15 July 2022

To:
Bank Negara Malaysia
Submitted to: Atikah Adnan, Ahmad Rusdi Ahmad Sabri, Nur Aqilah Zulkafali

RE: ASIFMA response to BNM Exposure Draft on Appendix of RMIT: Cloud Technology Risk Assessment Guideline (CTRAG)

Dear Sir/Madam,

ASIFMA[1] is grateful for the opportunity to respond to the Bank Negara Malaysia ("BNM") Exposure Draft of a proposed Appendix to the Risk Management in Technology ("RMiT")[2] policy document on Cloud Technology Risk Assessment Guideline ("CTRAG").

Our members[3] are global firms with many of them rolling out global cloud migration projects. As Malaysia is a key market for many of our members, we are keen to work with you to ensure that global financial institutions ("FIs") can implement their global cloud strategies in the Malaysia to enable them and the Malaysian markets to benefit from all the advantages cloud can bring.

In what follows, we provide some overarching suggestions, followed by more detailed feedback on some of the articles in the draft CTRAG.

Legal Application
We suggest that the proposed risk and control measures outlined in the draft CTRAG serve as suggested guidance for FIs to consider on a risk-based approach and that the draft CTRAG are not mandatory requirements for FIs to adopt. We note that this approach would be similar to the existing control measures set out in Appendices 1 to 5 of the RMiT which currently serve as a guide for sound practices in defined areas and that FIs should be prepared to explain alternative risk management practices that depart from the control measures outlined in the Appendices and demonstrate their effectiveness in addressing the FIs technology risk exposure. As the new suggested CTRAG would come in the form of a new Appendix to the RMiT, we would like to confirm that the control measures outlined therein will also serve as a guide for FIs to be adopted on a risk-based basis.

---

[1] *ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.*

[2] *https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078*

[3] *https://www.asifma.org/membership/members/*

Principle and Risk-based Approach
Technology and public cloud adoption are fast evolving and adopting the CTRAG on a principled and risk-based basis, would allow FIs flexibility to adopt evolving control measures that best fit their risk profile and benefit from future developments and innovation. Listing examples or prescribing specific tools within the CTRAG could make the document outdated when new tools emerge. Moreover, we encourage referencing to existing BNM Outsourcing and RMiT Policy Documents where applicable to minimise overlaps. Examples include the sections on access to authoritative third-party certifications, log retention, exit strategy, and data loss prevention.

Taking a principle and risk-based approach would be in line with the Monetary of Authority Singapore's 2021 Advisory[4] that addresses the technology and cyber security risks associated with public cloud adoption. The advisory outlines non-mandatory risk management principles and best practice standards to guide FIs in Singapore in managing the risks of public cloud adoption.

Recognition of Financial Institutions group level cloud arrangement and strategy
Global FIs are moving applications onto public cloud at firm-wide level to enjoy the vast benefits cloud could offer on innovation, efficiency, flexibility, security, and resilience among others. We suggest BNM allows global FIs in Malaysia to leverage group-level public cloud strategies and frameworks to enable them to take advantage of all the benefits public cloud can bring, without creating fragmentation.

Internal cloud
We submit that the draft CTRAG should only be applicable to public cloud, and not internal cloud. It is common for FIs to adopt internal cloud, i.e., one shared "utility" affiliate entity centrally providing internal cloud to service affiliated banks, securities, asset management entities and other affiliated FIs across multiple jurisdictions in the same group. The use of internal cloud is simply an internal automation and streamlining of how an FI manages its own hardware and data centers, in order to increase flexibility and resilience, and, as such, it does not involve third-party infrastructure, nor does it increase cyber risk.

Please find below some detailed feedback and suggestions on some of the provisions in the Draft CTRAG. We hope that you find our feedback useful and that it will be positively considered and reflected in the CTRAG.

