BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Management in Technology

Frequently Asked Questions

Last updated: 1 July 2026

Introduction

This Frequently Asked Questions (FAQ) document is designed to guide financial institutions in interpreting and implementing the requirements set out in the Risk Management in Technology (RMiT) policy document issued on 28 November 2025. It aims to clarify key provisions, address common queries, and provide practical insights to support compliance with regulatory expectations.

Please note that this FAQ **does not replace the RMiT,** rather, it serves as a complementary reference to promote consistent understanding and application across the industry.

Interpretation

1. Will the applicability of RMiT be extended to overseas entities of local financial conglomerates?

BNM expects financial institutions to practise robust risk management and adopt similar or more stringent requirements for its overseas branches and entities.

2. Are clauses marked with "G" (Guidance) considered mandatory requirements especially for Large Financial Institutions? [Paragraph 5.2]

Clauses marked with "G" in the RMiT Policy Document represent recommended practices that financial institutions are encouraged to adopt. They are not mandatory requirements, consistent with previous RMiT versions. Additionally, the latest RMiT has removed the distinction of "Large Financial Institution", with the intent of strengthening cybersecurity resilience across the entire financial sector by applying expectations more uniformly to all financial institutions.

3. What are the examples of systems categorised under Critical System? [Paragraph 5.2]

Example of critical systems may include but are not limited to:

a) Core Banking System;
b) Core Insurance System;
c) Payment Systems:
    i. eSpick;
    ii. RENTAS;
    iii. Interbank Fund Transfer (IBFT, MEPS IBG);
    iv. Mobile payments (DuitNow QR);
    v. Payment gateway (FPX);
d) Card System (Credit Card, Debit Card);
e) Treasury System;
f) Self-Service Terminals (CRM, CDM & ATM);
g) Internet Banking System (Retail and Corporate);
h) Mobile Banking System;
i) Call Centre;
j) Insurance eCover note;
k) Internet Insurance System (for public and agents, e.g. motor & travel insurance);
l) SWIFT.

The list of critical systems provided is not exhaustive. Financial institutions must assess and determine whether other systems qualify as "critical system", considering the potential impact of a system failure to customers, business operations, reputation or

compliance with regulatory requirements and laws. Financial institutions may also consult BNM for clarification on the classification of a specific system.

4. How should a non-bank registered merchant acquirer (MA) determine whether it meets the 5% market share threshold, given that aggregate market data for non-bank MA services is not publicly available? Is there a way to access such data or a formal process to obtain it? [Paragraph 5.2]

Aggregate transaction value and/or volume data for non-bank MA is not publicly published by BNM.

Financial institutions will be notified by BNM if they meet the 5% market share threshold and are therefore required to comply with the RMiT policy document. Such notification serves as confirmation that the identified MA falls within the scope of the RMiT.

Financial institutions that do not meet the threshold are not required to comply with RMiT. However, they remain subject to other applicable regulatory requirements, including the Technology Requirements Policy Document.

Responsibilities of the Board of Directors

5. Can a financial institution be given the flexibility to adapt its IT and cybersecurity strategic plan from the parent company or the Group? [Paragraph 8.2]

Yes. However, the plans shall align with local regulatory requirements including the requirements under RMiT after taking into consideration the complexity of the financial institution's operations, risk profile as well as the local entity business environment. The board of each financial institution must provide oversight and ensure the adequacy of these plans.

6. Can a board of a financial institution leverage on any existing board committee to perform oversight on technology-related matters? [Paragraph 8.3]

Yes. The board of a financial institution may either designate an existing board committee or establish a separate committee for this purpose. Where such a committee is separate from the Board Risk Committee (BRC), there must be appropriate interface between this committee and the BRC on technology risk-related matters to ensure effective oversight of all risks at the enterprise level.

7. What is the expected scope and depth of experience and competencies for a board member to meet this requirement? [Paragraph 8.3]

There is no prescribed set of specific technical skills for a board member to fulfil this requirement. However, it is essential that at least one board member possesses appropriate technology-related expertise and experience to contribute effectively to the board's oversight of technology matters.

The expected competency should be of sufficient depth to bridge the gap between technical technology and cyber risks, and enterprise-level risk management discussions. This enables the board to exercise effective oversight of cybersecurity resilience and the management of the institution's technology lifecycle on an ongoing basis.

In practice, board members with the relevant expertise often:

- Have held leadership roles in areas such as technology operations, consultancy, service delivery, digital innovation, or transformation;

- Bring experience in integrating business and technology functions, particularly within financial institutions, technology firms, or critical infrastructure providers;
- Possess academic backgrounds in fields such as information technology, engineering, or science, which support their understanding of emerging technologies.

Overall, the board member's competencies should be adequate to facilitate informed deliberation, provide credible challenge, and contribute effectively to decision-making on immediate priorities and strategic planning of technology-related matters to preserve public confidence in the integrity and security of digital financial services.

Responsibilities of the Senior Management

8. How should financial institutions determine when to trigger a crisis management plan, given that the actual impact on customers (e.g. duration, number of customers affected, and value of transactions) may only be fully known after an incident? Also, some disruptions may involve external dependencies (e.g. DDoS attacks, telco outages, or external payment operator failures. [Paragraph 8.6]

Financial institutions are expected to establish crisis management plans that incorporate indicative thresholds and escalation criteria, while retaining sufficient flexibility to account for uncertainty during an incident. Recognising that the full impact may not be immediately quantifiable, financial institutions should rely on reasonable estimates derived from available real-time data.

Financial institutions are expected to work closely with key third party service providers to strengthen real-time monitoring capabilities for critical digital services. During a disruption, financial institutions may leverage network and application telemetry to form reasonable estimates of impact, such as:

- Unusual network traffic patterns
- Failed login attempts
- Transaction decline rates
- Service availability and performance indicators

These indicators may be used to support timely escalation and the activation of the appropriate crisis management plan, based on predefined criteria and reasonable judgment at the point of detection.

Subsequently, financial institutions should update and reconcile impact assessments once more complete data, including logs and reports from relevant third party service providers, become available. This ensures accurate reporting and supports effective post-incident review and continuous improvement of crisis management processes.

Technology Risk Management Framework (TRMF)

9. Can the scenario analysis requirement under paragraph 9.2(j) be fulfilled through component-level disaster recovery (DR) exercises at the system level? Are there any best practices in addressing this requirement? [Paragraph 9.2]

Scenario analysis under paragraph 9.2(j) is intended to complement and not be replaced by component-level DR exercises. While DR exercises typically test system recovery capabilities, scenario analysis assesses a financial institution's ability to recover critical services under more severe and plausible stress conditions (e.g. cyber-attacks causing data corruption or data breaches) consistent with the expectations outlined in the Stress Testing Policy Document issued by BNM.

