澳 門 金 融 管 理 局
AUTORIDADE MONETÁRIA DE MACAU

Circular No. 021/B/2023-DSB/AMCM
(Date: 28/12/2023)

Industry Guidance on Cloud Outsourcing Controls

With the rise of cloud computing technology, more authorized institutions in Macao have taken initiatives to explore the use of cloud computing services offered by external cloud service providers ("CSPs") in order to enhance their operations. While the adoption of cloud computing services offers advantages such as business agility, scalability and cost savings, risks and challenges arising from the adoption of cloud outsourcing arrangements ("Cloud Arrangements") should be properly identified, addressed and monitored.

This Industry Guidance on Cloud Outsourcing Controls (the "Industry Guidance") is supplementary to the AMCM's "Guideline on Outsourcing".

Introduction

1. The purpose of the Industry Guidance is to outline the AMCM's requirements on Cloud Arrangements and major prudential issues to be considered when entering into Cloud Arrangements.

2. Cloud computing services include a wide range of services that enable on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released.

3. Cloud computing services can be deployed in various models which come with different inherent risks and prudential issues to be considered. These service models and deployment models are described below:

   (a) Service models:

   - Software as a Service ("SaaS") – provides a full cloud-based application that is managed and hosted by the service provider.
   - Platform as a Service ("PaaS") – provides development and/or application platform services, such as database, application platform, file storage and collaboration to facilitate development, testing and deployment.
   - Infrastructure as a Service ("IaaS") – provides on-demand fundamental computing infrastructure services, such as computer, storage and network services.

   (b) Deployment models:

   - Public Cloud – The cloud infrastructure is made available to the public over the

internet and all the components of the cloud infrastructure are owned and managed by the CSP.

- Private Cloud – The cloud infrastructure is used exclusively by a single organisation. It can be managed and operated by the organisation or a third party and can be located on-premise or off-premise.
- Community Cloud – The cloud infrastructure is used exclusively by a specific community of organisations that have shared concerns (e.g. mission, security requirements, policies and compliance considerations). It could be managed and operated by one or more communities of organisations, a third party, or a combination of both. It can be located on-premise or off-premise.
- Hybrid Cloud – The cloud infrastructure is composed of two or more cloud deployment models described above (i.e. private, community or public) where each model reserves its unique entities and are bound together by standardized or proprietary technology that enables data and application portability. This combination allows users to take advantage of the benefits that each model has to offer (e.g. organisations can store confidential data on private cloud and operate other less sensitive functions on public cloud).

Applicability

4. This Industry Guidance applies to all authorized institutions incorporated in Macao and to the Macao branches of authorized institutions incorporated overseas. Where applicable, this Industry Guidance also applies to other financial institutions that are under the supervision of the AMCM (with the exception of institutions that transact insurance activities and/or manage private pension funds).

5. The Industry Guidance applies to all types of material Cloud Arrangements[1], including but not limited to, each of the service models and deployment models described in paragraphs 3(a) and 3(b) above, that involve material business activities / functions which align with the definition set out in the "Guideline on Outsourcing". This applies to instances where authorized institutions engage in outsourcing arrangements, either with a CSP offering the relevant material outsourcing services, or with a service provider that

[1] Some examples of material Cloud Arrangements are provided below:
(a) storage or processes of customer information or staff data including Personal Identifiable Information ("PII"), sensitive financial information (e.g. credit card, payroll, bank account), and any other data that may lead to a material impact on customers if such data is leaked;
(b) business operational systems, including core banking applications, financial transaction and trading systems;
(c) storage or processes of regulatory reporting, accounting data, or the other non-public commercial sensitive information that could influence financial markets;
(d) internal control function systems such as audit, risk management and compliance; and
(e) outsourced business activities as defined as critical by authorized institutions.

relies significantly on a CSP for the delivery of such services.

6. Because of the typical characteristics of cloud computing services, such as multi-tenancy, data commingling, high propensity for data storage and processes to be carried out in multiple locations, authorized institutions should establish additional controls to manage material Cloud Arrangements and associated risks in relation to data access, confidentiality, integrity, sovereignty, security, recoverability, regulatory compliance, and auditing.

7. Before entering into agreements of any material Cloud Arrangements, authorized institutions should consult and discuss their plans with the AMCM.

Governance

8. Authorized institutions should establish a governance framework (the "Framework") for cloud outsourcing which aligns with the authorized institutions' overall business, IT strategy and relevant internal policies and processes. Roles and responsibilities, authority, and ownership for managing Cloud Arrangements should be clearly defined in the Framework and communicated with the board, senior management, and other relevant parties involved in the management of the authorized institution. The board and senior management are responsible for periodically reviewing and approving the Framework to manage the associated risks in each of the components of Cloud Arrangements.

9. The Framework should include, at the minimum, the following components:
   (a) Planning stage including business requirements, risk assessment, due diligence and approval of new Cloud Arrangements;
   (b) Roles and responsibilities of personnel responsible for documenting, managing and monitoring of Cloud Arrangements within the authorized institution;
   (c) On-going monitoring and risk assessment procedures;
   (d) Data location and transfer requirements;
   (e) Cloud subscription and billing management;
   (f) Security controls;
   (g) Audits / review arrangements;
   (h) Business continuity management; and
   (i) Exit strategy.