Draft CTRAG	**ASIFMA Comments**
A.1. Cloud risk management (a) A financial institution's board should promote sound governance principles throughout the cloud service lifecycle in line with the financial institution's risk appetite to ensure safety and soundness of the institution. (b) A financial institution's senior management should develop and implement a cloud risk management framework, for the Board's approval, proportionate to the materiality of	• We would like to confirm that the Cloud Risk Management included in CTRAG refers to existing third-party risk management framework. • Risks that come from the use of cloud should be treated as third-party risks. • The treatment of the risks that come with the use of cloud like other third-party risks is in line with the US Office of the Controller of the Currency's position, that

[4] *MAS (2021) https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Cloud-Advisory.pdf*

cloud adoption in its business strategy, to assist in the identification, monitoring and mitigating of risks arising from cloud adoption. (f) The use of cloud services may represent a paradigm shift in technology operation management as compared to on-premises IT infrastructure. Business processes may change and internal controls on compliance, business continuity, information and data security may be overlooked due to the ease of subscribing to cloud services. Therefore, the cloud risk management framework should also clearly articulate the accountability of the board and senior management and the process involved in approving and managing cloud service usage, including the responsibility of key functions across the enterprise in business, IT, finance, legal, compliance and audit, over the lifecycle of cloud service adoption.	is, that public cloud is a third-party relationship and third-party risk management for cloud computing is fundamentally the same as for other third-party relationships.[5] The same position is adopted by the Financial Stability Board in its 2019 "Third-party dependencies in cloud services" report.[6] The MAS also relies on its Outsourcing Supervisory Policy Manual[7] for various types of third-party outsourcing, including cloud. • Therefore, we would like to confirm that CTRAG does not require the FIs senior management to develop and implement an entirely new risk management framework for emerging technology like cloud, and allows FIs to leverage existing operational risk management, outsourcing, resilience, and cybersecurity framework. If gaps are identified, the existing operational risk management frameworks can be adapted to include new risks posed or existing risk associated with cloud adoption. For cyber risk management, we recommend that firms could leverage existing governance framework which includes third-party/dependency management. We recommend the Cyber Risk Institute Profile (also named as Financial Services Sector Cybersecurity Profile or FSP)[8] as a good framework governing cyber risk and also managing decency/third-party risks. The development of the cloud extension of the FSP can further help facilitate the management of risks.
A.2 Cloud usage policy (a) The senior management should develop and implement internal policies and procedures that articulate the criteria for permitting or prohibiting the hosting of information assets on cloud	• This statement assumes that cloud services present different risks than data centre outsourcing, which may not be the case. Instead, we suggest that the FI should be responsible for ensuring that

[5] https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html
[6] *See Section 2 on types of dependencies:* https://www.fsb.org/wp-content/uploads/P091219-2.pdf
[7] https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
[8] https://cyberriskinstitute.org/

services, commensurate with the level of criticality of the information asset and the capabilities of the financial institution to effectively manage the risks associated with the cloud arrangement. (b) A financial institution should maintain complete and centralised assets inventory of critical system and information assets hosted on the cloud services, with a clear assignment of ownership, and to be updated upon deployment and changes of IT assets to facilitate timely recalibration of cybersecurity posture in tandem with an evolving threat landscape. The full visibility and current view of the critical system and information assets should enable effective triaging, escalation and response to information security incidents.	cloud usage controls (security, technology, etc.) should correspond with the information asset. • For 2(b), in the existing RMiT document item 11.4, it has been explicitly mentioned that FIs are required to implement a centralised automated tracking system to manage its technology asset inventory which cloud falls under. Hence, a separate inventory is not necessary for cloud solutions. Therefore, we recommend removing section A.2.
A.3 Due diligence	
(d) Risk assessment should be promptly reviewed or re-performed upon material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislations and geopolitical development.	BNM's Outsourcing policy document defines "outsourcing risk" to include "country risk" that include risks described in A.3 (d). Therefore, we recommend CTRAG to refer to the BNM Outsourcing document and allow FIs to leverage existing risk assessment that include country risk dimension.
4. Access to authoritative third-party certifications A financial institution should review their cloud service providers' certifications prior to cloud adoption. At a minimum, a financial institution should: (a) Seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider`s action plans for mitigating any non-compliance; and (b) Obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. This should address requirements and guidance as stipulated in the Cloud Services section of the RMiT policy document and Outsourcing involving Cloud Services section in Outsourcing policy document.	Currently, BNM's Outsourcing document item 11.3 and RMIT item 10.51 cover third-party certification. We propose removing this section, and instead have a reference to these existing documents to minimise duplication.
A.5 Contract management 5 (b) The contract terms, obligations, and responsibilities of all contracting parties (this may	From a contractual arrangement perspective, an FI looks to the service provider for performance of all the obligations, responsibilities and liabilities, and where subcontractors are involved,