Accordingly, financial institutions are expected to design scenario analysis that are commensurate with their operating environment and evolving threat landscape. In advancing industry practices, collaborative platforms such as industry associations may also facilitate the sharing of best practices and practical approaches to strengthen institutional capacity in this area.

Designated Chief Information Security Officer (CISO)

10. What is the appropriate reporting structure for the CISO? [Paragraph 9.4]

BNM does not prescribe a specific reporting structure for the CISO. A financial institution is expected to determine an appropriate structure aligned with its business model and risk profile, to enable effective management of enterprise-wide technology risk in line with the enhanced CISO role under the Responsibility Mapping and RMiT policy document.

The CISO should:

- Maintain independence from day-to-day technology operations, typically by being positioned within the second line of defence;
- Has sufficient authority and stature to provide independent views; and
- Be supported with adequate resource and capacity to discharge responsibilities effectively.

The reporting structure should also facilitate the CISO's ability to:

- Provide timely and independent update to the Board on technology risk landscape;
- Advocate for necessary technology risk investments; and
- Support informed decision-making on residual risk acceptance within the institution's risk appetite.

11. Can financial institution leverage group-level CISO? [Paragraph 9.4]

BNM expects every financial institution to designate an entity-level CISO, who is accountable for technology risk management. The entity-level designation ensures that a competent CISO with sufficient capacity is responsible for ensuring the financial institution's information assets and technologies are adequately protected to preserve operational integrity and business continuity.

Financial institutions may leverage Group-level CISO to supplement expertise and strengthen capability development. However, any "double-hatting" arrangement, including where a Group-level CISO oversees technology risk management across related entities, is generally permitted only as an interim arrangement or under specific circumstances with appropriate safeguards. Such arrangements are subject to BNM's case-by-case approval.

Where permitted, the Group-level CISO is expected to ensure that all entities within the group have implemented robust technology risk management practices and maintain direct reporting lines to each entity's Boards of Directors. BNM may rescind the flexibility granted and require a financial institution to designate an entity-level CISO if elevated risks are observed during BNM's supervisory activity.

For the avoidance of doubt, the Group-level CISO must be based within a BNM-regulated entity in Malaysia and cannot be situated in an overseas entity or a non-BNM-

regulated entity. Financial institutions are encouraged to engage their IT Supervisor for further clarification.

12. Is it mandatory for the CISO to have experience in all three areas (audit, governance, and risk management), or would experience in one or two of these areas suffice? [Paragraph 9.4]

A CISO is required to possess the range of expertise and experience outlined in the policy to enable effective risk oversight, and their experience should be commensurate with the financial institution's technology profile. For example, a CISO should be well-versed in cloud technologies for a financial institution that has adopted cloud solutions for critical systems. To meet this requirement, the institution should implement measures to support the CISO's professional development within an appropriate timeframe.

Software Bill of Materials (SBOM)

13. How should financial institutions assess cyber supply chain risks, as outlined in paragraph 10.15, when vendors are unable to provide access to source code or detailed repository security information due to proprietary considerations? [Paragraph 10.15]

Financial institutions should assess third party service provider's secure development practices, governance frameworks and incident response capabilities, coupled with the incorporation of contractual clauses to manage security risks related to proprietary source code of critical systems developed by third party service providers.

This is typically implemented through regular engagements with critical third party service providers to explain the policy intent, establish information sharing arrangements, and identify relevant independent assurance reports, security attestations, or certifications to support the assessment of the security posture of such proprietary systems.

Financial institutions should determine whether the level of assurance obtained is commensurate with the criticality of the services and take appropriate mitigating measures where gaps are identified.

14. Does continuous monitoring of third party security vulnerabilities via vendor provided monitoring suffice to meet requirement under paragraph 10.15, or the use of tools such as software Composition Analysis (SCA) required for SBOM monitoring? [Paragraph 10.15]

The intent of paragraph 10.15 is to strengthen the financial institutions' cybersecurity posture in managing software supply chain risks. Continuous monitoring by third parties may suffice, provided it includes SBOM capabilities including the use of standardised SBOM formats and SCA tools. These capabilities should support transparency of software components enabling timely identification of vulnerabilities and strengthening overall software supply chain security in alignment with paragraph 10.15.

Where third parties monitoring does not provide sufficient SBOM visibility or dependency-level analysis, financial institutions are expected to progressively implement appropriate tools or processes to establish these capabilities, ensuring effective management of software supply chain risk management.

Patch and End-of-Life System Management

15. What is BNM's definition of "End of Life" (EOL) and motivation for applying EOL management to all systems? [Paragraph 10.17]

"End of Life" refers to the stage in an IT asset's, system's, or service's lifecycle at which it is no longer officially supported by the relevant third party service providers with new features or security patches and financial institutions are expected to migrate to alternative solutions. The expansion of scope from only critical systems to all systems reflects the systemic risk posed by unsupported components, where vulnerabilities in non-critical systems can still be exploited as entry points into the financial institutions environment[1]. To mitigate such vulnerabilities, financial institutions are expected to establish structured plans to upgrade all systems within defined milestones, drawing on industry best practices[2]. For legacy systems that cannot be migrated due to technical constraints or business dependencies, paragraph 10.17(d) has been introduced to allow management-approved exceptions following a thorough assessment.

References:
[1] The Equifax data breach involved the exploitation of a consumer complaint web portal that was operating on a legacy framework, which served as the entry point for attackers. For further information, see: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

[2]https://docs.oasis-open.org/openeox/standardization-framework/openeox-standardization-framework-technical-report.pdf.

16. Can virtual patching be considered as implementation patch due to enhanced coverage for all systems instead critical system? [Paragraph 10.17]

Virtual patching is an interim risk mitigation measure and not a substitute for permanent remediation. While it may reduce exposure to known vulnerabilities where immediate patching is not feasible, it does not address the underlying issue. Financial institutions are expected to ensure timely implementation of permanent fixes to defend against accelerated vulnerabilities discovery by frontier technologies.

Virtual patching should only be used on a temporary basis, supported by appropriate risk assessment and monitoring, until a fully tested and permanent patch is implemented.

Service Availability

17. How does paragraph 10.31 apply to insurance and takaful businesses when digital services do not involve real-time financial settlement or have manual/assisted alternatives? [Paragraph 10.31]

Paragraph 10.31 applies to insurance and takaful operators (ITOs) and provides a pathway for ITOs to progressively build capabilities in managing service degradation and intermittent issues affecting digital services.

