BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Technology Requirements for Payment Services Regulatees

Frequently Asked Questions

Issued on: 17 September 2026

Introduction

This Frequently Asked Questions (FAQ) document is designed to guide payment services regulatees (PSRs) in interpreting and implementing the requirements set out in the Technology Requirements for PSRs policy document (TR PD) issued on 12 March 2026. 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 TR PD**, rather, it serves as a complementary reference to promote consistent understanding and application across the industry.

Interpretation

1. Will the applicability of TR PD be extended to overseas entities of local PSRs?

TR PD applies to the regulated activities and operations of the PSR within its regulatory scope. Where a PSR has overseas branches or related entities, BNM encourages the adoption of equally sound and robust technology risk management and cybersecurity practices across the wider organisation, taking into account the nature, scale and risk profile of those operations.

2. 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) Payment Systems:
   i. Mobile payments (e.g. DuitNow QR)
   ii. Payment gateway (e.g. FPX)
   iii. Remittance system
   iv. e-wallet
b) Self-service Terminals;
c) Payments related mobile application system;
d) Call Centre; and
e) Fraud risk management system.

The list of critical systems provided is not exhaustive. PSR must assess and determine whether other systems qualify as “critical systems” to its payment services business, considering the potential impact of a system failure to customers, business operations, reputation or compliance with regulatory requirements and laws. PSR may also consult BNM for clarification on the classification of a specific system.

3. Can a PSR leverage controls previously implemented based on RMiT standards to meet the requirements of TR PD?

Yes. The foundational technology risk management and cybersecurity under RMiT remain applicable, and may be leveraged to meet the corresponding

requirements in TR PD. In addition, a PSR must comply with the additional requirements set out in paragraphs 2.7 and 13.3 of the TR PD, while Appendix 10 is applicable only to PSR that conduct merchant acquiring business.

4. **What is the process for notifying PSRs of their tier classification, and how will they know whether they have been classified as Tier 1, Tier 2 or Tier 3?** *[Paragraph 2.4]*

   For Tier 1, the Bank will notify the approved E-Money Issuer (EMI), registered Merchant Acquirer (MA) or Intermediary Remittance Institution (IRI) if it meets the relevant criteria set out in paragraph 5.2 of the RMiT Policy Document. This notification serves as confirmation that the identified EMI, MA or IRI falls within the scope of RMiT and must comply with the requirements in that Policy Document. Similarly, PSRs will be notified by the Bank in writing if they no longer fulfil the eligibility criteria for the application of RMiT.

   For Tier 2 and Tier 3, PSRs may generally determine their own tiering based on the criteria prescribed in paragraph 2.4 of the TR PD and the relevant data submitted to the Bank via STATsmart. Unlike RMiT, which relies on market share, the TR PD tiering criteria are based on prescribed thresholds. Where there is uncertainty, PSRs are encouraged to consult BNM for confirmation.

5. **If a PSR has non-regulated business (e.g. providing technology services to other organization, or acting as an agent), what should be done if a cyber risk or incident impacts these activities?** *[Paragraph 2.7]*

   Pursuant to paragraph 2.7, PSRs that conduct both regulated and non-regulated businesses within the same regulated entity must perform continuous risk assessment and put in place appropriate controls to ensure that the non-regulated business does not create contagion risk to, or compromise, the regulated business.

   In the event of a cyber incident affecting the non-regulated business, the PSR must contain the adverse impact of the incident on its regulated business activities and notify BNM accordingly.

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

Responsibilities of the Board of Directors

7. Can a PSR 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 TR PD after taking into consideration the complexity of the PSR's operations, risk profile as well as the local entity business environment. The PSR's board must provide oversight and ensure the adequacy of these plans.

8. Can a board of PSR leverage on any existing board committee to perform oversight on technology-related matters? *[Paragraph 8.3]*

Yes. The board of a PSR 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.

9. 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 expected 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 PSRs, 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

10. **How should PSRs 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]*

    PSRs 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, PSRs should rely on reasonable estimates derived from available real-time data.

    PSRs are expected to work closely with key third party service providers to strengthen real-time monitoring capabilities for critical digital services. During a disruption, PSRs 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, PSRs 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)

11. **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 PSR's ability to recover critical services under more severe and plausible stress conditions (e.g. cyber-attacks causing data corruption or data breaches).