include sub-contractor(s) if the sub-contractor is material to the provision of critical function(s)) should be explicitly stated in the contract. At a minimum, the contract should address requirements and guidance as stipulated in Third-Party Service Provider Management sections of the RMiT policy document and related sections in the Outsourcing policy document (Outsourcing agreement and Protection of data confidentiality). (e) The provision of cloud services by the primary cloud service provider may interconnect with multiple layers of other fourth-party cloud service providers (sub-contractors), which could change rapidly. For example, customer data were leaked due to exposure made by fourth party. To mitigate fourth-party risks, financial institutions should:…	obligations are imposed on the service provider to correspondingly impose the obligations and responsibilities on the subcontractors. The service provider retains full responsibility for and oversight of those services that it has subcontracted, therefore it is not necessary to explicitly name the subcontractor in the contract with the service provider nor to ensure enforceability of the controls and the SLAs with the subcontractor. A service provider is required to carry out due diligence on its subcontractors and seek consent from the FI before the appointment of any material subcontractors and as such an FI would have the information on the subcontractor as well as the portion of material services which has been subcontracted by the service provider. In any event, an FI would have the right to terminate the contract if there is an adverse effect on services provided by the service provider, including the services provided by the subcontractor. Moreover, the FI does review the performance of the overall services on an ongoing basis, regardless of whether it is provided by the service provider or its subcontractors.
5(c) Jurisdiction risk may arise because cloud service providers operate regionally or globally in nature and may be subject to the laws and regulatory requirements of its home country, the location of incorporation, and the country where the client receives the service. Therefore, a financial institution should: i) identify and address potential jurisdiction risks by adopting appropriate mitigating measures, where practically possible, to ensure the use of cloud services does not impair its ability to comply with local law and regulatory requirements; ii) understand the scope of local customer protection legislation and regulatory requirements as well as to ensure that the financial institution's customers receive adequate protection and recourse in the event of a data breach by the cloud service provider; and iii) address requirements as stipulated in the Outsourcing policy document for outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia.	Cloud service providers ("CSPs") generally do not have insight into its' customer content or its' customer's decisions regarding the collection and use of the cloud services, and on very limited circumstances, a CSP employee can access customer content but it is only to provide technical support, where such access is temporary, audited and logged. As such, whilst an FI would identify the jurisdiction of where the services are provided from as well as the jurisdiction where the data would be stored at, the focus should be on the **contractual terms** between the CSP and the FI on **security measures**, instead of on FIs to understand the scope of local customer protection legislation and regulatory requirements. We suggest removing 5(c) as the RMiT and BNM Outsourcing document has sufficient requirements that FIs adopt security measures.

A.6 Oversight over cloud service provider A financial institution should ensure effective oversight over cloud service providers and the cloud service providers' sub-contractor(s). This includes, at a minimum, the following: (a) Establish and define a continuous monitoring mechanism with alignment to the enterprise vendor management framework (or equivalent) to ensure adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis; (b) Identify, assign and document the key responsibilities within the financial institution for continuous monitoring of cloud service providers to ensure accountabilities are clearly defined; and (c) Perform periodic assessments of the cloud service provider`s control environment, including business continuity management, to assess the potential impact on the financial institution's business resilience. This should address the requirements and guidance of Outsourcing involving Cloud Services section in Outsourcing policy document.	• The assessment requirement in Section C is covered by the Outsourcing document portion on assessment of service provider. We suggest removing Section C and reference to the Outsourcing document instead. • On Item 6A, an FI has the right to terminate for convenience by providing advance written notice or cease to use the services at any time.
1. Cloud architecture **(**a) A financial institution should design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application. (b) A financial institution is encouraged to adopt zero-trust principles to provide enhanced access control via micro-segmentation of application and infrastructure with "deny-by-default", "least privilege" access rights or on a 'need-to-have' basis. (c) A financial institution should continuously leverage enhanced cloud capabilities to improve the security of the cloud services, amongst others, financial institutions are encouraged to: i) use immutable infrastructure for deployment to reduce the risk of failure when new deployment of applications enter production by creating a new environment with the latest version of the software. The on-going monitoring of the cloud environment should include automating the detection of changes to	• We propose that BNM adopt a principle-based approach and not list examples like zero trust and immutability as there are many concepts and frameworks that are used by FIs to enhance security. • We recommend BNM to change Article 1 to the text below to keep principles-based requirements and remove prescriptive requirements. "**1. Cloud architecture** **(**a) A financial institution should design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application. (b) A financial institution is encouraged to provide enhanced access control via micro-segmentation of application and infrastructure with "deny-by-default", "least privilege" access rights or on a 'need-to-have' basis.

