BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Technology Requirement for Payment Services Regulatees

Exposure Draft

Applicable to:
1. Approved issuers of electronic money
2. Registered merchant acquirers
3. Licensed money service business
4. Operator of a designated payment system

Draft issued on: 17 December 2024

BNM/RH/ED 040-1

This Exposure Draft (ED) outlines new requirements on the payment services regulatees (PSR)s' management of technology risks to improve the resilience of payment services and enhance system-wide cyber defence. This policy also aims to consolidate all technology requirements for the approved issuers of electronic money (EMI)s, registered merchant acquirers (MA)s and licensed money services businesses (MSB)s into a single policy document.

In developing these expectations, Bank Negara Malaysia (the Bank) has considered local and global IT risk outlooks, areas of improvements identified from IT incidents, and development in industry framework and best practices. This ED aims to:

1. Augment PSRs' resilience by elevating cyber security baseline across the industry and enhancing the state of preparedness to withstand service disruptions;
2. Improve protection against cybercrime while preserving the integrity and availability of payment services; and
3. Facilitate the secure adoption of technology advancement and innovation.

The Bank invites written feedback on the proposed requirements in this ED, including suggestions on areas to be clarified or alternative proposals that can deliver the intended outcomes. Respondents are also invited to provide views on the specific questions to calibrate the applicability, scope and implementation timeline of the new requirements. Please clearly notate the paragraph to which each comment is related to, and provide supporting rationale and evidence or illustrations, where appropriate.

Responses must be submitted electronically in the specified format to the Bank via e-mail to the officers below by 30th April 2025. In the course of preparing your feedback, you may direct any queries to the following officers:

1. Lau Kah Heng (khlau@bnm.gov.my)
2. Nor Alia Syuhada Shaharudin (aliashaharudin@bnm.gov.my)
3. Nur Nadiah binti Md Said (nadiahsaid@bnm.gov.my)

Submissions received may be made public unless confidentiality is specifically requested for the whole or any part of the submission.

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Payment Services Regulatees (PSR)s have played a pivotal role in the rapid growth of payment services. With the prevalent use of technology in the provision of payment services, PSRs must:

(a) invest in the required expertise and risk controls to prevent operational disruptions given the complexity of IT systems;
(b) achieve the highest level of security to combat fast-changing digital crimes to ensure public confidence;
(c) maintain robust oversight to prevent transmission of risks with increased third-party interlinkages;
(d) build operational resilience against sophisticated and malicious cyber threats amidst heightened cyber risks globally; and
(e) practice ethical and responsible use of technology for inclusive growth.

1.2 This policy document sets out the Bank's policy objectives in the management of technology risks by PSRs. The requirements in this policy document will be applied to the PSRs proportionately based on tiering, in order to cater for the diverse risk profiles among the PSRs. In applying this policy document within each tier, a PSR shall have regard to the size and complexity of its operations, the level of technology used and exposure to both external and internal cyber security threats. Accordingly, larger and more complex PSRs are expected to adopt more robust risk controls that commensurate with the increased technology risk exposure of the institution.

1.3 Enforcement or supervisory actions can be taken against the PSRs including its directors, senior management, officers and employees for any non-compliance with any provision marked as "S" in Part B of this policy document.

1.4 Where the Bank considers that PSRs' technology risk management has material weaknesses that might contribute to or result in a breach if not promptly and effectively addressed, among others, the Bank may:

(a) require an independent external party review of the overall or specific areas of the technology risk management;
(b) require PSRs to develop and take specific remediation plan; and/or
(c) take any other action, including corrective action where required.

2 Applicability

2.1 This policy document is applicable to all PSRs as defined in paragraph 5.2.

2.2 Notwithstanding paragraph 2.1, only paragraph 2.7 and Appendix 10 would be applicable for PSRs governed under the Risk Management in Technology Policy Document (RMiT).

2.3 For the avoidance of doubt, Payment System Operators which are regulated under Payment System Operators Policy Document are excluded from the requirements in this Technology Requirement Exposure Draft (TR ED).