    Accordingly, PSRs 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)

12. Does CISO need to be locally employed and physically based in Malaysia, or can the CISO be based outside Malaysia (for example, located in the UK while being employed under the Malaysian legal entity)? *[Paragraph 9.5]*

For a PSR subject to RMiT PD requirements, please refer to RMiT FAQ item 11.

While the appointment by the Malaysian entity is essential to ensure CISO directly reports to the local Board and senior management, the operationalization of the function may not need necessarily be physically based in Malaysia provided that effective oversight, clear accountability, and adequate visibility over the Malaysian entity's technology and cyber risk profile are maintained.

Where the designated CISO is located outside Malaysia, the PSR shall ensure that this individual remains readily accessible at least during local working hours and available to discharge their oversight, decision-making, and escalation responsibilities, particularly during technology and cybersecurity incidents affecting the Malaysian entity.

The PSR shall also ensure that any cross-border arrangement does not impair the effectiveness of incident response, crisis management, or engagement with BNM.

13. Can PSRs leverage group-level CISO? *[Paragraph 9.5]*

For a PSR subject to RMiT PD requirements, please refer to RMiT FAQ item 11.

BNM generally expects Tier 2 and Tier 3 PSRs to appoint and designate an entity-level CISO (by whatever name called) who is accountable for technology and cyber risk management within the Malaysian entity. The entity-level designation ensures that a competent CISO with sufficient capacity is responsible for ensuring the PSRs' information assets and technologies are adequately protected to preserve operational integrity and business continuity.

PSRs may leverage a Group-level CISO, i.e. through dual-appointment arrangements, if it assesses that its technology risk profile does not warrant an entity-level CISO *and* provided that such arrangements preserve entity-level governance and operational integrity. The PSR shall ensure that the designation is supported by clear and documented accountability arrangements, including defined roles and responsibilities, decision-making authority, reporting lines, and escalation mechanisms for matters affecting the Malaysian entity. The PSR shall be able to demonstrate that accountability for

the management of the Malaysian entity's technology and cyber risks remains clearly assigned, readily identifiable, and enforceable at all times. However, BNM may rescind this flexibility granted including requiring the PSR to designate an entity-level CISO if elevated risks are observed during BNM's supervisory activity.

14. **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 9.5]*

    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 PSR's technology profile. For example, a CISO should be well-versed in cloud technologies for a PSR 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)

15. **How should PSRs 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]*

    For a PSR subject to RMiT PD requirements, please refer to RMiT FAQ item 13.

    In order to strengthen their cyber resilience, Tier 2 and Tier 3 PSRs are encouraged to 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.

    PSRs 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.

16. **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]*

For a PSR subject to RMiT PD requirements, please refer to RMiT FAQ item 14.

The intent of paragraph 10.15 is to strengthen the PSRs' 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, PSRs may 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

17. **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 PSRs 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 PSR environment[1]. To mitigate such vulnerabilities, PSRs 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.

18. **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. PSRs are expected to ensure timely implementation of permanent fixes to defend against accelerated vulnerabilities discovery by frontier technologies.

---

[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] openeox-standardization-framework-technical-report.pdf

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

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

TR PD does not prescribe a specific methodology for calculating unplanned downtime. PSRs 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.

PSRs 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
2. Nov 2024 – Nov 2025: 5 hours
3. June 2025 – June 2026: ≥5 hours
4. November 2025 – November 2026: ≥3 hours

A PSR is considered compliant with the cumulative unplanned downtime requirement if its cumulative unplanned downtime remains within the internal threshold established under paragraph 10.32 of the TR PD.

20. 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? *[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.

PSRs 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

21. 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 PSRs' tolerable disruption level.

Based on globally[3] 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 PSRs' risk profile and sufficient to prevent compromise of the recovery environment, ensuring it remains trusted even if the production systems are affected.

22. Does tape backup with a combination of controls to achieve tamper-proof fulfil the requirement of paragraph 10.45?

The use of tape backup in combination with robust controls may fulfil the requirement, provided PSRs can demonstrate the overall arrangement is tamper-resistant and resilient against destructive cyber-attacks, including ransomware. At a minimum, PSRs 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.

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

Continuous Control Monitoring

23. 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 PSR 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.

