ASIA
INTERNET
COALITION

27 December 2018

Pengarah
Unit Pakar Risiko dan Penyeliaan IT
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: trsu@bnm.gov.my

Subject: Submission on Bank Negara Malaysia (BNM) - Risk Management in Technology (RMiT) Exposure Draft

---

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Bank Negara Malaysia (BNM) for the opportunity to provide comments on the Risk Management in Technology (RMiT) Exposure Draft, dated 4 September 2018.

AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure BNM that they will continue to actively contribute to the digital economy goals of Malaysia and support the rapid adoption of technology by the financial service institutions (FSIs).

We acknowledge the ultimate goal of this framework, i.e., to help financial institutions better manage technology-related risks and enhance technology resiliency. We also recognize the importance of cloud computing services that can help FSIs to reinvent and optimize their relationship with technology, quicken go-to-market access, automate and strengthen security, improve customer experience, and lower costs, compared to traditional IT models. We hope to bring that innovation and security empowerment capability to Malaysia's FSIs.

As such, please find appended to this letter detailed comments and recommendations, which we would like BNM to consider when reviewing the Exposure Draft. We are grateful to BNM for upholding a transparent, multi-stakeholder approach in developing the Risk Management in Technology Framework. We would greatly appreciate the opportunity to discuss our feedback in person at BNM's convenience.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Paine

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Before outlining the detailed recommendations below, we would like to highlight three main points for BNM's consideration.

1. **Aligning to Outsourcing Guidelines:** BNM issued the second exposure draft of its Outsourcing Guidelines on 20 September 2018. The Outsourcing Guidelines acknowledge that the use of cloud services provides business agility and allows FSIs to respond to customer needs and achieve economies of scale (Part A, Section 1.2), and provides an approval mechanism so that FSIs are able to enter into outsourcing agreement with Cloud Service Providers (CSPs). In direct contrast, section 10.76 of the RMiT states that "a financial institution shall not rely on public cloud computing services to manage, operate or host critical technology functions, systems and confidential information." If the RMiT were to come into effect as is, CSPs would effectively be barred from providing services to FSIs in Malaysia, as we believe the majority of workloads would fall into the definition in section 10.76. We also have concerns that this prohibition would extend to third party digital payments platforms, which would undermine Malaysia's efforts to drive financial inclusion.

   The Outsourcing Guidelines and RMiT Exposure Draft seem to embody two contradictory approaches to the use of cloud by FSIs. We are concerned that having two inconsistent policies issued from the same regulatory body will contribute to further uncertainty and confusion in the market and hinder the ability of FSIs to access the most cutting-edge innovations. We recommend aligning the RMiT to the principles embodied in the Outsourcing Guidelines to ensure that Malaysia's FSIs are able to take advantage of the innovative services and cost-saving features of the cloud, and do not fall behind peers in the region.

2. **Components of a Best Practice TRM:** We would like to briefly describe what we believe to be the components of a best practice Technology Risk Management (TRM) guideline, for BNM's consideration, and based on our experience across multiple countries. When drafting regulations and putting in place a regulatory framework to supervise its regulated entities, we believe regulators should take a "principles-based approach". Principles-based regulation means moving away from reliance on detailed, prescriptive rules and relying more on high-level, broadly stated rules, objectives or principles to set the standards by which FSIs must conduct business. These principles are then left to the FSIs to determine how to most appropriately implement them.

   A principles based approach is an outcome focused regulatory framework and recognizes that that an overly prescriptive approach to regulation (1) unnecessarily increases compliance costs, (2) increases the burden on regulators to constantly review and implement best practices (or else risk outdated controls), and (3) encourage a "check the box" focus, rather than a focus on implementing the best possible outcome. A prescriptive approach, on the other hand, which includes detailed and highly complex rules can divert attention away from the purpose of the regulatory framework by requiring FSIs to focus on adhering to the letter of the law.

