Our Ref.: B1/15C
B9/30C

31 August 2022

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

<u>Guidance on Cloud Computing</u>

We write to provide authorized institutions (AIs) with guidance on the HKMA's supervisory expectations with respect to the adoption of cloud computing.

In recent years, there has been a growing trend of AIs adopting cloud computing via the engagement of third-party Cloud Service Providers (CSPs). The scope of functions that AIs are deploying to the cloud is expanding from basic and non-core operations to more important ones.

The HKMA appreciates that cloud computing, if managed properly, provides a range of benefits, including cost efficiency, operational resilience and business scalability. Our supervisory policy has all along permitted AIs to utilise the technology so long as the associated risks are effectively managed, in compliance with the existing supervisory requirements, including those related to technology risk management and outsourcing. That said, given the growing trend of adoption, and considering that cloud computing does present specific risks, the HKMA considers it appropriate to set out its supervisory expectations on this area in a holistic manner.

Summary of guidance

The HKMA's supervisory expectations on cloud computing, as detailed in the **<u>Annex</u>**, are developed with reference to the results of a round of thematic examinations undertaken between 2021 and 2022. The key principles that AIs should pay attention to before they adopt cloud computing are summarised below:

I. Governance framework

1. AIs should put in place an effective governance framework overseen by the Board of Directors and senior management for cloud computing to enable them to formulate a cloud strategy suitable for their circumstances and have it updated from time to time;

2. A proper due diligence process should be established to assess the capabilities and suitability of a CSP before the engagement and regularly during the engagement;

II. On-going risk management and controls

3. AIs should clearly understand their roles and responsibilities under the agreement with the CSP and put in place corresponding controls to ensure the effective discharge of their responsibilities;

4. A comprehensive set of risk management procedures should be developed to enable AIs to continually identify, monitor and mitigate the risks posed by cloud computing;

5. There should be effective controls to ensure the security of the information assets of AIs and their compliance with relevant statutory requirements regarding customer data confidentiality;

6. A viable and effective contingency plan should be developed to cope with situations involving a disruption of cloud computing services;

III. Protection of access and other legal rights

7. There should be suitable arrangements which guarantee AIs' audit rights, and the HKMA's supervisory access to information stored in the cloud and relevant risk management controls for the purposes of undertaking on-site examinations;

8. A clear and enforceable CSP engagement agreement should be in place to protect AIs' interests, risk management needs and ability to comply with supervisory expectations; and

IV. Risk management capabilities

9. AIs should equip staff overseeing cloud operations with the knowledge and skills required to securely use and manage the risks associated with cloud computing.

AIs should note that the above principles serve to complement, and should be read in conjunction with, relevant existing HKMA guidance. These include SPM Modules SA-2 on *"Outsourcing"*, OR-2 on *"Operational Resilience"* and TM-G-1 on *"General Principles for Technology Risk Management"*. As with the HKMA's usual risk-based approach to supervision, AIs should apply the above guidance in a proportionate manner and in a way that is commensurate with the criticality of their cloud adoption and the potential impact that cloud computing may have on the AI's risk profile.

Should your institution have any questions about this circular, please contact Mr Ricky Liu on 2878 1458 or Mr Patrick Cheng on 2878 1660.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)