Monetary Authority of Singapore
10 Shenton Way MAS Building Singapore 079117 Telephone: (65) 6225 5577 Facsimile: (65) 6229 9229

Circular No. MAS/TCRS/2021/03

1 June 2021

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

ADVISORY ON ADDRESSING THE TECHNOLOGY AND CYBER SECURITY RISKS ASSOCIATED WITH PUBLIC CLOUD ADOPTION

Public cloud services[1] are adopted by a growing number of financial institutions ("FIs") to meet their business and operational needs, especially with the accelerated pace of digital transformation during the COVID-19 pandemic. While public cloud services can bring benefits, FIs should be aware of and adequately address the attendant technology and cyber security risks. FIs should perform a comprehensive risk assessment as they plan for public cloud adoption and manage the risks identified appropriately.

2 This advisory highlights some of the more common key risks and control measures that FIs should consider before adopting public cloud services. This includes:

(i) Developing a public cloud risk management strategy that takes into consideration the unique characteristics of public cloud services;
(ii) Implementing strong controls in areas such as Identity and Access Management (IAM), cyber security, data protection and cryptographic key management;
(iii) Expanding the FI's cyber security operations to include security of public cloud workloads;
(iv) Managing cloud resilience, outsourcing, vendor lock-in and concentration risks; and
(v) Ensuring FI's staff have adequate skillset to manage public cloud workloads[2] and risks.

[1] Public cloud services are a combination of a business and delivery model that enables on-demand, public access to a shared pool of resources such as applications, servers, storage and network security.
[2] A cloud workload is a virtualised instance of a specific application code or service that can be run on cloud resource and supports a defined process. This may include virtual machines, databases, containers and applications.

3 This advisory should be read as supplementary information to the MAS notices and guidelines[3].

Unique Characteristics of Public Cloud Services

4 For most FIs, public cloud services represent a new form of computing that involves new ways of acquiring and managing computing resources. FIs should note that certain risks that arise from public cloud usage need to be managed differently from traditional on-premise IT infrastructure risks due to the unique characteristics of public cloud services. A key difference is that the management and configuration of public cloud services are commonly achieved through a cloud metastructure (see diagram 1), which centralises administration of public cloud resources and is remotely accessible, often through a web or command-line interface. Misconfigurations or poor cyber hygiene could result in unauthorised access to the cloud metastructure, which could compromise the security of information assets that FIs place in the public cloud.

Data	Data and information that are stored and processed in the cloud
Software	Application and the underlying services
Metastructure	Protocols and mechanisms that provide the interface between the infrastructure layer and the other layers
Infrastructure	Computing hardware, memory, network and storage

Diagram 1: Logical Model of Cloud Computing

5 Cloud Service Providers ("CSPs") typically provide public cloud services in these cloud service models: Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS") and Software-as-a-Service ("SaaS")[4]. FIs should be aware that responsibilities for the administration, cyber security, and resilience of applications, operating system, virtual network, data and cloud workloads differ across the models. For example, FIs will have more responsibilities in managing cloud workloads in IaaS as compared to PaaS and SaaS (See diagram 2).

[3] The MAS notices and guidelines include the Notice on Technology Risk Management (TRM), Notice on Cyber Hygiene, TRM Guidelines and Outsourcing Guidelines.

[4] "Infrastructure-as-a-Service" (IaaS) typically provides customers with IT infrastructure (e.g. servers and storage) over the Internet on a pay-per-use basis. "Platform-as-a-Service" (PaaS) typically supplies customers with an on-demand environment for developing, running and managing software applications over the Internet. "Software-as-a-Service" (SaaS) typically allows customers to connect to and use cloud-based applications over the Internet on a subscription basis.