   As a sub-set of principle-based approach is a "risk-based approach". The risk-based approach is a more modern approach to regulation that is not solely focused on technical compliance and enforcement, but a more purpose-driven and flexible approach that makes a range of mechanisms available to address common objectives of the regulator and the FSI. More detail around the benefits of a risk-based approach are included in **Appendix 1.**

We recognize regulators' legitimate interest in ensuring that their FSIs are not shifting their responsibilities to third parties in the performance of key business functions. To impose sound risk management practices on outsourcing arrangements, the most forward looking and flexible approach involves taking into account the nature of the risks involved, the types of services being outsourced and the materiality of such services to the FSI and its customers. This approach has been adopted by other prominent financial services regulators, including the Monetary Authority of Singapore[1] and Australian Prudential Regulation Authority[2].

3. **Security in a Multi-tenanted Environment:** We would like to address outright a common theme throughout the RMiT that multi-tenanted environments pose a greater security risk than using traditional IT solutions. Not only is security built into every layer of the cloud infrastructure, but also into each of the services available on that infrastructure. Each service provides extensive security features to enable customers to protect sensitive data and applications.

Enclosure

Detailed Comments and Recommendations on the Bank Negara Malaysia's Risk Management in Technology (RMiT) Exposure Draft are as follows:

[1] MAS Technology Risk Management Guidelines 2013

[2] APRA Prudential Practice Guide CPG 234 (Management of Security Risk in Information and Technology)

Section	Issue	Comments	Recommendation
Section 4.2	A 5-year review cycle would not be prudent.	Technology is changing rapidly as are cyber threats and vulnerabilities. A 5-year review cycle could have a significant negative impact on the ability of Malaysian financial institutions to keep up with the changing times and technology.	We recommend that BNM reduce the review cycle to 2 years.
Section 5 (Definition of Critical System)	The definition of "critical system" varies from that of "material outsourcing arrangement"	The ambiguity between the two draft regulations could make it difficult for financial institutions to comply.	We recommend that BNM amend the definition of "critical system" to match the definition of "material" in the outsourcing guidelines. Specifically, we recommend the following definition of "critical system": "Application systems that involve an activity integral to the provision of a financial service by the financial institution, and in the event of a service failure, security breach, unauthorized access or disclosure, has the potential to significantly impact a financial institution's business operations, financial position, reputation, and compliance with applicable laws and regulatory requirements."
Section 5 (definition of "Eligible issuer of e-money")	The definition of "financial institution" does not align with the definition used in the	For consistency and to reduce ambiguity, the definition of "financial institution" should be amended to match the definition used in the Interoperable Credit Transfer Framework.	For consistency and to reduce ambiguity, the definition of "financial institution" should be amended to match the definition used in the Interoperable Credit Transfer Framework: "Financial institution" means a banking institution, an approved issuer of a designated

	Interoperable Credit Transfer Framework		payment instrument and a registered merchant acquirer.
Section 5- Question 3: (What would be the key challenges for smaller financial institutions and the locally incorporated foreign institutions which rely on the Group for IT support and services, to comply with the requirements in this exposure draft?)	Smaller financial institutions who are not able to use public cloud services would be at a potential handicap in that they would not be able to take advantage of the investment made by large cloud providers in security. This could create security risks for such institutions. Locally incorporated foreign institutions that rely on the Group for IT support and services would need to duplicate infrastructure efforts, creating additional attack surfaces and related security risks. Small or newly established FSIs don't have large capital resources or the deep experience needed to build, maintain, and defend a complex IT system. Without scalable technology partners, such as cloud service providers, they may be exposed to security risks during their start up and early operation phase. What's more, from a business perspective, small or newly established financial institutions rely on cloud technology to quickly grow and scale. Without scalable technology partners such as cloud service providers, they may struggle to create and build financial services or to expand and grow regionally.		
Section 5- Question 4 (Is the definition of "public cloud" sufficient to include public cloud services	Public cloud technology has not proven less secure from a contagion risk perspective. Public cloud service providers designed the infrastructure to be multi-tenant by default with appropriate security measures in place to address contagion risks. Taken together, these measures further improve the security posture of the system overall, providing enhanced security capabilities. These measures include: • Architecting for multi-tenancy with logical segregation and strengthened common services • Data encryption at rest and in transit • Controlled change management		