immutable infrastructure to combat evolving cyber-attacks; ii) use the latest network architecture approach such as Software-defined wide-area networking (SD-WAN) for managing and monitoring granular network security and centralised network provision in managing complexity of the cloud network environment; and iii) leverage available tools and services to enforce and monitor access control to cloud services. Examples of common tools and services include the use of Cloud Access Security Brokers (CASBs) or Secure Access Service Edge (SASE). (d) A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms. This includes the use of a network segregated from production networks for cloud migration and on-going administration of the management plane. (e) For financial institutions leveraging their financial group's cloud infrastructure, consider an appropriate level of network segregation (e.g., logical tenant isolation in the shared environment of the cloud) to mitigate the risk of cyber-attacks from propagating cross-border or cross-entity and affecting the Malaysian financial institution's operations. (f) The increasing use of application programming interfaces (API) to interconnect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface and any mismanagement may amplify the impact of an information security incident. A financial institution should ensure APIs are subject to rigorous management and control mechanism which include the following: i) APIs should be monitored under the financial institution's patch and end-of-life (EOL) management framework to minimise security vulnerabilities; ii) APIs should be tracked in the technology asset management and are de-commissioned on a timely basis when no longer in use; iii) APIs should be configured for secure communication with external application service providers with appropriate access controls;	(c) A financial institution should continuously leverage enhanced cloud capabilities to improve the security of the cloud services."

iv) APIs should be designed for service resilience to avoid the risk of single points of failure and included in the financial institution's business continuity arrangement; and v) APIs should be monitored against cyber-attacks with adequate incident response measures.	
B.2 Cloud application delivery models (a) A financial institution should review its risk management policies and practices should be reviewed at least once every three years to ensure effective oversight over the cloud application delivery model. (b) Cloud application delivery models may evolve to support faster time-to-market in response to consumer demand. Currently, DevOps and Continuous Integration / Continuous Development (CI/CD)7 are amongst the prevailing practices and processes for cloud application delivery. For instance, the ability to enforce segregation of duties for CI/CD where application developers may require access to the management plane for service configuration. A financial institution should ensure CI/CD pipelines are configured properly to enhance security of automated deployments and immutable infrastructure. (c) A financial institution is encouraged to adopt industry best practices such as Infrastructure as Code (IaC)8 to automate the provisioning of IT infrastructure in a consistent, scalable and secure manner. (d) Where relevant, a financial institution should implement appropriate controls on the IaC process to minimise the risk of misconfiguration and reduce the cyber- attack surface. This includes the following measures that should be taken by the financial institution: i) conduct vulnerabilities scanning on IaC, and ensure issues are remediated prior to the provisioning of IT infrastructure; (d) i) conduct vulnerabilities scanning on IaC, and ensure issues are remediated prior to the provisioning of IT infrastructure; (ii) enable audit logs for real-time monitoring and identification of cyber threats. The logs should be	• In Section d(ii), we submit that the industry practice for retaining audit logs for investigations and forensics purposes is 6 months. Three-year period retention is challenging and is out of step with current practice given the large volume of the logs. It might also create pushback from vendors. • Sections B and C should be principle-based and we propose BNM to not describe approaches as delivery models my evolve from time to time. FIs should be allowed to define their own control processes. • On "digitally signed" images, we recommend that BNM not prescribe solutions due to evolving technology. • Again, we recommend BNM to take a principle-based approach and change Article 2 to the following: "(a) A financial institution should review its risk management policies and practices should be reviewed at least once every three years to ensure effective oversight over the cloud application delivery model. (b) Cloud application delivery models may evolve to support faster time-to-market in response to consumer demand. (c) A financial institution is encouraged to adopt industry best practices to automate the provisioning of IT infrastructure in a consistent, scalable and secure manner."