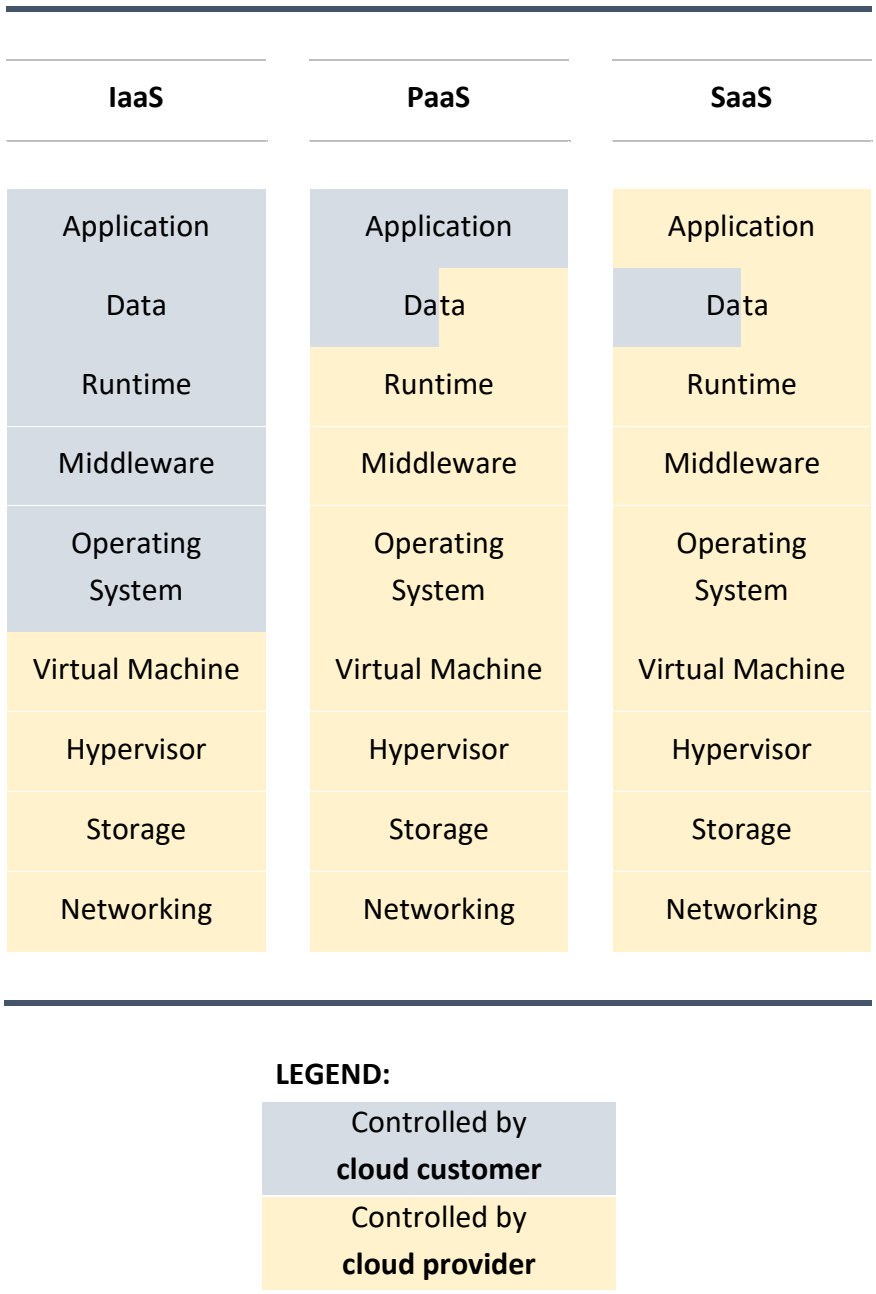

Diagram 2: Cloud Service Model [5]

6 FIs should establish a cloud risk management strategy that is tailored to their respective needs, taking into consideration the unique characteristics of public cloud services and the risks unique to each cloud service model.

[5] Source: NIST Special Publication 800-210 "General Access Control Guidance for Cloud Systems", National Institute of Standards and Technology, U.S. Department of Commerce, July 2020.

Shared Cyber Security Responsibilities

7 While CSPs are responsible for "Security-of-the-Cloud", FIs would be responsible for "Security-in-the-Cloud".

a) **"Security-of-the-Cloud"** refers to the security of the public cloud services under the CSPs' responsibility. In an IaaS or PaaS arrangement, these would typically include the security of the underlying hardware, system software and the hypervisor. For SaaS, this would also include the underlying security of the application software.

b) **"Security-in-the-Cloud"** refers to the security of the cloud workloads under the FIs' responsibility. In an IaaS or PaaS arrangement, these should typically include securing IT systems components such as applications, operating system and orchestration tools. In a SaaS arrangement, it would generally include managing user account privileges and data access rights.

8 FIs should be aware that while CSPs are responsible for "Security-of-the-Cloud", in some cases, FIs may have shared responsibilities for managing the controls implemented by the CSPs. For example, while a CSP may support data encryption using FI-managed encryption keys, FIs may be responsible for generating, transporting and protecting their own keys.