where the risk of contagion arising from multi-tenanted environment is more pervasive such as Amazon Web Services, Microsoft Azure and Google Cloud?)	• Transparency/auditability of administrative access • Virtual private cloud (VPC) • Third-party assessments		
Section 10.9	A financial institution is also encouraged to consider diversity in technology to obtain greater resiliency, which may include use of different technology architecture design and application as well as technology platforms and network infrastructure to ensure the critical infrastructure are not exposed to similar technology risk.	It is unclear how FSIs will comply with this requirement nor the security objective it is meant to meet. One of the bedrock principles for cloud services is the avoidance of single points of failure in underlying physical infrastructure. This motivates building software and systems that use multiple zones and are resilient to failure of a single zone. Similarly, systems are built to be resilient to failure of a single compute node, single storage volume, or single instance of a database. Unlike virtually every other technology infrastructure provider, the regions served by CSPs has multiple Availability Zones and data centers. This entails data centers with significant excess bandwidth connections, so if a major disruption occurs; there is sufficient capacity to enable traffic to be load-balanced to the remaining sites, minimizing the impact on customers. There are customers who start off believing that they are going to split their workloads in the cloud amongst	Remove or modify this requirement as it will unnecessarily impede the adoption of cloud computing and increase the cost of business to FSIs.

		multiple technology platforms. But when they get to the practicality and the rigor of assessing it, very few end up going down that route. Most end up picking one provider. The reasons are as follows: ● This forces customers to standardize to the lowest common denominator, because these platforms are at widely different levels of maturity at this point. With this requirement, customers will be forced to go with a technology platform not based on security capabilities but just to meet compliance requirements. ● It is not cost effective to maintain resources and development teams who are fluent with multiple technology platforms which do the same things.	
Section 10.12	A financial institution shall conduct comprehensive source code review independent of development, prior to introduction of or material changes to critical systems, to ensure the accuracy of system design and functionality, and to	Source code is proprietary intellectual property (IP) and highly confidential. We do not disclose source code to any external parties. Requirements to compel organizations to divulge their intellectual property without binding assurances that their IP will be protected will inhibit industries and innovators from bringing the best technologies and practices to Malaysia. For-profit organizations rely upon proprietary IP, including source code, to ensure business success. Third party software vendors would typically conduct audits of their Software Development Life Cycle and	We recommend changing the wording here to: "A financial institution shall conduct comprehensive source code review independent of development, prior to introduction of or material changes to critical systems, to ensure the accuracy of system design and functionality, and to identify any security vulnerabilities. Where third party software is used, leverage provided independent audit reports to determine if the service provider's Software Development Life Cycle and Change Management processes are sufficiently robust."

	identify any security vulnerabilities.	Change Management processes to ensure that it is sufficiently robust. They would also provide independent assurance / audit reports to assure their customers. We recommend that financial service customers leverage these audit / assurance reports to conduct their due diligence.	
Section 10.13 A financial institution must ensure up-to-date source code continues to be readily accessible in the event of discontinued product support or insolvency of the vendor.	The review of source code may not be feasible in certain technology use cases. In the case of Software as a Service, the service provider's source code is generally proprietary and confidential.		We recommend that BNM amend this requirement to clarify that source code reviews are optional and should be considered appropriate at the financial institution's discretion. Specifically, we recommend that BNM strike the second sentence of 10.13 ("A financial institution must ensure up-to-date source code continues to be readily accessible in the event of discontinued product support or insolvency of the vendor.")
Section 10.15	Physical segregation should not be mandated for systems. A financial institution shall establish three physically segregated environments between production, development and	It would not be cost effective or logical to require physical separation. Logical separation would be an adequate control for both critical and non-critical systems. Logical separation has significant technological controls in place to ensure data is not co-mingled. In addition, certain services may also have encryption at rest and full disk encryption. These controls should be sufficient. Financial institutions may struggle to implement this section if mandated, and the costs associated with the	We recommend that BNM remove the requirement for physical separation and replace it with a logical separation requirement.