A risk-based approach may be adopted, particularly for services that do not involve real-time payments or time-sensitive transactions and where manual or assisted alternatives are available. In such cases, proportionate controls may be applied, provided there are adequate contingency arrangements in place to manage disruptions and minimise customer impact, with clear rationale and supporting evidence documented.

18. Would active-active, multi-site architectures be sufficient to meet the resilience requirement, or is a logically independent application for transaction authorisation expected in the event of a complete primary core banking system failure? [Paragraph 10.31]

The latter statement aligns with the intent of stand in processing. While active-active and multi-site architectures enhance infrastructure resilience and support high availability, unplanned system disruptions may still occur. As a contingency arrangement, stand in processing should operate through an independent or logically segregated capability to minimise failure and ensure continuity, particularly for time-sensitive transactions during disruptions.

19. Is there a prescribed methodology for calculating cumulative unplanned downtime, or how should financial institution approach this calculation? [Paragraph 10.32]

RMiT does not prescribe a specific methodology for calculating unplanned downtime. Financial institutions may compute unplanned downtime using a combination of monitoring tools, including application, network and infrastructure monitoring, supported by quantitative indicators such as system response time, transaction success and failure rates, transaction volumes and user sessions.

Financial institutions are expected to maintain robust availability monitoring to support timely escalation and root cause analysis to prevent recurrence.

Illustration on cumulative unplanned downtime (12 months rolling basis):

1. June 2024 – June 2025: 2 hours (compliant)
2. Nov 2024 – Nov 2025: 5 hours (non-compliant)
3. June 2025 – June 2026: ≥5 hours (non-compliant)
4. November 2025 – November 2026: ≥3 hours
   (compliance may be maintained provided no future outage exceeds 1 hour).

20. Is there a defined implementation timeline for paragraph 10.35 (d), given that paragraph 10.35 (e) specifies a deadline of 15 October 2027? [Paragraph 10.35]

As set out in RMiT, all requirements take effect immediately upon issuance except when stated otherwise. Financial institutions should progressively publish real-time availability and performance status of its customer-facing digital services on the corporate website to enhance transparency and customer experience.

21. Where disclosure of certain information may raise security sensitivities or reputational concerns, would a communication-based approach (e.g. advisories and outage notifications) be considered acceptable, particularly for banks serving institutional and corporate clients? [Paragraph 10.35]

Yes. Paragraph 10.35 is intended to be applied on a risk-based basis, with a focus on ensuring clear and timely visibility of service availability, particularly for retail customers.

Financial institutions may exercise proportionality in their disclosures, taking into account security and reputational sensitivities. In this regard, a communication-based approach such as timely advisories and outage notifications through official channels, may be appropriate, provided the information is clear, relevant, and focused on customer impact without exposing sensitive details.

System Backup and Restoration

22. What are the expectations for an isolated recovery environment (IRE), particularly in terms of design, controls and degree of isolation? [Paragraph 10.45]

An IRE should be designed and operated in a manner that the environment remains trusted and reliable, even in the event of a destructive cyber-attacks affecting production system and is able to support recovery within the financial institutions' tolerable disruption level.

Based on globally[1] observed practices, an IRE commonly incorporates the following controls and characteristics (including but not limited to cyber recovery vault principles or isolated backup/ tertiary backup guidance):

i. strong logical and administrative separation, including segregation of networks, identities, credentials, and management systems;
ii. restricted and controlled privileged access;
iii. time-bound connectivity between the production environment and the IRE for recovery or testing purposes, provided such connectivity is governed and does not permit lateral movement, credential compromise, or undermine the integrity of the recovery environment.

"Isolation" does not necessarily require permanent or full logical and physical disconnection from the production environment. The degree of separation should be commensurate with the financial institutions' risk profile and sufficient to prevent compromise of the recovery environment, ensuring it remains trusted even if the production systems are affected.

[1] *Hong Kong Secure Tertiary Data Backup (STDB) and U.S Sheltered Harbour initiative which is being transferred to FS-ISAC for ongoing maintenance. FI may refer to 2022-06-asifma-data-vaulting-paper-formatted-final-pdf.pdf for reference.*

23. Does tape backup with a combination of controls to achieve tamper-proof fulfil the requirement? [Paragraph 10.45]

The use of tape backup in combination with robust controls may fulfil the requirement provided financial institutions can demonstrate the overall arrangement is tamper-resistant and resilient against destructive cyber-attacks, including ransomware. At a minimum, financial institutions should ensure controls include immutability/ write-once (WORM) protection during the retention period, strong access controls, protection against alteration, deletion or encryption by compromised credentials and regular testing to ensure recoverability.

Continuous Control Monitoring

24. Does paragraph 10.49 apply to all third party service providers, including SaaS providers, or only to those assessed as material or critical (e.g. with access to customer data or core systems)? [Paragraph 10.49]

Paragraph 10.49 applies on a risk-based basis and is intended for a financial institution to prioritise material or critical third party service providers, including SaaS vendors, for continuous monitoring. Non-critical vendors may be subject to proportionate oversight, but this determination must be documented and governed.

25. How should financial institutions measure their IT infrastructure footprint and the extent of customer information accessible to third parties, and what practices are considered sufficient to manage such external exposure risks? [Paragraph 10.49]

Financial institutions are expected to adopt a risk-based and comprehensive approach to identify, measure, and manage their IT infrastructure footprint and third party access to customer information.

This includes maintaining an up-to-date inventory of systems, assets, and third party integrations, along with a clear understanding of the data accessible to external parties. Financial institutions should assess exposure points across their technology environment, including interfaces, APIs, and outsourced services.

To demonstrate effective management of external exposure risks, financial institutions should implement practices such as:

- Robust third-party risk assessments and ongoing monitoring
- Strong access controls and least-privilege principles
- Data classification and protection measures (e.g. encryption, masking)
- Continuous vulnerability and exposure management
- Regular review of third party access and dependencies

These measures should be commensurate with the financial institutions' risk profile and sufficient to mitigate potential cyber-attack surfaces arising from external exposures.

26. How should financial institutions determine the priority set of security controls that require more frequent assurance from third party service providers, and what forms of assurance are considered adequate? [Paragraph 10.49]

Financial institutions are expected to identify security controls requiring more frequent assurance based on a risk assessment, taking into account factor such as the criticality of the service, data sensitivity, and the potential impact to business operations and customers arising from the controls' failures.