9 FIs are reminded to ensure that the cyber security responsibilities of all contracting parties are clearly delineated in their outsourcing agreement with CSPs. It has been observed that many public cloud security incidents globally (e.g. data leakage) were caused by poor management of "Security-in-the-Cloud" by public cloud users, such as insecure configuration of SaaS applications, and poor access control to the CSPs' cloud metastructure. FIs should be aware of their security responsibilities and undertake adequate measures to secure their workloads in the public cloud.

Identity and Access Management (IAM)

10 As IAM is the cornerstone of effective cloud security risk management, FIs should enforce the principle of "least privilege"[6] stringently when granting access to information assets in the public cloud.

11 FIs should implement multi-factor authentication (MFA) for staff with privileges to

[6] Access rights and system privileges are granted based on job responsibility and the necessity to have them to fulfil one's duties. No person by virtue of rank or position is given any intrinsic right to access confidential data, applications, system resources or facilities. Only personnel with proper authorisation are granted access to and use information assets.

configure public cloud services through the CSPs' metastructure, especially staff with top-level account privileges (e.g. known as the "root user" or "subscription owner" for some CSPs).

12 Credentials used by system/application services for authentication in the public cloud, such as "access keys", should be changed regularly. If the credentials are not used, they should be deleted immediately.

13 FIs that are integrating public cloud workloads with an on-premise authentication service should adopt prevailing best practices in securing such implementations to minimise contagion risk (e.g. security breach in on-premise environment could affect cloud workloads).

14 FIs using multiple public cloud services may need to centrally manage security policies over the use of different public cloud services and ensure that the policies are consistently enforced. FIs may consider adopting solutions such as Cloud Access Security Broker (CASB) or Secure Access Service Edge (SASE) to facilitate policy implementation, enforcement, and timely follow-up on non-compliance issues. CASB solutions manage connections between cloud users and CSPs to enforce security and compliance policies for public cloud services. SASE are solutions that combine networking and security services, which may include the capabilities of CASB, to enforce security and compliance policies for public cloud services.

Securing Applications in Public Cloud

15 FIs migrating legacy applications to the public cloud or adopting cloud-native approaches such as microservices architecture, containers and Application Programming Interfaces (APIs), should adopt prevailing best practices in the design, implementation, maintenance and operations of the public cloud workload. FIs should consider adopting zero-trust[7] principles in the architecture design, where access to public cloud services and resources is evaluated and granted on a per-request and need-to basis.

16 Where applications are developed for the public cloud environment, FIs are reminded to adopt appropriate Secure Software Development Life Cycle (SSDLC) processes, conduct robust threat modelling, and implement prevailing best practices in software security (e.g. using Open Web Application Security Project "OWASP" guides and frameworks). Should FIs use a continuous development-operations process ("DevOps"), security should be embedded throughout the Continuous Integration/Continuous Development (CI/CD) toolchain. FIs

[7] Zero trust is a cyber security paradigm focused on protecting information assets and computing resources by always evaluating each access request and not granting access based on implicit trust.

should adopt DevSecOps, which is the practice of automating and integrating IT operations, quality assurance and security practices in their software development process.

17 Microservice architecture are sometimes adopted when redesigning and implementing applications for the public cloud environment. When adopting a microservice architecture, FIs should recognise that such an architecture could potentially broaden the attack surface of an application in the public cloud, due to the increased deployment of APIs which could be targeted by threat actors. FIs should be aware that applications adopting microservices architectures have to be secured differently from the traditional defence-in-depth model of a typical web application architecture. Threats specific to microservices could include malicious insertion of rogue microservices, redirection of requests and API attacks. FIs should ensure that adequate security controls are in place, including, securing the service discovery mechanism, using service mesh[8] for fine-grain access control to APIs and implementing robust authentication for microservices.

18 When securing APIs, FIs should implement fine-grain access control and adopt the principle of least privilege i.e. strictly limit access to services to what is needed only, with the minimum level of privileges needed. FIs should also enforce robust IAM to authenticate service requests. FIs should not rely on implicit trusts when granting access (e.g. allow access based on the static IP addresses of requestor). For microservices, FIs should not assume that API security is sufficiently provided by API gateways or service mesh proxies, and should ensure that prevailing best practices in API security, including secure coding practices, are adopted in the implementation of APIs.