	testing for critical systems. Where facilities do not allow for this, logical separation of development and testing environment is allowed only for non-critical systems.	physical separation may outweigh the perceived benefits. CSPs provide multi-tenant services with industry-leading tenant separation security. This logical separation between customer environments provides more effective and more reliable security as that of dedicated physical infrastructure. For systems that are accessible over a network or the Internet, physical separation of those systems, such as placing them in a locked cage or a separate data center facility, does not provide added security or control over access. Simply put, all access controls for connected systems are managed via logical access controls, permission management, network traffic routing and encryption. CSPs address any physical separation concerns through the logical security capabilities provided to all of their customers and the security controls they have in place to protect customer data. Smaller, physically separated environments don’t have parity with generally-available cloud environments; hence any physical separation requirement can limit or delay a customer’s ability to leverage innovative investments (including security feature innovations) made on behalf of all customers using CSP services. Disadvantages also include higher cost structure and lower utilization resulting from less efficient use of space as well as limited redundancy options and	

		features compared with the geo-diversity of commercial data center regions.	
Section 10.16 (first sentence)	The maintenance of systems and infrastructure is generally managed by a cloud service provider. Any review or approval of such changes would not be feasible if required of a cloud provider.	The systems and infrastructure are shared resources and major and or emergency patching cannot be held up due to a customer not having approved such maintenance. If approvals or notifications were required, this could cause significant security risks to all users of the infrastructure given the delays in conducting the maintenance work. Cloud service providers expend significant financial and human resources to monitor, maintain and patch their systems and infrastructure.	We recommend that BNM clarify that the requirement for review and approval does not apply in cases where the financial institution has outsourced the system
Section 10.17	As with section 10.16, verifying the changes to systems and infrastructure is not feasible	The systems and infrastructure are shared resources and major and/or emergency patching cannot be held up due to a customer having to verify the maintenance. If verification were required this could cause significant security risks to all users of the infrastructure given the delays in conducting the maintenance work.	We recommend that BNM clarify that this section does not apply in cases where the financial institution has outsourced the system
Section 10.20	Certain outsourced services – such as a SaaS-based cloud computing services – will not allow for a	SaaS-based services are fully managed according to a shared responsibility model. If a financial institution was to manage their own key, it would add a considerable amount of workload and risk.	We recommend that BNM clarify that the principles proposed are only for situations where the financial institution manages and controls the encryption keys.

	customer to manage or supply their own encryption key. Therefore, financial institutions should rely on ISO certifications and SOC reports to ensure a vendor uses appropriate controls and processes to manage encryption keys.		
Section 10.20- Question 8 What is your institution’s current practice to ensure consistent standards are applied with regards to key management and adoption of cryptographic protocols?	Cloud service providers have robust controls and practices in place to manage and adopt cryptographic protocols. Cryptographic controls are tested and audited in both ISO certifications and SOC-2 reporting. Financial institutions can gain significant improvements in security by leveraging the robust management and adoption of cryptographic protocols by cloud service providers. Financial institutions should review information provided by cloud service providers and other outsourcing providers regarding how the provider manages and adopts cryptographic controls.		
Section 10.27	Cryptographic technology is evolving at a rapid		We recommend that BNM adopt a principles-based approach and replace the term

	pace. For example, service providers may use key management services instead of hardware security modules.		"cryptographic device” with "secure processing environment.”
Section 10.28	A fully automated key management system will be extremely onerous and resource intensive for a financial institution to maintain.		We recommend that BNM strike this requirement.
Section 10.30 (Key generation must be secured on premises and not shared with third parties.)	This restriction would prevent Malaysian financial institutions from adopting many cloud-based technologies, including CRMs, Office Productivity Tools, HR Platforms, Accounting Platforms and many other SaaS and PaaS services	If this requirement were to be implemented, all presently used tools would need to be replaced with those that generate keys at a financial institution’s premises	We recommend that BNM strike the requirement that key generation must be secured on premises and not shared with third parties.

