management** – Enhancing BCP and testing arrangements, as well as incident management programmes to reflect operational resilience considerations, with a view to narrow recovery timelines and afford greater buffer to stay within the tolerances for disruption set in the event of more extreme disruptions.

AIs are encouraged to review the good practices in detail, consider their applicability, and take timely action to enhance related risk management practices where appropriate.

Leading up to the May 2026 implementation deadline, the HKMA will continue to provide supervisory support to AIs at both industry and individual levels. Thereafter, the supervisory focus will shift to supporting AIs to continually uplift and sustain their operational resilience posture. Further guidance will be provided as appropriate in due course.

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)