retained for investigations and forensics purposes for at least three years; **(iii)** ensure virtual machine images (VMI) or container images of IaC templates are trusted and digitally signed; iv) implement appropriate access control to prevent unauthorised changes to IAC templates. iv) implement appropriate access control to prevent unauthorised changes to IAC templates.	
B.5 Cloud backup and recovery (c) A financial institution should ensure sufficient backup and recovery of virtual machine and container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following: i) ensure the capability to restore a virtual machine and container at point-in-time as per the business recovery objectives; ii) make virtual machine and container images available in a way that would allow the financial Institutions to replicate those images at alternate and recovery site ; and iii) allow virtual machine and container images to be downloaded and ported to new cloud service providers. (d) A financial institution should assess the resilience requirements of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. To ensure service availability, financial institution should consider a risk-based approach and progressively adopt one or more of the redundancy approaches, including diversifying away from a single CSP. Amongst the viable options are: iii) adopt hybrid cloud (combination of on-premises and public cloud setup); v) adopt multi-cloud strategy, with the use of services from different cloud service providers to mitigate concentration risks and geopolitical risks.	• We recommend removing (c) iii) "allow virtual machine and container images to be downloaded and ported to new cloud service providers." It is too prescriptive and need not be a definite method to ensure recoverability. Part (c) already lays out what the requirements are which is in summary to have sufficient backup and recovery of applications running in Cloud. (c) i) and ii) covers the requirement and methods that can be employed at general level sufficiently. • We would like to clarity that multi-cloud and hybrid cloud strategies are not resiliency solutions. We propose removing the section on multi-cloud and hybrid cloud. • Multi-cloud strategies are primarily adopted for accessing unique services across CSPs. While multi-cloud can reduce concentration risk to some extent, the technical, process and resource complexity needed to support multiple CSPs can lead to decreased resilience overall. In seeking to mitigate systemic risk, it is important that authorities avoid placing additional complexity or restrictions on an FIs ability to make commercial decisions and adapt to emerging business models and technologies, as some solutions to address industry-wide concentration risk currently proposed by authorities may limit the FIs ability to make commercial decisions and adapt to emerging business models and technologies.

	• We would also like to highlight that hybrid cloud is not a resilience solution either. Hybrid cloud suffers from similar drawbacks as multi-cloud when it comes to needs for resources and expertise. FIs adopts single cloud, multi-cloud or hybrid cloud based on its business and technology need and should not be forced to adopt one or other due to mis-perceived resilience benefits. • We therefore suggest that d(iii) and d(v) be removed, and suggest that FIs can adopt a risk-based approach which would provide them with flexibility based on their usage and technical needs. This should involve the choice to adopt multiple complementary solutions for resilience, rather than specific solutions being mandated for all.
B.6. Interoperability and portability Interoperability standards for cloud services continue to evolve such that porting data, related configuration and security logging across different cloud service providers may be challenging. To facilitate the smooth process of interoperability and portability between on-premise IT systems and alternate cloud service providers, financial institutions are encouraged to:…	• While we support greater efforts towards increased and improved interoperability and portability, it is important to ensure that multiple CSP approaches remain optional, depending on FIs' own business strategies, and does not become mandatory or considered as the ultimate solution for vendor lock-in and concentration risk, as there are currently inherent limitations without supporting more interoperability or resilience. • Some of the proposed requirements (around standardised network and communication protocols, common electronic data formats etc.) seem to be dependent on CSPs and are outside of the control of the FIs. Cross-CSP resiliency is not deemed feasible in the current environment due to the lack of this standardisation. Interoperability between CSPs is minimal, and it would limit either cloud usage overall or limit cloud usage to commonly available services (effectively stifling innovation and reducing the ability to derive business value from using CSPs).[9]

[9] *https://www.afme.eu/Publications/Reports/Details/detail/Building-Resilience-in-the-Cloud*

	• The concept of portability has significant technical limitations when seeking to utilise it as a primary mechanism for increasing resilience (particularly in a stressed exit from a CSP). Portability poses significant technical limitations and a loss of differentiated cloud benefits as a mechanism for increasing resilience. Challenges around portability include: a) technical complexity introduced into cloud environments; b) variation based on cloud service type (SaaS, PaaS, IaaS); c) loss of differentiated service benefits; and d) lack of comparable services to achieve portability. Also, in case of a potential CSP stressed exit a bank may have reduced or no access to its data, or limiting cloud-use to CSP foundational services only).[10] • If BNM's underlying concern is vendor lock-in for 6(a), we would propose for 6(a) to be amended to read as "mitigate vendor lock-in in the contractual agreement with the cloud service providers". We recognise interoperability and portability have been discussed at a global level, for example at the Financial Stability Board (FSB), in the context of concentration risk and there's yet an agreement on best and realistic approaches. We encourage BNM to join global dialogue and shape the dialogue and approaches to the issue, and refrain from mandating interoperability and portability.
B.7 Exit strategy (a) A financial institution should establish a robust cloud exit strategy as part of its cloud risk management framework to prepare for extreme adverse events such as the unplanned failure or termination of cloud service providers. The exit strategy should: …… i) be developed during the cloud deployment planning phase rather than on an ex-post basis; ii) identify alternative cloud service providers (multi-cloud approach) or third-party solutions to	• Refer to RMiT item 10.48 "A financial institution must ensure any critical system hosted by third-party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third-party service provider." We propose that BNM reference this high-level principle for exit strategy rather than prescribing the approach in CTRAG.