Typically, controls that directly affect the confidentiality, integrity and availability of systems or customer data would warrant higher priority, (e.g. controls relating to vulnerability management, patch management, access controls or security configurations).

Adequate assurance may include independent assurance reports, certifications, external attestations, or other credible evidence, commensurate with the third party service provider's risk profile. The selection of controls and frequency of assurance should be justified, documented, and subject to periodic review.

Access Control

27. Is Multi-Factor Authentication (MFA) mandatory for critical systems accessed solely by internal staff, and can it be fulfilled through network-level controls (e.g. VPN or access controls) instead of system-level MFA? [Paragraph 10.55]

Yes. MFA is mandatory for all critical systems, including those accessed exclusively by internal staff. This requirement reflects an "assume breach" posture, recognising that internal accounts remain exposed to risks such as phishing, credential theft, and social engineering.

As set out in paragraph 10.55, MFA must be implemented in a manner that effectively defends against such threats. Accordingly, MFA cannot be satisfied solely through network-layer controls (e.g. VPN authentication or device-based access controls).

Instead, MFA should be enforced at the system or application level when users access critical systems, sensitive functions, or privileged actions.

Centralised identity solutions (e.g. Active Directory with integrated MFA) may be used, provided that MFA is triggered at the point of authentication to the critical system, rather than only at network access.

28. Would BNM accept risk-based MFA implementation where MFA is prioritized for internet facing customer application rather than uniformly applied across all internal systems that already require access control? [Paragraph 10.55]

No. For clarity, a financial institution must implement MFA for authenticating user access to critical internal systems. For non-critical systems, a financial institution may consider MFA based on risk assessment.

29. Does the requirement permit two-factor authentication (e.g. username-password with email OTP or biometric), and does this differ where a centralised identity solution is used (e.g. Active Directory)? [Paragraph 10.55]

Yes, a combination of strong authentication factors, at a minimum of two, that can effectively defend against social engineering attacks is required to meet the MFA requirement in paragraph 10.55. Integration with a centralised identity solution does not change the requirement under paragraph 10.55 and financial institutions are expected to select authentication methods with sufficient security strength to fully meet the requirement.

Cyber Risk Management

30. Can we combine Red Team simulation and annual intelligence-led penetration testing (VAPT)? [Paragraph 11.5]

Penetration testing and red team simulation differ in scope, purpose and techniques. Both assessments are used complementarily to enhance the identification and remediation of security gaps to strengthen an institution's cyber posture.

While financial institutions may leverage or combine these exercises for cost effectiveness, financial institutions must ensure that the intent of the respective requirements is preserved in the scope, objectives, and approach of each exercise. The exercises should be risk-based and proportionate, and designed with distinct scenarios and threat intelligence inputs, profiles or attack scenarios. The scenarios used must remain relevant, realistic, and applicable to the institution's evolving threat landscape and risk profile. Combining these exercises should not dilute their effectiveness, and should collectively enhance the institution's ability to identify, test, and remediate security gaps.

Financial institutions must ensure that any combined or coordinated approach remains risk-based, proportionate, and aligned with supervisory expectations. Where there is any uncertainty, financial institutions are encouraged to engage with their respective IT supervisors on a case-by-case basis to validate that the proposed approach and scope are appropriate.

Cyber Response and Recovery

31. Are there any specific expectations for hosting an out-of-band communication channel (e.g. outside the bank's internal network), and is a paid subscription required? [Paragraph 11.16]

Financial institutions are given the flexibility to determine and establish the specific hosting arrangement for their out-of-band (OOB) communication channel. Financial institutions are expected to ensure that the OOB communication channel is operationally independent from their primary network and is designed to remain secure, available, and effective in the event of a cyber security incident, including situations where the primary network may be partially or fully compromised.

The choice of medium or application should be guided by a risk-based assessment that considers the institution's threat landscape, business continuity arrangements, and operational dependencies. The established OOB channel should also be subject to appropriate governance, periodic testing, and ongoing review to ensure continued effectiveness and alignment with the institution's risk profile and operational needs.

Digital Fraud Management and Customer Awareness

32. Are financial institutions expected to perform penetration testing and assumed-breach simulation exercises (e.g. covering phishing, malware, scam scenarios) as part of continuous surveillance and monitoring to detect exploitation and strengthen fraud-related controls under paragraph 12.3 (c)? [Paragraph 12.3]

Financial institutions are expected to conduct regular penetration testing, including targeted assessments on fraud-related attack vectors, to evaluate the effectiveness of controls in detecting and preventing unauthorized access, fraudulent transactions, and system vulnerabilities.

In addition, financial institutions should engage experts to simulate scam/phishing and malware attacks with various scenarios to robustly assess the adequacy of their security controls as well as their responses to scam cases. These scenarios should be designed under an assumed-breach approach, where customers are assumed to have been tricked into disclosing banking credentials or compromising their device, and could be acting under the scammer's influence.

Any gaps identified should be remediated within a reasonable timeline, including enhancement to fraud detection system, banking security controls or business processes. Financial institutions are also expected to continuously strengthen its fraud management system to combat evolving fraud technique beyond security control breaches to detecting "push payments" authorised by customers under duress as observed in Macau scam.

33. Is a financial institution expected to provide customers with a dedicated tool to verify the authenticity of callers, or is reliance on customer education and existing tools (e.g. True caller) considered sufficient? [Paragraph 12.5]

Financial institutions are expected to provide customer with a practical means to verify authenticity of callers, typically through bank-controlled verification feature integrated with online banking platforms.

For example, some financial institutions have implemented in-app call verification features that allow customers to verify a caller's legitimacy directly within the banking app during or immediately after the call.

While customer education remains important, it is not sufficient on its own. Financial institutions are expected to complement awareness efforts with effective verification tools that materially reduce the risk of vishing and impersonation scams.

34. In enhancing customer awareness and understanding of fraud risks, what are the expectations for the use of interactive simulations (e.g. demonstrating security features), and would awareness videos be sufficient to meet these expectations? [Paragraph 12.7]

The use of interactive simulations is intended to enhance customer understanding by demonstrating security features and common fraud scenarios, with customer input and immediate feedback. This may include in-app prompts, short quizzes, or scenario based walkthroughs adopted by financial institutions, such as identifying phishing messages, verifying legitimate channels, or recognising when not to share credentials).

BNM has no objection to financial institutions using awareness videos as part of their broader customer awareness programme. Financial institutions should ensure that such videos adequately cover all relevant areas outlined under paragraph 12.7, including the demonstration of key security features, common fraud or scam scenarios, and appropriate customer actions to mitigate fraud risks.