Section 10.33(b) "Keys are stored in temper resistant cryptographic vault, such as a hardware security module (HSM)."	Not all devices have hardware security modules or "vaults" to store keys.	This requirement could preclude payments systems from working on mid-tier and low-end devices, which would likely not have such vaults. It could thereby detract from BNM's efforts to promote financial inclusion.	We recommend that BNM remove this requirement.
Section 10.39	Uptime Institute Standards such as Tier III are not considered as industry standard.	Many hyper-scale cloud service providers (let alone smaller independents) eschew this certification, as it's not seen as industry standard. A requirement mandaring Tier III risks precluding usage of many robust cloud infrastructures.	We recommend that BNM remove this requirement.
Section 10.44	A financial institution operating its production data centers on shared third-party facilities must ensure the following: (a) Dedicated secured space with proper caging for its server and equipment racks; (b) For shared critical power equipment, clearly	CSPs provides multi-tenant services with industry-leading tenant separation security. This logical separation between customer environments provided by a CSP provides more effective and reliable security as that of dedicated physical infrastructure. For systems that are accessible over a network or the Internet, physical separation of those systems, such as placing them in a locked cage or a separate data center facility, does not provide added security or control over access. Simply put, all access controls for connected systems is managed via logical access controls, permission management, network traffic routing and encryption.	We recommend that BNM remove this requirement.

	document the arrangement for power allocation between tenants in the service level agreements including prioritization given to the financial institution during power outages; and (c) Adequate power capacity and physical space are available for future technology system expansion.		
Section Section 10.44(b)	Data centers with multiple tenants will not be able to prioritize an individual customer during power outages.	A power outage affects all customers of a co-location or public cloud infrastructure.	We recommend that BNM strike the requirement in 10.44(b) that the "prioritisation given to the financial institution during power outages" be documented.
Section 10.45	A financial institution is required to appoint a technically competent external service provider to carry out regular	The CSPs tend to provide threat and vulnerability reviews of data centers. These reviews are in addition to an initial environmental and geographic assessment of a site performed prior to building or leasing. The quarterly reviews are validated by independent third-party auditors during our SOC, PCI, and ISO assessments. Customers can leverage these audit	We recommend changing the wording here to: "A financial institution is required to appoint a technically competent external service provider to carry out regular production data centre resiliency and risk assessment (DCRA) and set proportionate controls aligned with its enterprise risk appetite. The assessment must consider all

	production data center resiliency and risk assessment (DCRA) and set proportionate controls aligned with its enterprise risk appetite. The assessment must consider all major risks and determine its current level of resiliency.	assessments to conduct their due diligence prior to using cloud services.	major risks and determine its current level of resiliency. If this is not possible, the financial institution should rely on independent third-party assurance reports provided by service provider to conduct their due diligence to ensure that similar risk assessments have been covered."
Section 10.47	A financial institution operating its data centers on shared facilities should ensure the service provider does not host more than 30% of all financial institutions within a single facility to mitigate concentration risk. The guidance of no more than 30% of resources being on a service provider is not feasible or	It is not clear how FSIs or CSPs can comply with this requirement as CSPs would be breaching customer confidentiality, if they were to disclose their current set of customers. If mandated this could mean financial institutions in Malaysia would need at least four facilities to mitigate concentration risk, a significant strain on resources. The security objective which needs to be met here is the avoidance of a single point of failure. One of the principles for CSPs service design is the avoidance of single points of failure in underlying physical infrastructure. This involves building software and systems that use multiple Availability Zones and are resilient to failure of a single zone. Such systems are	We recommend that BNM strike this requirement and replace with rounded, principles-based approaches.

	realistic in certain architectures.	built to be resilient to failure of a single compute node, single storage volume, or single instance of a database. Unlike virtually every other technology infrastructure provider, the CSPs have multiple Availability Zones and data centers. This entails data centers with significant excess bandwidth connections, so if a major disruption occurs; there is sufficient capacity to enable traffic to be load-balanced to the remaining sites, minimizing the impact on customers.	
Section 10.49(a)	A financial institution must establish real-time application and infrastructure monitoring systems to track capacity utilization and performance of key processes and services. This monitoring system shall: (a) Run independently from production services;	It is not clear what is meant by "run independently from production services" and the security objectives this is meant to achieve. Specifically, for cloud services, would the monitoring services provided by a CSP to customers be considered separate from production services, even if they are running production workloads on a CSP platform?	We recommend changing the wording here to: "A financial institution must establish real-time application and infrastructure monitoring systems to track capacity utilization and performance of key processes and services.
Section 10.55	As currently written, this section would require system		We recommend that BNM adopt a yearly downtime budget of 24 hours, with a max outage duration of 4 hours.