24. How should PSRs 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]*

PSRs 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. PSRs should assess exposure points across their technology environment, including interfaces, APIs, and outsourced services.

To demonstrate effective management of external exposure risks, PSRs 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 PSRs' risk profile and sufficient to mitigate potential cyber-attack surfaces arising from external exposures.

25. How should PSRs 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]*

PSRs 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

26. 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.

27. 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, PSRs must implement MFA for authenticating user access to critical internal systems. For non-critical systems, PSRs may consider MFA based on risk assessment.

28. 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 PSRs are expected to select authentication methods with sufficient security strength to fully meet the requirement.

Cyber Risk Management

29. 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 PSRs may leverage or combine these exercises for cost effectiveness, PSRs 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.

PSRs must ensure that any combined or coordinated approach remains risk-based, proportionate, and aligned with supervisory expectations. Where there is any uncertainty, PSRs 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.

30. Is a PSR required to establish an in-house Security Operations Centre (SOC)? *[Paragraph 11.9]*

TR PD does not prescribe a specific operating model for SOC. PSRs may adopt an in-house, third-party, or hybrid SOC model, as long as it facilitates proactive monitoring and timely detection of anomalies across their technology infrastructure, and meets all requirements stipulated in the PD.

PSRs remains accountable for the effective monitoring and management of cyber threats across all critical systems and infrastructures.

Cyber Response and Recovery

31. Are there any specific expectations for hosting an out-of-band communication channel (e.g. outside the PSR's internal network), and is a paid subscription required? *[Paragraph 11.15]*

PSRs are given the flexibility to determine and establish the specific hosting arrangement for their out-of-band (OOB) communication channel. PSRs 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 PSR'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 PSR's risk profile and operational needs.

32. Are cyber drill exercises and disaster recovery (DR) exercises the same? *[Paragraph 11.16]*

No. While both exercises are intended to test PSRs' preparedness and resilience, they serve distinct but complementary operational objectives.

Cyber drill exercise simulates a cybersecurity incident to assess an organization's ability to detect, respond, contain and recover from cyber threats (e.g. ransomware, phishing attacks, and data breaches), whereas a DR focuses on restoring critical systems, applications and services following a disruption or disaster (e.g. natural disaster, hardware failures, system and power outages).

While a cyber incident scenario may involve the activation of DR arrangements, cyber drill exercises and DR generally conducted to meet different testing objectives and requirements.

Locally, most organization conduct cyber drills and DR testing separately. Only a few have integrated DR failover into cyber exercises by switching production systems to a secondary site under simulated attack scenarios.

This suggests that integrated cyber resilience testing remains nascent, although some institutions are adopting a more holistic approach that combines cyber incident response and technology recovery.

PSRs retain the flexibility to implement complementary activities to further strengthen service resilience.

Digital Fraud Management and Customer Awareness

33. Are PSRs 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]*

PSRs 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, PSRs 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 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, security controls or business processes. PSRs 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.

34. Is a PSR 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]*

PSR are expected to provide customer with a practical means to verify authenticity of callers, typically through verification feature integrated with mobile application.

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

35. 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 PSRs, such as identifying phishing messages, verifying legitimate channels, or recognising when not to share credentials).

BNM has no objection to PSRs using awareness videos as part of their broader customer awareness programme. PSRs 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

Technology Audits

36. Is it permissible to outsource the internal IT audit function? If so, can an Internal Liaison Officer (e.g., a Compliance Manager) be appointed to coordinate with the outsourced service provider? *[Paragraph 13.3]*

Yes, PSRs may outsource the IT audit function as provided under paragraph 13.3. A dual-hatting arrangement is allowed, for example, where a Compliance Head also oversees IT audit function, provided the individual has the requisite skills, expertise and capacity.

The PSR must ensure that the designated IT Audit Head is an employee of the regulated entity and remains accountable for the effective discharge of the IT audit function.

PSRs should ensure that key staff in the outsourced IT audit team are suitably competent, appropriately experienced and professionally certified.

37. Can PSRs appoint internal auditor as IT Audit Head?

Yes, provided that the individual possesses the appropriate competencies and professional certifications, is adequately conversant with the company's technology systems and delivery channels and has sound knowledge of the areas being audited, consistent with Paragraph 13.3 of the TR PD.