External Party Assurance

35. As a regional bank, our critical systems are hosted at regional data centre. While only non-critical system such as door access, printing system, file storage and network equipment is maintained locally in the technical room, is the technical room at both production and business continuity site subject to Data Centre Resilience Assessment (DCRA)? [Paragraph 14.1]

No. The scope of the DCRA applies to the financial institution's production and recovery data centres that host critical system. For clarity, financial institutions are still required to submit the DCRA (or equivalent assessment reports) to IT Supervisors for the designated/identified data centres hosting the critical system, even if the critical systems are hosted at regional data centres.

36. As a regional bank, our critical systems are hosted at regional data centre and only non-critical system such as door access system, printing system, file storage and network equipment is maintained in local technical room. Are the production and business continuity site subject to Network Resilience Assessment (NRA)? [Paragraph 14.2]

The scope of the NRA applies to the financial institutions' network infrastructure on an enterprise-wide basis, including the production and recovery sites, as well as the broader network, endpoints and any local infrastructure that could be exploited to compromise critical system.

Notwithstanding that IT operations may be centrally managed or supported by group function, the financial institution remains fully accountable for ensuring compliance with the spirit and intent of the requirements. Hence, the financial institution is expected to obtain and submit a suitable NRA report (or equivalent assessment) with appropriate coverage of risks arising from the Malaysian/domestic infrastructure and its connectivity to the group/enterprise network.

Security Awareness and Education

37. Is it sufficient for financial institutions to assess third party service providers' own security awareness program, or must third party service providers participate in the financial institutions' programme? [Paragraph 15.1]

Financial institutions are expected to ensure that key personnel of third party service providers are subject to an appropriate security awareness program. While assessing the adequacy of a third party service provider's own programme may be considered, such assessment alone would not be sufficient unless it is aligned with the institution's risk profile, service criticality, and operating environment.

BNM provides flexibility in implementation. Nevertheless, the financial institutions remain accountable for ensuring the effectiveness of cybersecurity awareness arrangements for third party service providers, in line with paragraph 15.1.

Notification for Technology-Related Applications

38. Does the transmission of customer data within digital services of the same financial group qualify for simplified notification? [Paragraph 16.3]

Transmission of customer data within digital services of the same financial group may qualify for simplified notification, particularly where the entities involved are subject to equivalent regulatory and information security standards.

This is consistent with the intent of Appendix 6(1)(c) to mitigate third party cyber risks. Such enhancements may qualify for simplified notification where the change is minor, does not introduce new technology, and does not result in material changes to the system architecture.

39. What are examples of application architecture or network design that qualify for simplified notification process (e.g. a major front-end UI overhaul that leverages existing backend APIs qualify)? Should this be assessed based on system classification? [Paragraph 16.3]

The qualification for simplified notification is not determined solely by system classification, but also by the materiality of the enhancement introduced. The following scenarios may serve as a guidance:

Scenario 1:
Modification of a critical system's front-end user interface (UI) critical system requiring major architectural or technology changes

Description:
Front-end UI changes that necessitate material changes to the application architecture, technology stack, or system design of a critical system. Some illustrative examples include the following:

- Transition from web view-based or cross-platform mobile applications to native mobile application development
- Addition of new features that materially impact security requirements (e.g. handling, processing, or storage of sensitive data)
- Architectural changes from monolithic to microservices-based application architecture

Qualified for simplified notification: Not eligible

Scenario 2:
Modification of a critical system's front-end UI utilizing existing architecture

Description:

- Front-end UI changes that continue to maintain the existing application architecture and technology stack (e.g. web development stack) with no material impact on security and resilience requirements.

Qualified for simplified notification?
Eligible. Financial institutions must ensure robust risk assessment and mitigation in line with paragraph 16.3.

Scenario 3:
Enhancement of critical system that introduces emerging technology or involves migration to cloud**.**

Qualified for simplified notification?
Not eligible. Financial institution is subject to Section 17 of RMiT given the introduction of emerging technology or migration to cloud for a critical system.

Scenario 4:
Enhancement of non-critical system that introduces emerging technology or involves migration to cloud.

Qualified for simplified notification?
Eligible. Financial institutions should conduct risk assessment and ensure that the relevant documentation is available to BNM, in accordance with paragraph 17.5.

Consultation and Notification related to Cloud Services and Emerging Technology

40. RMiT requires financial institutions to appoint an external service provider to perform certain risk assessments. In this context, can a technically competent independent party within the same institution or group be appointed to undertake the required assessment instead of an external service provider?

BNM requires all financial institutions to appoint external service providers to carry out the required risk assessment. In the future, BNM may consider allowing suitable financial institutions to perform the assessment internally. Any changes to this requirement will be communicated in due course.

41. Is technology-related application enhancement that does not impact prior assessments changes subject to the notification requirement?

Notification to BNM is not required for enhancements (e.g. cosmetic changes) that does not materially alter prior assessments and representations made by a financial institution to BNM. However, the relevant information must be documented and readily available for BNM's review as and when requested.

42. What preparations are required to initiate a consultation review for inaugural public cloud adoption of critical systems under paragraph 17.1? [Paragraph 17.1]

BNM encourages early engagement by the financial institutions on their cloud adoption plans, i.e. via submission of annual outsourcing plan, IT profile, and related documents, to facilitate timely feedback on potential areas of concern prior to committing significant resources to the initiatives.

To support robust and effective discussions, the financial institution should demonstrate that it has thoroughly considered and addressed the risks outlined in paragraphs 10.50 10.52 and Appendix 10, supported by the submission of sufficient information prior to the briefing sessions.

43. What are examples of emerging technology use cases that are subject to consultation and notification processes? [Paragraph 17.1 and 17.2]

Examples of emerging technologies include, but are not limited to:
a) Artificial intelligence (e.g. Generative AI, Agentic AI)
b) Blockchain technology (e.g. asset tokenisation)

Emerging technologies are typically associated with limited impact understanding, evolving risk profiles and higher complexity. These factors may introduce significant uncertainties and make the associate risks more difficult to assess, thereby warranting closer regulatory consideration through consultation and notification process. Accordingly, greater flexibility in the review approach may be applied as risk management practices as those technologies continue to mature.

Assessment and Gap Analysis

44. Is there a requirement for the gap analysis to be tabled to the board of the financial institution prior to the submission to BNM? [Paragraph 18.1]

No. However, the gap analysis must be robust, adequately deliberated and the financial institution must adhere to its own due process and internal governance process.