	operators to massively increase redundancy, completely change how site reliability engineers respond to outages, and rewrite large sections of the software stack.		
Section 10.66	A financial institution should establish dedicated switches for critical systems separate from the general technology environment of the entity.	The CSPs provide multi-tenant services with industry-leading tenant separation security. This logical separation between customer environments provides more effective and more reliable security as that of dedicated physical infrastructure. For systems that are accessible over a network or the Internet, physical separation of those systems, such as placing them in a locked cage or a separate data center facility, does not provide added security or control over access. Simply put, all access controls for connected systems is managed via logical access controls, permission management, network traffic routing and encryption. Smaller, physically separated environments don’t have parity with generally-available cloud environments; hence any physical separation requirement can limit or delay a customer’s ability to leverage innovative investments (including security feature innovations) made on behalf of all customers using CSP services. Disadvantages also include higher cost structure and lower utilization resulting from less efficient use of	We recommend removing this requirement.

		space as well as limited redundancy options and features compared with the geo-diversity of commercial data center regions.	
Section 10.70(b)	A financial institution must establish service-level agreement (SLA) when engaging third party service providers. At the minimum, the SLA shall contain the following: (b) Any material changes that may affect a financial institution's outsourced functions and any sub-contracting of critical work must obtain approval from the financial institution;	Hyperscale CSPs offer the same self-serve services to all of their customers at scale. Because of this, hyperscale CSPs are not in a position to offer any individual customer the ability to approve or reject a subcontractor appointment which could potentially impact the rollout or provision of the service offerings provided to all of their customer base. Hyperscale CSPs, needs to be able to operate its business at scale without individual customers having the ability to control decisions that could affect the provision of services to all customers. We recognize that the two primary concerns that financial services regulators around the world have in relation to subcontractors used by outsourcing service providers are: (a) to ensure that the service provider should remain responsible to the FSI if it chooses to use subcontractors to provide a part of the services and (b) that the FSI should be given sufficient transparency in the use of subcontractors that have a significant impact on the delivery of the outsourced services. To address these concerns, CSPs, for example, provide prior notice of subcontractors that perform a fundamental role in the provision of the services on its website and offers customers the right to move their	We recommend removing the requirement for the financial institution to approve subcontracting of critical work. BNM can instead rely on the notice requirement set out in subsection (c) of Section 10.70.

		content to an alternative CSPs region or to terminate their services with no penalty.	
Section 10.70(d)	A financial institution must establish service-level agreement (SLA) when engaging third party service providers. At the minimum, the SLA shall contain the following: (d) Written undertaking on compliance with secrecy provisions as provided by the relevant legislation;	It is inappropriate to require CSPs to provide a "written undertaking on compliance with secrecy provisions as provided by the relevant legislation" and we therefore recommend removing this requirement or clarifying that such undertaking is applicable only to the FSI.	We therefore recommend removing this requiremen or clarifying that such undertaking is applicable onl to the FSI.
Section 10.74	A financial institution must ensure that storage of its data is clearly segregated from the other clients of the third party service provider. There shall be proper control and periodic review of		We recommend that BNM clarify that logical separation is sufficient to meet the requirement that "storage of [the financial institution's] data is clearly segregated from the other clients of the third party service provider"

	the access provided to authorized users.		
Section 10.76	As currently written, the draft does not specify which specific workloads are to be excluded from highly-secure public cloud computing services. Definitions of "critical technology functions and systems" could be interpreted very broadly, preventing institutions from using the most advanced, secure technology solutions.	Technology systems evolve and improve over time to handle different challenges. Set definitions of terms like "public cloud" run the risk of preventing financial institutions from adjusting their technical capabilities and adopting a risk-based approach when choosing how to manage information and systems. Instead of set definitions, financial institutions should be allowed to adjust their technical capabilities and adopt a risk-based approach when choosing how to manage information and systems.	We recommend that BNM replace "A financial institution shall not rely on public cloud computing services to manage, operate or host critical technology functions, systems and confidential information." with "A financial institution should use a risk-based approach to manage, operate, and host critical systems."
Section 10.76	A financial institution shall not rely on public cloud computing services to manage, operate or host critical technology functions, systems and	If the RMiT were to come into effect with this language in place, CSPs would effectively be barred from providing services to FSIs in Malaysia. The definition of "confidential information" or "sensitive data" in 5.2 of the Guideline encompasses the majority of data that a FSI may choose to deploy using a CSP, and limits the use of cloud computing services to low value, margin use-cases. In addition, the definition of "critical system" in Section 5 is broad to the point where FSIs will be straitjacketed into only using cloud for the most	We recommend removing the requirement.