[10] https://www.afme.eu/Publications/Reports/Details/detail/Building-Resilience-in-the-Cloud

ensure no business recovery objectives disruption or vendor lock-in; iii) be properly documented including details on the various exit trigger scenarios, roles, responsibilities and sufficient resources to manage exit plans and the transition activities; and iv) be updated in a timely manner to reflect any material developments. **…**	• Overall, we recommend a risk-based approach that is proportionate to the inherent risk and criticality of the services being provided. Developing an exit plan should take into consideration criticality of workload and tolerance for disruptions.
B.8 Cryptographic Key Management (c) For critical systems hosted on the cloud, financial institutions should retain ownership and control of the encryption key (themselves or with an independent key custodian), independent from the cloud service provider, to minimise the risk of unauthorised access to the data hosted on the cloud. As example, this could be achieved by deploying the hardware security module (HSM) on-premises or by utilising HSM-as-a-service from a different cloud service provider. (d) Multiple encryption key management systems may add complexity and introduce new challenges of comprehensively maintaining and managing all the cryptographic keys as the usage would increase as cloud adoption increases. A financial institution should consider implementing a centralised key management system to unify key management and encryption policies for efficient scale operation	• Security is a shared responsibility between CSPs and FIs. • We recommend that BNM remove HSM as it is too prescriptive, and suggest BNM adopt a risk-based approach as opposed to an up-front strategy as this will allow FIs flexibility to strategise the key management policy according to the different CSP engagement, services and models. • We also submit that using the HSM service offered by a different CSP might not increase resilience and security. In both cases, the management of the cryptographic are not under the control of the FI. Moreover, if the HSM-as-a-service is a service that the primary CSP sub-outsourced, the FIs contract with the primary CSP may or may not apply to the sub-outsourcer. We suggest an alternative approach in which a security review/audit would be conducted on the cryptographic key management provided by the service provider (if any) and stated in the contractual agreement. • We also submit that a centralised key management system (especially if multiple CSPs are involved), would contribute to more complexity, complication, and establish a different single point of failure, this could affect the applications running on the multi-cloud environments at the same time.
9. Access Controls (d) Point-to-point connections with cloud services may proliferate with the ease of cloud adoption, resulting in fragmentation of identity and access	• Access controls is already covered in the RMiT and we recommend BNM make reference to the access control

management and the risk of unsanctioned data being migrated to the cloud. In view of this, rigorous planning is recommended for the design of identity and access management as it is inherently complex. Financial institutions are encouraged to: i) implement a federated11 approach for identity and access management to mitigate risks of identities in cloud services being disjointed from the internal identities, unauthorised access and to ease user access management; and ii) consider additional attributes in context-aware decisions for identity and access management such as geographical location of access to further mitigate the risks associated with remote access.	requirements in the existing RMiT document. • Point (d), items (i) and (ii) are prescriptive in nature and we recommend that BNM allows respective FIs the flexibility to implement controls based on risk assessment to address the concern highlighted in point (d).
10. Cybersecurity Operations	• We would like to highlight that security in cloud is a shared responsibility between FIs and CSPs and some requirements in Article 10 could be interpreted that FIs are expected to perform on behalf of CSPs in addition to their own responsibilities. For example, article 10 (b) requires an FI to manage VAPT for cloud services, which could be interpreted that an FI is responsible for CSPs' VAPT program. • We agree with BNM on segregation of responsibility in security management (article 10 (c) and recognise the importance of understanding the shared responsibility model as clearly defined roles and responsibility and common understanding is fundamental to FIs and the CSPs. • The financial sector developed the FSP Cloud Extension that provides guidance to FIs and CSPs on commonly understood responsibilities related to cloud deployment across software-as-a-service, platform-as-a-service, and infrastructure-as-a-service delivery models. It helps clarify where a firm's responsibilities end and a CSPs responsibilities begin. • We support a principle-based approach that allows FIs the flexibility to address ever-evolving cyber threat landscape. Prescriptive requirements may