45. My organisation has submitted a gap analysis in 2020 to BNM as per the requirement under the RMiT dated 28 November 2025, is the financial institution required to perform a gap analysis again? [Paragraph 18.1]

Yes, financial institutions must maintain continuous compliance by regularly updating its level of compliance (taking into account the new and revised requirements) on an annual basis and the relevant document or assessment has to be made available to BNM upon request.

Appendix 3: Control Measures for Digital Services

46. Under Item 4 of Appendix 3, financial institutions are required to adopt MFA for financial and high-risk non-transaction. How does this requirement apply to Insurance and Takaful Operators (ITO), particularly for activities such as contribution top-ups, fund switches, or other self-service activities within a participant's own certificate? In this context, does the definition of "financial transactions" include internal allocations or payments initiated via digital platforms?

The MFA requirement for financial transactions primarily applies to payment service providers (e.g. banks and e-money issuers) that facilitate monetary transfers, including premium payments, contribution collections, and claims payouts. As ITO generally do not support real-time fund transfers or payment processing within their own digital platforms, this requirement may not typically apply in that context.

However, MFA requirements remain applicable for high-risk non-financial activities within ITO's platforms. These include actions that may lead to fraud or misuse, such as updating participant or policyholder details, changing beneficiaries, adding payout accounts, or modifying sensitive policy information. MFA should be enforced for such scenarios, while lower-risk activities may be addressed through a risk-based approach with appropriate justification.

47. Is secure device binding under Section 3(a) applicable to Insurance and Takaful Operators?

The device binding requirement is targeted at banking institutions that handle financial transactions to mitigate fraud risk. Insurers should evaluate the risks of their digital services and apply the requirement where applicable.

48. What kind of notifications should be sent to customers?

Customers must be notified of transactions through secure and reliable communication channels to ensure timely awareness and enhanced account security. The primary method of notification shall be via the financial institution's official application, which is bound to the customer's registered mobile device. This ensures real-time delivery of transaction alerts that supports secure authentication protocols.

In addition to in-app notifications, financial institutions are expected to provide alternative notification channels. These supplementary channels serve as a redundancy measure to ensure customers are informed even in cases where the primary application may be temporarily inaccessible. Financial institutions must ensure that supplementary notification methods do not require any further input from the user to view and must be sufficiently descriptive of the nature and details of the transaction.

49. Can financial institutions continue to use ATM card number and PIN/CVV for authentication purpose? This is in view that ATM card is credible physical authentication mechanism which is always in possession of the customer. Moreover, activation of secure app/soft token is now subject to strong verification such as branch, ATM and call back verification.

Financial institution may continue to use ATM/debit card number as a unique identifier (e.g. for onboarding customers to online banking facility), provided that additional effective controls are implemented to mitigate risks such as phishing attacks.

However, financial institutions must cease the use of card PIN and CVV for non-designated purposes, including online banking registration or activation, as these credentials are highly susceptible to phishing attacks. Card PIN and CVV must be used exclusively for its designated purpose only namely:

- PIN for transactions at payment terminals and ATM machines; and
- CVV for card-not-present transactions.

Financial institutions are also expected to remind customers that they will never ask for their PIN or CVV number for any other purpose.

Appendix 5: Control Measures on Cybersecurity

50. What are the expectations for conducting a compromise assessment (CA), and can CA be performed by an independent party within the institution instead of an external service provider?

A compromise assessment is expected to provide assurance that the institutions' technology environment has not been subject to any undetected or unknown compromise, including the presence of persistent threat actors.

This involves conducting a comprehensive and in-depth review across the environment to identify potential indicators of compromise or artefacts that may not be detected through routine security monitoring. The ambit of assessment should be broad, rigorous and sufficiently comprehensive to detect unauthorised access, malicious activity, or residual threats. The assessment is expected to be conducted at least once every three years to ensure continued assurance and compliance to the requirement.

The assessment may be conducted by a technically competent and independent party within the institution or group, provided that the party operates independently from day-to-day business operations, possess the necessary expertise and is able to exercise effective oversight in meeting the intent of the requirement.

51. Where a financial institution performs an annual intelligence-led penetration testing (ILPT) based on a defined threat intelligence profile, how should newly introduced systems or digital products within the same assessment cycle be addressed?

In particular:
(a) Can existing threat intelligence and attack scenarios from the annual ILPT be reused to validate new systems, where the threat profile remains unchanged?
(b) Is it acceptable to engage the same ILPT service provider to assess the new systems or products, subject to appropriate scope extension and independence safeguards?

(a) Yes, the financial institution may leverage existing threat intelligence profile and attack scenarios from annual ILPT for new systems or digital products, provided they remain relevant and are adjusted for any material differences in technology or architecture.

Financial institutions are expected to ensure that the ILPT scope is appropriately updated and continues to assess threat-actor pathways, vulnerabilities, control effectiveness, and response capabilities.

(b) BNM strongly encourages financial institutions to maintain independence and objectivity in ILPT engagements. Where feasible, engaging a different independent service provider may provide broader assurance through diversity testing approaches.

Nevertheless, the same provider may be retained for assessing new systems, subject to clear scope extension and adequate safeguards. Financial institutions should ensure

that any reuse of threat intelligence, scenarios or providers does not compromise the integrity and effectiveness of ILPT.

52. What is the expected scope of API security inventory, whether it applies only to externally exposed APIs, and should data flow or data type included?

Financial institutions are expected to maintain visibility and apply appropriate security controls across all APIs, including both internal and external connections. While externally exposed APIs typically warrant more stringent monitoring and controls, the level of controls implemented should be commensurate with the associated risk.

The requirements apply to all APIs regardless of data flow (inbound or outbound) or data type. These factors do not determine the scope of APIs to be included in the inventory but should instead be considered in assessing risk and determining the appropriate level of security controls.

Appendix 6: Criteria for Simplified Notification for IT Services Enhancements

53. With the new amendment to Appendix 6, are all the categories highlighted in the prior issuance (1 June 2023) no longer applicable?

Financial institutions may refer to categories listed in the previous version as examples of IT projects that qualify for simplified notification. In addition, financial institutions can apply the criteria outlined in Section 16 of current version to determine whether other IT projects may also qualify for simplified notification.

Appendix 10: Key Risks and Control Measures for Cloud Services

54. Does Appendix 10 apply to non-critical systems?

Financial institutions are encouraged to consider the common key risks outlined in Appendix 10 in the implementation of control measures for any cloud adoption. Notwithstanding, BNM does reserve discretion to require a financial institution to observe Appendix 10 for non-critical systems.

55. Does Appendix 10 apply in a circumstance where a financial institution deploys critical system to hybrid cloud operated by Group of companies and Group owned the data centre and its operations?