19 Applications that run in a public cloud environment may be packaged in containers, especially for applications adopting a microservices architecture. FIs should ensure that each container includes only the core software components needed by the application to reduce the attack surface. As containers typically share a host operating system, FIs should run containers with a similar risk profile together (e.g., based on the criticality of the service or the data that are processed) to minimise risk exposure. As security tools made for traditional on-premise IT infrastructure (e.g. vulnerability scanners) may not run effectively on containers, FIs should adopt container-specific security solution for preventing, detecting and responding to container-specific threats.

20 FIs should ensure stringent control over the granting of access to container orchestrators (e.g. Kubernetes), especially the use of the orchestrator administrative account, and the orchestrators' access to container images. To ensure that only secure container

[8] A service mesh is a configurable, dedicated infrastructure layer that facilitates and manages service-to-service communications using APIs.

images are used, a container registry could be established to facilitate tracking of container images that have met the FIs' security requirements.

Data Security and Cryptographic Key Management

21 FIs should implement appropriate data security measures to protect the confidentiality and integrity of sensitive data in the public cloud, taking into consideration data-at-rest, data-in-motion and data-in-use where applicable.

a) **For data-at-rest** i.e. data in cloud storage, FIs may implement additional measures e.g. data object encryption, file encryption or tokenisation[9] in addition to the encryption provided at the platform level.

b) **For data-in-motion** i.e. data that traverses to and from, and within the public cloud, FIs may implement session encryption or data object encryption in addition to the encryption provided at the platform level.

c) **For data-in-use** i.e. data that is being used or processed in the public cloud, FIs may implement confidential computing solutions if available from the CSPs. Confidential computing solutions protect data by isolating sensitive data in a protected, hardware-based computing enclave during processing.

22 FIs should consider adopting cryptographic key management strategies that accord them a high level of control and protection over cryptographic keys used for encrypting sensitive data. Two ways which FIs can retain greater control of the keys are "Bring-Your-Own-Key" (BYOK) and "Bring-Your-Own-Encryption" (BYOE). BYOK allows FIs to retain control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption. In BYOE, data is encrypted before it enters the cloud and the keys are not transferred to the cloud.

23 To secure cryptographic keys used for encrypting sensitive data, FI may consider generating, storing and managing the keys in a hardware security module (HSM) and hosting the HSM in an environment that the FI has a higher degree of control over (e.g. FI's own on-premise IT infrastructure) rather than with the CSP.

24 For cryptographic keys managed by CSPs, FIs should ensure that the CSPs' cryptographic key management policy, standards and procedures are adequate to protect the

[9] Tokenisation is the process of substituting a sensitive data element with a non-sensitive data element (a "token").

keys from unauthorised access, usage and disclosure throughout the cryptographic key management life cycle. This includes key generation, distribution, installation, renewal, revocation, recovery and expiry.

Immutable Workloads and Infrastructure-as-Code (IaC)

25 FIs may consider using immutable workloads[10] to ensure the security and stability of workload components especially during software upgrades or security patching. For immutable workloads, server instances are replaced with updated images instead of being changed. Should a server instance be compromised, it could be replaced with a clean image quickly. Testing should be performed on immutable workloads images to ensure that an image is secure and stable before implementing in the production environment.

26 FIs using Infrastructure-as-Code (IaC)[11] to provision or manage public cloud workloads should implement the necessary controls to minimise the risk of misconfiguration (e.g. by enforcing maker-checker), and avoid using both IaC and non-IaC approaches concurrently in order to reduce the complexity of the IT environment. FIs should also ensure that IaC configuration files are protected from unauthorised access and modification.

Cyber Security Operations

27 To maintain holistic cyber situational awareness of information assets, FIs should avoid performing security monitoring of on-premise applications or infrastructure, and public cloud workloads in silo. FIs should feed cyber-related information on public cloud workloads into their respective enterprise-wide IT security monitoring services to facilitate continuous monitoring and analysis of cyber events.

28 FIs should also ensure that their incident response, handling and investigation processes are adapted for public cloud workloads.

Cloud Resilience Risk Management

29 FIs should evaluate the track records of the CSP in maintaining the resiliency of its public cloud services to verify that they are commensurate with the FIs' business needs. Such evaluation should be performed prior to engaging the service of a CSP, and on a regular basis after engaging the CSP.

[10] Immutable workloads are cloud workloads where IT components are replaced rather than changed.
[11] Infrastructure-as-Code (IaC) is the process of provisioning or managing an IT environment (e.g., networks, virtual machines, load balancers) through machine readable definition files.