10. Authorized institutions should establish a proper due diligence process for assessing the capabilities and suitability of a CSP before and during Cloud Arrangements. In addition to the requirements specified in the AMCM's "Guideline on Outsourcing," cloud-specific

considerations like multi-tenancy risks, concentration risks, and supply chain risks should be included in the assessment. In situations where cloud operations are deployed across multiple geographical locations, authorized institutions should conduct additional due diligence to assess the risks specific to the relevant overseas jurisdictions.

11. Authorized institutions should establish on-going monitoring and risk assessment procedures to identify, monitor and mitigate the associated risks of Cloud Arrangements. In addition to the operational, security and system resilience risks, authorized institutions should be aware of possible concentration risks, especially for critical operations. In this regard, authorized institutions should regularly review (i) the adequacy of contingency, including the interoperability and portability of data and services; (ii) the feasibility of adopting a multi-cloud strategy; (iii) the existence of exit strategies to facilitate a timely exit when necessary. Where a CSP may rely on third parties or suppliers to carry out its functions, authorized institutions should take appropriate measures to manage the potential supply chain risk. Authorized institutions should also have mechanisms in place to obtain on-going assurances that the CSP itself will manage risks appropriately and conform to applicable industry standards.

Data location and transfer

12. Authorized institutions should understand the relevant legal and regulatory requirements, contractual requirements and restrictions that apply to data handling before migrating systems and data to the cloud. Acceptable countries or jurisdictions for data processing and storage should be determined and agreed upon between authorized institutions and CSPs. Authorized institutions should retain a contractual right to reject the proposed changes or terminate the outsourcing agreement in the event of undesirable changes introduced by CSPs concerning the location of data stored. For Cloud Arrangements involving personal data transfer outside Macao, reference should be made to the Personal Data Protection Act "個人資料保護法" for specific notification, approval and control requirements.

Outsourcing agreements

13. Among the requirements set out in the AMCM's "Guideline on Outsourcing", agreements for Cloud Arrangements should also address the following matters:

    (a) Acceptable data centre location in supporting the authorized institution's data processing and storage;

    (b) Notification requirements for changes to data centre locations including notification timeline and approval procedure;

    (c) Obligations of the CSP to assist with providing response, investigation and recovery in the event of an incident; and

(d) Obligations of the CSP to assist with the exit process, including but not limited to conducting sufficient tests to ensure the smooth transition to the authorized institution's own environment or another CSP's cloud environment.

14. Given the nature of the cloud products, CSPs also offer the option of a consumption billing model (i.e. Pay As You Go) that charges based on authorized institutions' cloud usage. During the contractual negotiations, authorized institutions should agree with CSPs on the billing model, usage monitoring requirements and notification requirements over key services, including monitoring platforms and reporting periods. In any case, measures should be in place to prevent cessation of services based on quotas being exceeded.

Audit / review arrangements

15. External or internal audits over Cloud Arrangements should be conducted on a regular basis. The audit scope and frequency should be clearly defined, having considered the nature and extent of risks, and the impact on the authorized institution from the outsourcing arrangements. Third party certifications or equivalent reports are also acceptable if:

    (a) The party performing the audit possess the requisite knowledge and skills and is independent of the units or functions involved in providing or supporting Cloud Arrangements;

    (b) The scope of the audit reports should cover the CSP's systems and operations used to store or process the authorized institution's data.

16. Authorized institutions are responsible for following up with the CSP to ensure appropriate and timely remediation actions are taken to address any audit findings.

Additional key controls

17. To further address security risks associated with Cloud Arrangements, robust security controls should be implemented, including but not limited to those set out below under paragraphs 18 to 35. Depending on the service models deployed, authorized institutions may share the responsibilities with CSPs over the management and operation of security controls. For example, risks regarding network security are commonly managed by CSPs in the SaaS service model, while it might be a shared responsibility among authorized institutions and CSPs in the IaaS service model. Nevertheless, authorized institutions are held accountable for protecting their information. Therefore, authorized institutions should identify and implement appropriate controls where applicable in relation to their Cloud Arrangements.

(A) Architectural design

18. Authorized institutions should ensure the cloud's architectural design and its underlying infrastructure components are capable of providing a high level of security, availability, resiliency and performance. Authorized institutions should leverage available functionalities to enhance system resilience, such as auto-scaling. Authorized institutions should also implement resource health checks and real-time monitoring to detect service faults or outages in the cloud environment.

19. A proper network architecture should be designed to secure access control, taking into consideration common threats (e.g. DDoS attacks) and risks associated with cloud connectivity, logical segregation and public access. Where applicable, appropriate technologies should be adopted to enhance network isolation for multiple virtual networks and cloud accounts / segments, such as software-defined networks.

(B) Virtualization and containerization

20. Virtualization and containerization are the fundamental technologies used in cloud computing that enable a pool of resources to be deployed and scaled up / down more easily. Authorized institutions should define the security standards of implementing and utilising virtualization and containerization technologies in the cloud environment. The roles and responsibilities between authorized institutions and CSPs should be agreed upon and documented for operational references.