Yes, since Appendix 10 is applicable to the scope of critical system operating on public cloud.

56. Can SaaS be exempted from the Appendix 10 requirements, given the services are commercially available and provided as-is where the users have no or limited controls over the backend process?

No. As the use of SaaS relies on third party IT infrastructure services, financial institutions should understand the associated risks, identify applicable provisions in Appendix 10 and apply cloud risk management proportionate to the criticality and materiality of the service. For example, the use of SaaS for critical systems which store, or process customer data would require stronger security controls.

Financial institutions should obtain sufficient assurance that the quality of risk management by the third party service provider is in line with their respective risk appetites. Procurement decisions relating to the service level and added functionalities should also be driven by information security objectives (e.g., sufficient storage to meet high level of resilience, cyber threat detection for highly sensitive data).

57. Do other cloud service models (e.g. Unified communications as service – UCaaS, Function as a Service – FaaS) also need to adhere to the guidance?

Yes, if the cloud service is classified as a critical system. Financial institutions should identify the relevant provisions in Appendix 10 when assessing the risks of specialised variation of the cloud service models, e.g., UCaaS is a form of SaaS. Financial institutions are also encouraged to leverage on industry standards to identify key risk considerations for commonly used cloud service models as they evolve.

58. Is a Virtual Private Cloud (VPC) considered to be a private cloud?

No. A VPC provided by a public cloud service provider is not considered a private cloud. While a VPC offers logical isolation through virtual networking, it operates within shared infrastructure managed by the cloud service provider. In contrast, a private cloud involves dedicated infrastructure exclusively owned and controlled by a single organisation, allowing full autonomy and control over hardware, security, and compliance.

59. Can a financial institution combine cloud technology risk management framework with the current technology risk framework under RMiT in one documentation?

Yes.

60. For financial institutions leveraging on group's cloud services, what is the expectation for ongoing monitoring and periodic assessment? Can the financial institution rely on the parent company or the group assessment outcome?

Appendix 10 does not preclude financial institutions from leveraging group IT services, including master service agreement with cloud service providers for economies of scale.

The financial institution must make an objective assessment to ensure the group's contract terms and on-going monitoring are adequate to meet the Malaysian operation's business objectives and regulatory requirements.

The financial institution is ultimately accountable for managing the risks from cloud arrangements, regardless of whether they are performed by an external cloud service provider or by group. Therefore, financial institutions should not rely solely on the monitoring and periodic assessment conducted by the group. Financial institutions must ensure that the monitoring and assessments conducted by the group are appropriate and that the cloud services comply with BNM's policy requirements, as well as obtain additional independent assurance if necessary.

61. Clarification on oversight and reliance on third party attestation reports

A financial institution is required to ensure that the cloud service provider is capable of securely managing and protecting sensitive information and data. The financial institution may rely on a third-party attestation report or obtain assurance from an

independent evaluation of the cloud service provider's security, privacy, and compliance controls and processes provided that such reliance is supported by an adequate understanding of the scope and methods. Some of the commonly recognized third party attestation reports that the financial institution can rely on include but not limited to SOC 1, SOC 2, and ISO 27001.

Financial institutions must perform due diligence on the appointed cloud service providers on on-going basis and supplement their review of the cloud service providers' performance based on actual service delivery and the state of compliance of the cloud service providers to meet the information security objectives.

62. Must IT Operation personnel obtain cloud certification even when they have working experience?

IT personnel managing day-to-day cloud operations should possess the necessary competencies, supported by relevant certifications and continuous training. Financial institutions should ensure these skills are maintained and regularly updated through ongoing professional development.

63. Clarification and expectations on multi-cloud strategy

There is a range of service availability and redundancy options for financial institutions to achieve operational resilience under various potential scenarios. Financial institutions are given flexibility to decide on the appropriate solution that commensurate with their information security objectives and are encouraged to adopt a forward-looking approach in their cloud migration journey to achieve operational resilience. This includes the adoption of a multi-cloud strategy, where appropriate, to avoid the concentration risks associated with a single cloud service provider.

64. Expectations for testing an exit plan

Given increasing reliance of financial institutions on cloud service providers to support financial institutions' critical day-to-day operations, financial institutions must be prepared for the possibility of unplanned termination of outsourced services and have effective plans in place as clarified in paragraph 7 of Part (B) Appendix 10: Exit Strategy.

Financial institutions are expected to ensure that the exit plans are sufficiently tested and reviewed periodically to provide reasonable assurance on the feasibility of the plan in the event of the unplanned termination of cloud services. Financial institutions are given flexibility to adopt suitable test methods in line with industry best practices such as the technical paper on cloud strategy testing of exit plans issued by the European Banking Federation Cloud Banking Forum.

65. Why is it crucial to maintain independence in cryptographic key management from the cloud service provider in the case of critical systems?

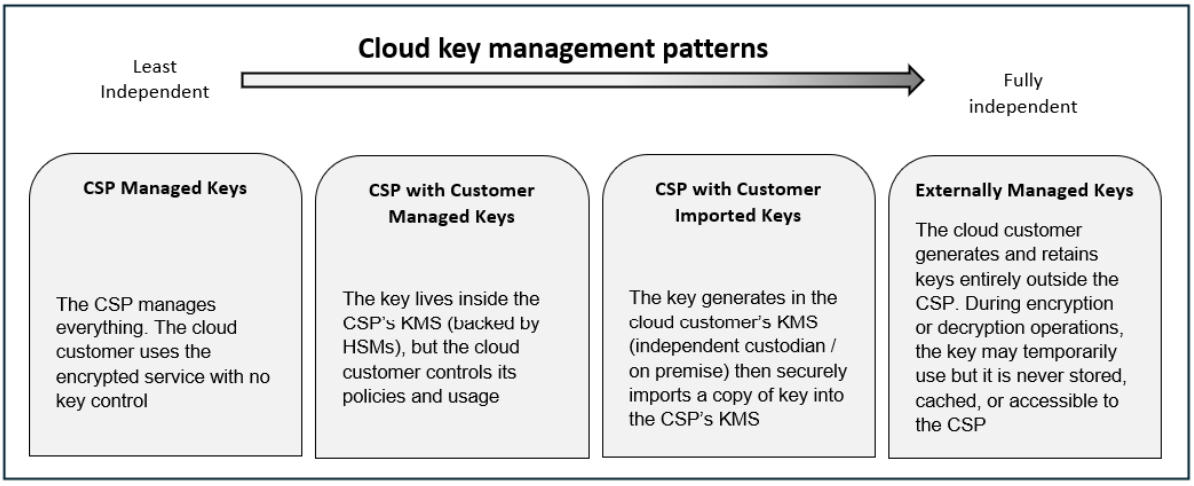
Maintaining independence in cryptographic key management is crucial for systems that handle sensitive or confidential information. As clarified in paragraph 8 of Part (B) Appendix 10: Cryptographic Key Management, possession of encryption keys grants the ability to access the data stored on the servers. The risk of unauthorized access to data and potential compromise of sensitive information increases when the cloud service providers (who are responsible for managing the production data) have access to the encryption keys.