	inadvertently limit FIs ability to leverage most advanced technology to defend against new cyber threat. • We would like to register that FIs' penetration testing should be risk-based and take into consideration system criticality and system's exposure to cyber risk. • We recommend BNM to keep principle-based guidance and remove prescriptive requirements under sub-bullets (a) (b) (c) and (d). Below is proposed revised text: "(a) A financial institution should ensure the governance and management of cybersecurity operations is extended to cover cloud services, with appropriate control measures to prevent, detect and respond to cyber incidents in the cloud environment to maintain the overall security posture of the institution. (b) The interconnected cloud service supply chain could become a source of cyber risk. (c) A financial institution should understand the segregation of responsibility in security management, which varies across the cloud service models. A financial institution should manage the sources of vulnerabilities appropriately. (d) A financial institution should review loss provision to ensure its adequacy to cover cyber incidents based on its scenario analysis of extreme adverse events."
11. Distributed Denial of Service (DDoS) (a) A financial institution should ensure the subscription of DDoS mitigation service is commensurate with the size and complexity of the cloud adoption. (b) The risk of a single point of failure (SPOF) may surface when a financial institution leverages solely on a cloud-based solution to mitigate DDoS attacks. As such, a financial institution is encouraged to engage alternative DDOS mitigation providers or establishing circuit	• DDOS is covered in RMiT, and we recommend BNM references to DDOS requirements in RMiT document that covers all outsourcing, including cloud. • The shared responsibility model also means that CSPs also have responsibility for DDOS that applies to them.

breakers to avoid service disruption when the main DDOS mitigation provider is disrupted.	
12. Data Loss Prevention (DLP) (a) A financial institution should ensure the DLP strategy and processes are extended to protect data hosted in cloud services, including the following: i) tailor control procedures and appropriate technologies to enforce DLP policies over the entire data lifecycle; and ii) manage the expansion of the endpoint footprint if the financial institution allow staff to use their own devices to connect to cloud services. (b) As it becomes increasingly easy to distribute digital content to customers via cloud services, a financial institution should adopt the appropriate digital rights management solution to preserve the confidentiality of its proprietary and customer information.	• DLP is covered in RMiT sections 11.14 – 11.16, and we recommend BNM references to DLP requirements in RMiT document. • We highly recommend the digital rights management (DRM) requirement to be removed to leave FIs the flexibility to implement based on risk-based assessment and practicality in implementing.
B.14 Cyber response and recovery (c) A financial institution should consider the following additional measures in the development of its CIRP: i) enhance its ability to detect security breach incidents to achieve effective incident management, including the ability to detect data leakage on the dark web; ii) provide adequate assistance to customers in the event of a security breach in view that the complexity of cloud arrangements and sophistication of cyber-attacks often exceed the response range reasonably expected of customers; and (f) For critical systems hosted on the cloud, a financial institution should establish arrangements with their cloud service providers to conduct annual cyber drills to test the effectiveness of the financial institution's CIRP.	We submit that the requirement to conduct annual cyber drills would place a disproportionate burden on the CSPs who would – as currently drafted – have to conduct annual cyber drills separately with each of their FI clients in Malaysia. Instead, we suggest that BNM can also help bring together FIs and CSPs in joint industry-level resilience exercises to evaluate how real-world scenarios would impact operations and recovery, which has already proven useful in some jurisdictions and at the global level, for example the GFMA Quantum Dawn exercises, the UK-US System Integrity Reconnection Exercise and the U.S. Treasury OCCIP Hamilton tabletop CSP Exercise for large FIs. Such exercises and testing would allow all concerned parties to better understand roles and responsibilities, identify any potential gaps in these relationships, increase collaboration and ultimately strengthen the resilience of the overall system. We also encourage BNM to actively participate in global discussions at FSB level and on best resilience exercises at industry and global level.

	In addition, we would like to again emphasise the importance of a principle-based approach to cybersecurity and recommend BNM only keep principle-based guidance.

We would welcome the opportunity for further engagement and remain at your disposal for any further questions you might have. Do not hesitate to reach out to us at lvanderloo@asifma.org or phone: +65 6622 5972.

Sincerely,

Laurence Van der Loo
Executive Director, Technology & Operations
Asia Securities Industry & Financial Markets Association