HONG KONG MONETARY AUTHORITY
香港金融管理局

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

31 August 2022

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Guidance on Cloud Computing

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 **Annex**, 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)

Annex

Guidance on Cloud Computing

Introduction

There has been a growing trend of authorized institutions (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. 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.

Detailed guidance

The HKMA's supervisory expectations on cloud computing, as detailed below, are developed with reference to the results of a round of on-site examinations focused on cloud computing undertaken by the HKMA between 2021 and 2022.

AIs should note that the below principles serve to complement, and should be read in conjunction with, relevant existing HKMA guidance, including 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.

I. Governance framework

1. **Maintaining an effective governance framework for cloud computing.** In line with TM-G-1, AIs should put in place an effective governance framework for cloud computing. The framework should enable AIs to: (i)

make an informed decision on whether a cloud strategy is appropriate for their circumstances, (ii) determine the specifics of a cloud strategy (e.g. the types of services to be hosted on the cloud, and the appropriate deployment model); and (iii) assess and manage the risks associated with cloud computing. AIs' Board of Directors (Board) should be ultimately responsible for approving the governance framework and for overseeing its implementation to ensure the safety and soundness of their institution's cloud operations. Senior management should implement the framework and provide regular and timely reports to the Board to facilitate the Board's oversight. The Board and senior management should regularly review the suitability and effectiveness of the governance framework.

2. **Conducting proper due diligence on CSPs before and during engagement.** AIs should establish a proper due diligence process to assess the capabilities and suitability of a CSP before the engagement and regularly during the engagement. Besides the general business aspects outlined in SA-2, AIs should ensure that cloud-specific considerations are taken into account during the assessment. Depending on the cloud deployment model adopted, these may include multi-tenancy risks, as well as those concerning concentration risk (the risk of over-reliance by an AI on the services of a single operator) and supply chain risks more generally. Where cloud workloads may be deployed across multiple geographical locations, AIs should conduct additional due diligence to assess the risks specific to the relevant overseas jurisdiction. In line with OR-2, AIs should also verify that engaging a given CSP will not reduce their level of operational resilience. In taking forward the above, AIs may adopt a risk-based approach and appropriately leverage on independent third-party assessment reports and pooled audit exercises on the CSPs, so long as the quality and comprehensiveness of the work undertaken by the independent third party meet the intended purpose and requirements.

II. On-going risk management and controls

3. **Understanding the institution's roles and responsibilities under the CSP agreement.** 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. This is particularly important with respect to CSPs engaged under the "shared responsibility model". Under this model, AIs typically bear the responsibility for "security in the cloud" (e.g. ensuring adequate encryption keys, and access and identity management) whereas the CSPs bear the responsibility for "security of the cloud" (e.g. underlying hardware and software security).

4. **Maintaining effective risk management procedures for cloud operations.** AIs should develop a comprehensive set of risk management procedures to enable them to continually identify, monitor and mitigate the specific risks posed by cloud computing. In addition to operational, cyber, and system resilience risks, AIs should stay alert to possible concentration risk particularly when delivering critical operations and vendor lock-in risk. In this connection, AIs should, following a risk-based approach, keep under regular review: (i) the possibility of cloud portability (i.e. their ability to move applications or data from one cloud service to another), (ii) the availability of interoperability solutions (i.e. the ability for one cloud service to interact with a customer's system or other cloud services by exchanging information), (iii) the feasibility of adopting a multi-cloud strategy, and (iv) whether viable exit strategies are in place to enable an orderly exit when needed, particularly under a stress scenario. Where a CSP may depend on third parties or suppliers in the discharge of their functions, AIs should take steps to manage the potential supply chain risks. AIs should also have procedures in place to gather on-going assurances that the CSP itself will properly manage risks and adhere to relevant industry standards.

5. **Adopting effective measures to protect information deployed to cloud.** AIs should have effective controls to ensure the security of their information assets and compliance with relevant statutory requirements regarding customer data confidentiality. To this end, AIs should implement layers of security control measures to protect the integrity and confidentiality of customer information stored in the cloud. These should include: (i) adequate identity and access management controls; (ii) clear and effective cryptographic key management policies, procedures and standards; (iii) adequate controls to ensure correct security configurations and cyber hygiene; (iv) effective cyber incident response and recovery management processes to ensure the on-going cyber resilience of the cloud; and (v) where relevant, adequate controls to ensure that a CSP sufficiently addresses the security and operational risks associated with multi-tenancy cloud architecture.

6. **Putting in place robust contingency plans.** AIs should develop viable and effective contingency plans to cope with situations involving a disruption of cloud computing services. These plans should be subject to regular drills and testing to prove that they are operable, with the involvement of the CSPs where feasible. Where AIs' critical operations are dependent on cloud-based platforms, they should also satisfy themselves that a disruption in cloud services will not impact their operational resilience. Any deficiencies identified in this regard should be addressed as soon as practicable. AIs should also have comprehensive understanding of their CSPs' resilience

capabilities, including their contingency plans and procedures, and to ensure that these plans and procedures are subject to regular and effective testing.

III. Protection of access and other legal rights

7. **Taking steps to guarantee audit rights and supervisory access.** AIs should put in place suitable arrangements to 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. They should regularly exercise their audit rights to obtain assurance on a CSP's risk management and security standards. As specified in SA-2, the HKMA expects AIs to ensure that appropriate and up-to-date records are kept available for inspection by the HKMA in accordance with Sections 55 and 56 of the Banking Ordinance, and that data retrieved from CSPs remain accurate and available in Hong Kong on a timely basis.

8. **Keeping clear and enforceable CSP agreements.** AIs should ensure that clear and enforceable CSP agreements are in place to protect their interests, risk management needs and ability to comply with supervisory expectations. The agreements should clearly set out the types and levels of services to be provided by the CSPs, as well as the liabilities and obligations of the CSPs. They should also contain clear provisions to address the specific issues associated with cloud computing[1]. AIs should regularly review the agreements and consider whether they need to be renegotiated and renewed to bring them in line with current market standards and to enable AIs to cope with emerging risks and changes in their business strategies.

IV. Risk management capabilities

9. **Ensuring responsible staff have necessary capabilities to oversee cloud operations.** AIs should provide regular training to staff overseeing cloud operations to equip them with the knowledge and skills required to securely

[1] These include, but are not limited to, provisions that provide for or ensure: (i) effective means to define, monitor and incentivise a CSP's business performance and risk management; (ii) the need for a CSP to establish viable and effective contingency plans to ensure the operational resilience of the AI, and where applicable, the need to conduct joint regular drills and BCP testing; (iii) the supervisory access of the HKMA; (iv) audit rights by both AIs and the HKMA on the CSPs; (v) effective vendor exit management, under both stressed and orderly scenarios; and (vi) that an AI has adequate monitoring of and/or control over sub-contracting. As part of this, AIs may consider, where appropriate, inserting a clause that mandates a CSP to notify them or seek approval or a "no objection" before proceeding with material changes to the sub-contracting arrangements. The relevant agreement should also include obligations of the CSP in ensuring confidentiality of the AI's information obtained by its agents and complying with the AI's relevant IT control policies and procedures.

use and manage the risks associated with cloud computing. The training should be provided to relevant staff across the three lines of defence and the level of training should be commensurate with the roles and functions of the staff.

The HKMA will review the above guidance from time to time, having regard to market developments relating to cloud computing. Should your institution have any questions about this guidance, please contact Mr Ricky Liu on 2878 1458 or Mr Patrick Cheng on 2878 1660.

Hong Kong Monetary Authority
August 2022