By retaining control over the encryption keys, financial institutions can ensure that only authorised parties have access to their data, thereby reducing the risk of data breaches and protecting the confidentiality, integrity, and availability of the information.

Some financial institutions may face challenges in managing and retaining control of the encryption keys, especially when lacking the necessary resources, expertise, and infrastructure. In such cases, financial institutions may consider utilising a trusted third party key custodian to protect the encryption keys and sensitive data.

Some cloud service providers (CSP) may not allow the customers to manage their own keys due to technical limitation or security concerns. For such cases where there are no alternative and financial institutions must rely on the cloud service provider's key management system, financial institutions should carefully review the cloud service providers' key management practices to ascertain that the information is sufficiently safeguarded and consider whether the additional risk exposure remains within its risk appetite.

There are various cloud key management system (KMS) models that offer differing levels of customer control and complexity. Terms such as Bring-Your-Own-Key (BYOK), Hold-Your-Own-Key (HYOK) and Customer-Managed-Key (CMK) are not formally standardised and are often used inconsistently across cloud and cryptographic service providers. Financial institutions should therefore focus on the underlying control objective and risk management outcomes. The diagram below illustrates an example of how varying degrees of independent cloud key management patterns from least independent to fully independent key management patterns.



Appendix 11: Fraud Detection Standards

66. Does Appendix 11 apply to non-retail segments, commercial banks, investment banks, and insurance and takaful operators?

Appendix 11 is primarily intended to address fraud and scam risks affecting retail customers using digital services. For non-retail segments, such as commercial and corporate customers, as well as business lines within commercial banks, investment banks, insurance companies and takaful operators, the relevant controls under Appendix 11 should be applied on a risk-based and proportionate basis, where appropriate.

In determining the extent to which the relevant Appendix 11 controls should be applied, financial institutions should consider the nature of services offered, customer journey, transaction initiation and approval mechanisms, fraud risk exposure, existing authentication controls, and potential customer impact. Where relevant fraud risks are identified, financial institutions should adopt appropriate fraud detection and customer protection controls, supported by documented risk assessment, internal governance and periodic review.

67. With regards to requirement in Appendix 11, paragraph 3, what are the expectations for financial institutions in detecting and terminating hijacked sessions?

Financial institutions are expected to implement robust and adaptive measures to safeguard interactions and digital services against evolving threats. Financial Institutions should be capable of identifying anomalous behaviours that may indicate hijacked sessions or compromised devices, and take appropriate action to mitigate risks, including terminating suspicious sessions when necessary.

Threat actors often employ various techniques to gain control over customer devices and impersonate legitimate users. Common methods include alluding customers to install sideloaded applications, facilitating screen overlay attacks, utilizing screen mirroring, or leveraging remote access and keylogging tools.

To counter these threats, in alignment with paragraph 2(a) of Appendix 4, financial institutions should ensure digital services are able to block the threats and continuously enhance their security measures to align with the rapidly changing threat landscape. This entails investing in advanced capabilities to protect customers from sophisticated scams and ensuring that their cybersecurity controls remain effective, resilient, and responsive.

RMiT Policy Document Revision History

Version No.	Effective Date	Summary of Changes
1.0	18 July 2019	Initial policy creation.
2.0	19 January 2020	Key updates to the policy document dated 19 January 2020 includes: i. Refine notification requirements and supervisory processes for non-material enhancements (*paragraph 14.3 and 14.7*); and ii. Expand the items in Category 1 and Category 3 of the Appendix 6 - Positive List for Enhancement to Electronic Banking, Internet Insurance and Internet Takaful Services.
3.0	1 June 2023	Key updates to the policy document dated 1 June 2023 includes: i. Additional guidance to strengthen financial institution's cloud risk management capabilities (*paragraph 10.50*

		and Appendix 10 - Key Risks and Control Measures for Cloud Services); ii. Shift to a risk-based approach in cloud consultation and notification, with corresponding updates in the risk assessment and submission requirement process (*section 15 - Consultation and Notification related to Cloud Services*); and iii. Update cross references, including the multi-factor authentication (MFA) security control denoted as a standard requirement (*paragraph 10.68 and 10.70*).
4.0	28 November 2025	Key updates to the policy document dated 28 November 2025 include the following: i. Expand the applicability to include non-bank Merchant Acquirer (MAs) and Intermediary Remittance Institution (IRIs) with more than 5% market share of transaction value or volume; ii. Enhance financial institutions' resilience to service disruptions including – a. Establish customer impact tolerance in FI's risk appetite (*paragraph 8.6*) b. Elevate CISO's qualification and capabilities (*paragraph 9.4*) c. Enhance requirement on enterprise technology architecture framework and processes (*paragraph 10.4*) d. Providing a structured pathway for capacity building in managing intermittent or service degradation (*paragraph 10.31*) e. Promoting a customer-centric approach to manage service disruptions (*paragraph 10.31 and 10.35*) f. Introduce isolated recovery environment to enhance resumption capability against destructive cyber-attacks (*paragraph 10.45*) iii. Augment baseline security across the industry by – a. Extending baseline security requirements beyond large financial institutions to mitigate systemic risk b. Elevate security controls in line with global standards and best practices (Section 10 – Technology Operation Management and Section 11 – Cybersecurity Management); and c. Enhance cyber supply chain risk management (paragraph 10.47); and

		d. New continuous control monitoring over third parties' cyber security posture (paragraph 10.49) iv. Strengthen the security of digital services through stronger fraud detection, proactive monitoring and customer empowerment (*section 12 – Digital Services*); and v. Facilitate the secure adoption of new and advanced technologies by – a. Enhancing simplified approach for mature technology *(section 16 - Notification for Technology-Related Applications)*; and b. Streamlining the cloud consultation process for emerging technologies (*section 17 - Consultation and Notification related to Cloud Services and Emerging*). c. Introducing new guidance on emerging technologies *(Appendix 9)*

Refinements to this FAQ may be updated by BNM from time to time. Financial institutions with additional queries related to the RMiT policy document should engage their respective IT Supervisors.