	confidential information.	minimal and low-value use cases, undermining the value proposition of hyper-scale cloud computing. This is in direct contrast to the principles of BNM’s draft Outsourcing Guidelines which acknowledge that the use of cloud services provides business agility and allows FSIs to respond to customer needs and achieve economies of scale (Part A, Section 1.2), and provides a risk-based approval mechanism so that FSIs are able to enter into outsourcing agreement with CSPs.	
Section 10.76	Regarding the definition of a Critical System, Section 10.76 of the RMiT states that “a financial institution shall not rely on public cloud computing services to manage, operate or host critical technology functions, systems and confidential information.”	If the RMiT were to come into effect as is, CSPs would effectively be barred from providing services to FSIs in Malaysia, as we believe the majority of workloads would fall into the definition in section 10.76.	Instead of the broad categories included under “critical system” as defined in Section 5 of the RMiT, we recommend the following language for the definition of a critical system: *“Critical system is: one in which, as determined by the financial institution, if disrupted could result in an extreme impact on the financial and reputational standing of the financial institution or potentially threaten the ongoing ability of the financial institution to meet its material obligations under applicable Malaysian laws. Examples of extreme impact include public cloud arrangements involving systems of record which maintain the controlling copy of critical information that determines financial institutions’ obligations to its customers, such as current balance and transaction history.”* This proposed language is based on regional best practices from other FS regulators in the Asia-

			Pacific, and our expertise in working with FS customers.
Section 10.77	A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct risk assessment prior to cloud adoption which considers the inherent architecture of cloud services which rely on sharing of resources and services across multiple tenants over the Internet. This risk assessment must include consideration of the following:	While we recognize the importance for a FSI to bear in mind security controls when choosing a service provider, we do not think that adopting cloud services, nor utilizing a multi-tenant environment, poses an inherent risk. Furthermore, using this type of language to describe cloud services, will dis-incentivize FSIs from using cloud, thus cutting off access to leading edge service and products, automated security functions, and lower costs. FSIs should be able to seek access from their CSP to independently produced information about their outsourced services to enable them to understand and manage the relevant risks. For example, CSPs attains industry certifications and independent third-party attestations for its security controls and practices including SOC 1/SSAE 16/ISAE 3402, SOC 2, SOC 3, ISO 27001, ITAR and PCI DSS Level 1.	We suggest changing the wording to: A financial institution should conduct risk assessment prior to cloud adoption.
Section 10.78(a)	On-premises DLP may not be feasible for all cloud computing deployments due to	We are not sure why there is a specific requirement to have DLP tool deployed on-premise. There are cloud native solutions which provide for data loss prevention. It is not clear what additional security objectives (if any at all) would be met if the solution	While financial institutions should certainly consider DLP, we recommend that BNM remove the requirement that it be implemented for all cloud based services. We also recommend changing the wording here to: “Deploy data loss

	issues of cost and availability.	were deployed on-premise compared to being on cloud.	prevention (DLP) to protect confidential information”
Section 10.78(b)	Certain outsourced services – such as SaaS-based cloud computing services – will not allow for a customer to manage or supply their own encryption key. Therefore, financial institutions should rely on ISO certifications and SOC reports to ensure a vendor uses appropriate controls and processes to manage encryption keys.	SaaS-based services are fully managed according to a standard responsibility model. If a financial institution was to manage their own key, it would add a considerable amount of workload and risk.	We recommend that BNM clarify that the principles proposed are only for situations where the financial institution manages and controls the encryption keys.
Section 10.97- Question 12 The Bank seeks comments on whether single factor authentication (1FA) should be	MyDebit has a threshold of RM250. As such, we recommend that BNM adopt this threshold to maintain consistency and to prevent user confusion.		