38. Can PSRs appoint an external IT auditor to conduct the annual IT audit, or is the Head of IT Audit required to be an in-house employee with day-to-day oversight responsibilities?

There is no explicit requirement in the TR PD for the Head of IT Audit to be physically present on a daily basis to monitor or audit the institution's IT systems. A PSR may engage external auditors to perform IT audit reviews; however, the internally appointed Head of IT Audit must retain oversight and accountability for the IT audit function, including setting the audit strategy and plans, determining audit scope, overseeing the conduct of audits, and ensuring that material findings are appropriately reported and escalated to management and the board with adequate monitoring on remedial actions until closure. Audit work performed by external auditors should be subject to the oversight of, and reported through, the Head of IT Audit to ensure clear accountability for the IT audit function.

External Party Assurance

39. 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 PSR’s production and recovery data centres that host critical system. For clarity, PSRs are still required to submit

the DCRA (or equivalent assessment reports) to IT Supervisors for the designated/identified data centres hosting the critical systems, even if the critical systems are hosted regional data centres.

40. 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 PSRs' 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 systems.

Notwithstanding that IT operations may be centrally managed or supported by group function, PSRs remains fully accountable for ensuring compliance with the spirit and intent of the requirements. Hence, PSRs are 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

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

PSRs 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 PSR's risk profile, service criticality, and operating environment.

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

Assessment and Gap Analysis

42. Is there a requirement for the gap analysis to be tabled to the board of the PSR prior to the submission to BNM? *[Paragraph 17.1]*

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

43. Are the PSRs required to submit gap analysis periodically to BNM after the initial submission? *[Paragraph 17.1]*

PSRs are expected to update BNM periodically on their remediation progress based on the timelines committed in the submitted report until all gaps are rectified. This may include:

- Providing periodic updates on implementation status;
- Highlighting any material changes or delays to the agreed timelines; and
- Demonstrating that identified gaps are being progressively addressed according to the remediation plan.

44. Our headquarters is based in Singapore, and as a group we undergo annual audits against the MAS Technology Risk Management (TRM) Guidelines. Can we rely on these audit results instead of conducting a separate TR PD gap analysis? *[Paragraph 17.1]*

PSRs may leverage the audit outcome of their parent group, provided that they can:

- Demonstrate that the parent group has implemented a technology risk and cybersecurity management framework that is aligned with the expectations set out in the TR PD;
- Verify that the control assessments are relevant to the IT systems, infrastructure and services supporting the Malaysian operations, with remedial plans formulated to address any identified gaps; and
- Ensure that the validation is rigorous and comprehensive against the applicable requirements of the TR PD, and adequate to assess the technology risk profile of the Malaysian operation on a standalone basis.

45. Can PSRs leverage its Payment Card Industry Data Security Standard (PCI DSS) certification report for the gap analysis submission? *[Paragraph 17.1]*

Yes. A PCI DSS certification report may be leveraged as supporting evidence for the gap assessment where the report covers technology risk and security controls that are relevant to the requirements set out in the TR PD.

However, the gap assessment should still be conducted against the applicable requirements of the TR PD. As PCI DSS is designed for payment card security and has a different scope and objective, PSRs should assess whether there are any TR PD requirements that are not fully addressed by the PCI DSS assessment and identify any resulting gaps.

Notwithstanding the reliance on PCI DSS assessments results, the PSR remains responsible for demonstrating compliance with the TR PD requirements and ensure that the gap analysis adequately reflects its current level of compliance against the policy document.

Appendix 5: Control Measures on Cybersecurity

46. 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.

47. Where a PSR 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 PSR 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. PSRs 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 PSRs 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. PSRs should ensure that any reuse of threat

intelligence, scenarios or providers does not compromise the integrity and effectiveness of ILPT.

48. 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?

PSRs 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 8: Key Risks and Control Measures for Cloud Services

49. Does Appendix 8 apply to non-critical systems?

PSRs are encouraged to consider the common key risks outlined in Appendix 8 in the implementation of control measures for any cloud adoption. Notwithstanding, BNM does reserve discretion to require a PSR to observe Appendix 8 for non-critical systems.

50. Does Appendix 8 apply in a circumstance where a PSR deploys critical system to hybrid cloud operated by Group of companies and Group owned the data centre and its operations?