21. For any virtual machine or container images, a standard set of configurations should be designed and maintained by authorized institutions to standardize the level of security for any new instance created in the cloud environment. Access and authentication controls should be enforced in accessing or changing the configurations of virtual machines and container images.

(C) Data security and encryption

22. Authorized institutions should review the existing data classification policies to ensure they encompass considerations for the cloud environment. Additional security controls, such as advanced encryptions, tokenization, and logical segregation, should be considered by authorized institutions for any sensitive information stored or processed in the cloud environment.

23. To enhance the protection of sensitive information, both data-in-motion and data-at-rest encryption with advanced encryption algorithms should be implemented on sensitive information and any backup copies. Detailed policies and procedures should be in place to govern the cryptographic material lifecycle from generation, usage, renewal to disposal of cryptographic keys. Strong protective measures, such as access controls,

encryption, should also be implemented to protect the integrity of private keys and other cryptographic keys stored in the cloud environment.

24. Monitoring or surveillance controls should also be deployed to identify and alert of any unauthorized access or changes to sensitive information, for example, containing personal identifiable information ("PII") or payment related information. Additional data loss prevention controls, such as Cloud Access Security Broker ("CASB"), should be implemented if the cloud services are accessible via the internet.

25. Authorized institutions should obtain and validate independent assessment reports from CSPs, covering data centres that support the authorized institutions' business operations to ensure sufficient protection measures are implemented properly. Authorized institutions should ensure remediations are performed promptly by CSPs on any threats, risks or security issues identified in the independent assessment.

(D) Application security

26. Similar to any on-premise applications and related hosting arrangements, authorized institutions should review the existing System Development Life Cycle ("SDLC") process to ensure that cloud-specific security risks and mitigation strategies are incorporated in the different phases of the SDLC process. Security tests, such as penetration test and source code review, should be considered with reference to applicable regulatory requirements, industry best practices, or internal guidelines.

27. For applications hosted by CSPs (e.g. cloud application under the SaaS model), authorized institutions should also perform reviews on the security controls implemented by CSPs to secure cloud applications.

(E) Identity and access management

28. Identity and access management policies should be updated to incorporate measures for the cloud environment, covering user account management, access control and remote access. Authorized institutions should closely monitor trends and threats in the cloud environment, and conduct regular reviews to ensure that its identity and access policies and controls for the cloud environment remain robust with reference to industry best practices and standards.

29. User access controls should be consistently implemented to cloud services and functions such as the assignment of least privilege and segregation of duties. Changes in user access rights should be assessed and reviewed by a specific role owner or independent assurance functions. Where the CSP cloud environment (e.g. cloud management console) is accessible from the Internet, authorized institutions should implement strong

authentication controls such as multi-factor authentication, especially for privileged accounts access, and all user access to material business functions and activities involving sensitive or confidential data in order to reduce the risk of impersonation and unauthorized data access.

(F) Change and configuration management

30. A formal change management process should be established and agreed with the CSP to standardise the handling of program or configuration change, e.g., initiation of a change request, testing, fall-back, approval, reporting, and accountability. Change windows for patching and software releases should be clearly defined to avoid any unexpected service interruption. Audit trails for all changes should be kept for further review.

31. Authorized institutions should also establish baseline configurations for the cloud environment and review the baseline configurations periodically to ensure appropriateness. Alerts should be triggered for any detected deviations from the baseline configurations. Where possible, automatic solutions should be deployed to revert the cloud environment to the baseline configurations where strict enforcement of the baselines is required.

(G) Event and security incident management

32. Authorized institutions and CSPs should effectively monitor events of networks, infrastructure and applications to ensure the confidentiality, availability and integrity of the cloud environment. Authorized institutions should implement relevant processes and tools, such as Security Incident and Event Monitoring ("SIEM") tool, to automatically perform log consolidation and correlation analysis integrating with intelligence feeds.

33. Authorized institutions should establish a clear and effective incident response plan to ensure that security incidents are detected and responded to promptly in the cloud environment. Roles and responsibilities and notification path for incident responses should be agreed upon between the authorized institutions and CSPs; and should be documented in the incident response plan for operational references.

(H) Business continuity management

34. Authorized institutions should develop disaster recovery plans and procedures for information assets in the cloud environment and perform testing regularly (e.g. at least annually for material business activities and functions) in order to validate their effectiveness and completeness. For material business activities and functions, testing should be performed jointly with the CSP where possible to ensure that the services can be resumed shortly and fulfil the authorized institution's business recovery requirements.

Where material control deficiencies are identified during the tests, appropriate follow-up actions should be considered, reviewed and closely monitored by senior management, and reported to the board.

(I) Training

35. Authorized institutions should ensure the staff who oversee Cloud Arrangements to have the knowledge and skills necessary to execute their responsibilities. All relevant staff should undergo regular training to ensure their knowledge and skill remain current so as to ensure the cloud technology can be used securely and the associated risks are properly managed.

36. Authorized institutions should comply with this Industry Guidance as soon as practicable and within 12 months of the date of this Guidance.