allowed for low-value transactions subject to appropriate safeguards (e.g. transaction limits and the facility for users to lower or zerorise such limits). This is intended to promote proportionate regulation, while fostering a more enabling environment for the adoption of emerging e-payment methods such as mobile payments. Where 1FA is allowed for low-value transactions, the Bank also seeks views on whether the Bank should prescribe the threshold for "low-value	

transactions", and/or the specific type of 1FA permissible for such transactions?			
Section 10.106	A financial institution must undertake a comprehensive risk assessment of the advanced technologies and the algorithms deployed in their digital services to mitigate associated risks. Algorithms must be regularly reviewed and validated to ensure they remain appropriate and accurate.	CSPs often use proprietary algorithms or algorithms that are otherwise protected intellectual property, for example, trade secrets. As a result, an algorithm audit might not be possible. Requirements to compel organizations to divulge their intellectual property without binding assurances that their IP will be protected will inhibit industries and innovators from bringing the best technologies and practices to Malaysia. For-profit organizations rely upon proprietary IP, including source code, to ensure business success. Third party software vendors would typically conduct audits of their Software Development Life Cycle and Change Management processes to ensure that it is sufficiently robust. They would also provide independent assurance / audit reports to assure their customers. We recommend that financial service customers leverage these audit / assurance reports to conduct their due diligence.	We recommend changing the wording here to: “A financial institution must undertake a comprehensive risk assessment of the advanced technologies and the algorithms deployed in their digital services to mitigate associated risks. Algorithms must be regularly reviewed and validated to ensure they remain appropriate and accurate. Where third party software is used, leverage provided independent audit reports to determine if the service provider’s Software Development Life Cycle and Change Management processes are sufficiently robust.”
Section 11.29	A financial institution must conduct annual cyber drill exercise to test	Security and Compliance is a shared responsibility between CSPs and the customer. This shared model can help relieve customer’s operational burden as CSP operates, manages and controls the components from	We recommend changing the wording here to: “A financial institution must conduct annual cyber drill exercise to test the effectiveness of CIRP based on various current and emerging

	the effectiveness of CIRP based on various current and emerging threat scenarios (e.g. social engineering) with the involvement of key stakeholders including members of senior management, the Board and third party service providers.	the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the CSP provided security group firewall. Customers (FSIs) retain control of data and applications. The customer is responsible for architecting their own Disaster Recovery/ Business Continuity / Emergency Response plans. CSPs provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on the cloud. CSPs also test its Business Continuity plan and its associated procedures at least annually to ensure effectiveness of the plan and the organization readiness to execute the plan. CSPs does not share the results with customers due to security and confidentiality risks. The results are reviewed and validated by independent third-party auditors. Customers should leverage CSP's independent third -party assurance reports to gain assurance that BCP tests are conducted periodically.	threat scenarios (e.g. social engineering) with the involvement of key stakeholders including members of senior management and the Board."

Appendix 1: Risk Based Approach to Regulatory Compliance

Rather than mandating prescriptive requirements to apply universally to all types of outsourcing, a risk based approach to regulatory compliance encourages regulated institutions to implement outsourcing guidelines in a way that reflects the nature of risk in, and materiality of, the outsourcing agreements. A risk-based approach encourages innovation, scalability while maintaining an appropriate risk management regime.

The benefits of adopting a risk based approach to regulatory compliance include:

1. The ability to account for different types of outsourcing and providing the FSI the ability to adjust the controls and security measures they implement to be commensurate with the nature of the risks associated with the service being outsourced.
2. Avoid paying to implement security measures or controls that are mandated by the outsourcing guidelines, but might not be relevant for your business or the specific service being outsourced. This includes the cost of hiring and training employees on new control processes and procedures. It is commercially untenable to require a business to incur additional expenses to implement new processes and controls that are not appropriate for its business operations.
3. A prescriptive approach to outsourcing can limit an institutions ability to expand into new markets or new product lines because it might be unable to comply with strict regulatory requirements that apply to all outsourcing, limiting its ability to expand its business.
4. A risk-based approach fosters innovation, including the development of fintechs and other startups, who might not have the budget to implement all the requirements set out in a prescriptive regulation. A risk based approach should allow for non-production development and testing without the high costs associated with the prescriptive regulation approach. The ability to set up development and testing environments and test new products will nurture innovation in the market and ultimately provide end customers more selection and value.

---End of Submission---