30 FIs should be aware that their cloud workloads are not resilient by virtue of being in the public cloud. For cloud workloads that require high availability, it is the FI's responsibility to ensure that the CSP has appropriate cloud redundancy or fault-tolerant capability (e.g. use of the auto-scaling feature to enable auto-recovery of failed services) and that the appropriate features are enabled for the cloud workloads. Cloud workloads could also be deployed in multiple geographically separated data centres (e.g. "zones" or "regions") to mitigate location-specific issues that may disrupt the delivery of public cloud services.

31 FIs should be proactive in monitoring the maintenance schedule, service disruptions, changes to services and end-of-life of services announced by the CSPs, such as via the CSPs' websites or through the cloud metastructure, so as to be able to take timely measures to ensure that FIs' systems remain available.

Outsourcing Due Diligence on CSPs

32 Some CSPs may offer FIs using public cloud services contractual terms and conditions that are tailored for the financial sector to enable the FIs to better meet their outsourcing due diligence, risk management and regulatory compliance needs. These terms and conditions may include the granting of audit and information access rights to FIs and their regulators for the purpose of performing outsourcing due diligence and carrying out supervisory reviews. In considering a cloud outsourcing arrangement, FIs should ensure that their ability to manage risk and meet regulatory requirements/expectations is not impeded by contractual terms and conditions.

33 FIs should ensure that independent audits and/or expert assessments of cloud outsourcing arrangements are conducted as part of their outsourcing due diligence and risk management:

a) FIs may adopt a risk-based approach in exercising the necessary due diligence, such as conducting direct audits on the CSP, or relying on one or more of the following: (i) "pooled audits" that are performed by independent and qualified auditors jointly engaged by the FIs or clients using the same cloud service; (ii) provision of reputable audit reports that evidence compliance with recognised risk management standards; and/or (iii) provision of reputable industry certifications for IT security, resiliency and services.

b) FIs should assess the adequacy of the assurance provided to ensure that the CSP is delivering the cloud service in line with the FIs' risk management and regulatory

compliance needs. For example, FIs are to verify that the scope of the audits and/or assessments is adequate for the cloud service model (IaaS, PaaS or SaaS) that the FIs are adopting. Contractual agreements should provision the rights for FIs to request the CSP to remedy the issues identified during the audits and/or assessments in a timely manner.

Vendor Lock-in and Concentration Risk Management

34 FIs should establish a process to assess their exposure to CSP lock-in and concentration risk. Such risk evaluation should be performed when FIs are planning to enter into an outsourcing arrangement with a CSP and re-performed periodically as part of the FIs' strategic planning, risk management and internal control review of the outsourcing arrangement.

35 To mitigate the risks of vendor lock-in, FIs may adopt cloud portability or interoperability solutions, and use open standards for data and software interfaces to facilitate redeployment of cloud workloads to an in-house IT infrastructure or public cloud infrastructure managed by another CSP. For cloud workloads that are critical to the FIs, exit strategies should be developed. The exit strategy could consider the pertinent risk indicators, exit triggers, exit scenarios, portability of the data and possible migration options.

36 To mitigate CSP concentration risks, FIs may consider implementing vendor diversity measures such as implementing a multi-cloud strategy[12]. However, FIs should be cognisant of the added complexity of operating in a multi-cloud environment, such as having adequate resources and appropriate expertise in securing and managing the use of different public cloud services and ensuring the consistent enforcement of policies.

Skillset

37 FIs should ensure that their cloud risk management strategy considers whether staff have the requisite expertise and experience to understand and manage the risks of public cloud adoption. In addition, as one CSP's metastructure typically differs from another, a staff with proficient skillset to manage a particular CSP's service may not be able to do so for another CSP. Hence, FIs should ensure staff have the necessary knowledge and skillset to manage the attendant technology and cyber risks for different cloud services which are used in their organisations.

[12] A multi-cloud strategy refers to the use of services from different CSPs.

Summary

38 FIs are ultimately responsible and accountable for maintaining effective oversight and governance of their engagement with CSPs for public cloud services. A risk-based approach should be taken to ensure that risk associated with the use of public cloud services are adequately addressed, and to ensure that the level of governance and controls are commensurate with the risks posed by public cloud services.

TOMMY TAN
DIRECTOR & HEAD (DIVISION I)
TECHNOLOGY AND CYBER RISK SUPERVISION DEPARTMENT