Yes, since Appendix 8 is applicable to the scope of critical system operating on public cloud.

51. Can SaaS be exempted from the Appendix 8 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, PSRs should understand the associated risks, identify applicable provisions in Appendix 8 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.

PSRs 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).

52. 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. PSRs should identify the relevant provisions in Appendix 8 when assessing the risks of specialised variation of the cloud service models, e.g., UCaaS is a form of SaaS. PSRs are also encouraged to leverage on industry standards to identify key risk considerations for commonly used cloud service models as they evolve.

53. 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.

54. Can a PSR combine cloud technology risk management framework with the current technology risk framework under TR PD in one documentation?

Yes.

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

Appendix 8 does not preclude PSRs from leveraging group IT services, including master service agreement with cloud service providers for economies of scale.

The PSRs 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 PSRs 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, PSRs should not rely solely on the monitoring and periodic assessment conducted by the group. PSRs 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. PSRs are reminded to ensure legal arrangement is established between itself and its group, as part of its governance process.

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

A PSR is required to ensure that the cloud service provider is capable of securely managing and protecting sensitive information and data. The PSRs 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 PSRs can rely on include but not limited to SOC 1, SOC 2, and ISO 27001.

PSRs 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.

57. 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. PSRs should ensure these skills are maintained and regularly updated through ongoing professional development.

58. Clarification and expectations on multi-cloud strategy

There is a range of service availability and redundancy options for PSRs to achieve operational resilience under various potential scenarios. PSRs 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.

59. Expectations for testing an exit plan

Given increasing reliance of PSRs on cloud service providers to support PSRs' critical day-to-day operations, PSRs 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 8: Exit Strategy.

PSRs 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. PSRs 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.

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

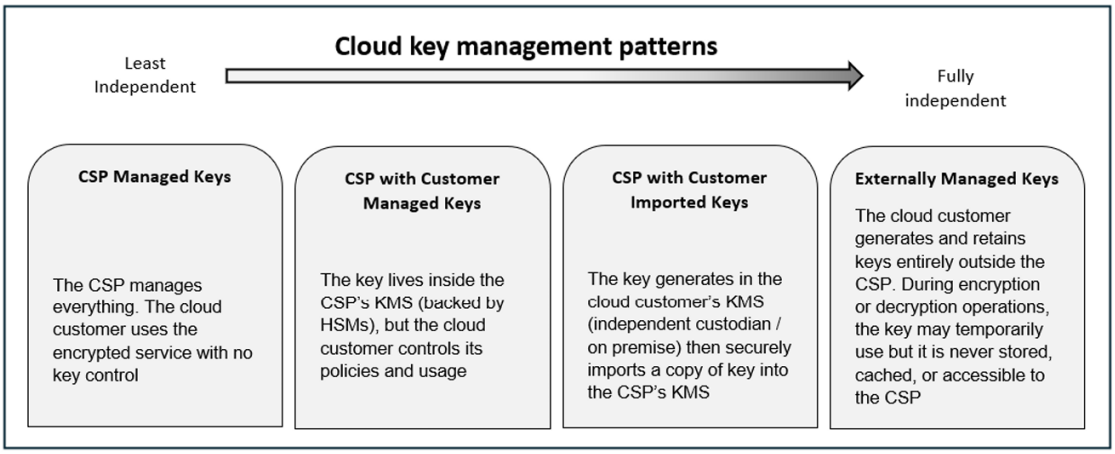
Maintaining independence in cryptographic key management is crucial for systems that handle sensitive or confidential information. As clarified in paragraph 8 of Part (B) Appendix 8: Cryptographic Key Management, possession of encryption keys grants the ability to access the data stored on the servers. 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, PSRs 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 PSRs may face challenges in managing and retaining control of the encryption keys, especially when lacking the necessary resources, expertise, and infrastructure. In such cases, PSRs 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 PSRs must rely on the cloud service provider's key management system, PSRs 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. PSRs 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 9: Fraud Detection Standards

61. With regards to requirement in Appendix 9, paragraph 3, what are the expectations for PSRs in detecting and terminating hijacked sessions?

PSRs are expected to implement robust and adaptive measures to safeguard interactions and digital services against evolving threats. PSRs 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, PSRs 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.

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