2.4 In order to cater for proportionate regulations, PSRs will be tiered as follows:

Tiers	Criteria	Regulations Applied
Tier-1	PSRs that fulfill the criteria for inclusion under RMiT.	RMiT
Tier-2	PSRs with annual transaction value[1,2] of more than RM1.5 billion or annual transaction volume of more than 7 million and not categorised as Tier-4.	TR ED
Tier-3	PSRs with annual transaction value of less than or equal to RM1.5 billion or annual transaction volume of less than or equal to 7 million and not categorised as Tier-4.	TR ED
Tier-4	PSRs who are non-digital money services business licensees[3] carrying on currency exchange business or wholesale currency business.	TR ED

Question 1:
Tiering concept and criteria used

The applicability of the requirements in this TR ED would depend on the tiering of the PSRs, whereby a higher tier would require compliance to stricter requirements as indicated under paragraph 2.6. Hence, PSRs would need to identify the tiering that is applicable to itself based on the

[1] For Tier-2 and 3 PSRs, the annual transaction value or volume for a single entity is summed up for all regulated businesses excluding currency exchange and currency wholesales. E.g. If a PSR is an approved E-Money Issuer (EMI), registered Merchant Acquirer (MA), licensed Remittance Service Provider (RSP) and licensed Currency Exchangers (CE), the annual transaction value/volume will be the sum from the EMI, MA and RSP business only.

[2] The criteria shall be determined every January based on the value or volume for the past calendar year.

[3] Non-digital MSBs refers to the MSBs that do not offer digital services as per definition of "digital services" in paragraph 7.2 of the Governance, Risk Management, and Operations for MSB Policy Document.

specified criteria and ensure compliance to the applicable requirements accordingly. Please provide views or comments on the tiering concept and the criteria used to determine the tiering.

2.5 For purposes of applying paragraph 2.4, the annual transaction value/volume of PSRs that operate payment services businesses in more than one entity within the same group, must be combined when determining the RM1.5 billion (for annual transaction value) or 7 million (for annual transaction volume) threshold, if the entities share the same technology infrastructure or controls[4].

2.6 In applying the requirements applicable for each tier in paragraph 2.4, the treatment for specific types of PSRs are as follows:

(a) Paragraphs 12.6 and 12.8(a) are not applicable for MAs;
(b) Requirements in Appendix 10 are only applicable to MAs;
(c) For Tier-3 PSRs, paragraphs 9.4, 9.6, 10.36, 10.53(d), 11.3(d), 11.9, 11.10(a), 11.16, 11.17 and 12.8(a) as well as their corresponding appendices are treated as “G” instead of an “S”;
(d) Tier-4 PSRs are subject to requirements under paragraph 16 “Simplified Approach” only; and
(e) The requirements under paragraph 16 - "Simplified Approach" do not apply to Tier-1, 2 and 3 PSRs.

2.7 For PSRs that conduct both regulated business and non-regulated business within the same regulated entity, the Bank reserves the right to require the PSRs to:

(a) provide justification, with supporting evidence that its non-regulated business does not cause contagion risk or compromise the regulated business; and
(b) put in place risk mitigation measures or take certain actions to eliminate or reduce any risks or negative impact to its regulated business.

Question 2:
Regulated and non-regulated business

Does your institution conduct both regulated and non-regulated business within the same legal entity? If yes, please provide information on the following:

(a) Services of products offered under the non-regulated business;

(b) Key areas that the non-regulated business share, if any, with the regulated business such as technology infrastructure, policies and procedures, personnel or governance structure; and

[4] An example of entities that share the same technology infrastructure is where two companies under the same group (or are affiliated) placed their systems within the same data center (or cloud environment), sharing the same infrastructure such as network, load balancer, server, etc. Example of controls include firewalls, policies and procedures.

(c) If there are shared key areas under (b) above, please explain the risk mitigation measures or actions currently in place (if any) to eliminate contagion risks or negative impact to the regulated business.

3 Legal provisions

3.1 The requirements in this policy document are specified pursuant to:
(a) Sections 18(2), 33(1), 47(1), 123(1) and 143(2) of the Financial Services Act 2013 (FSA);
(b) Sections 43(1), 57(1), 135(1) and 155(2) of the Islamic Financial Services Act 2013 (IFSA); and
(c) Section 34(2) and 74(1) of Money Services Business Act 2011 (MSBA).

3.2 The guidance in this policy document is issued pursuant to section 266 of the FSA, section 277 of the IFSA and section 74 of the MSBA.

4 Effective date

4.1 This policy document comes into effect immediately after the issuance of the final policy document.

Question 3:
Effective implementation date

The Bank plans for the final policy document to be effective immediately after its date of issuance.

While some of the requirements remains the same as per the E-Money, Merchant Acquiring Services and Governance, Risk Management and Operations (GRMO) policy documents, there are also new requirements and enhancements categorised as “Standard” for Tier-2 and 3 PSRs, which includes paragraphs 8.6, 8.8, 8.9, 10.15, 10.16, 10.19, 10.27, 10.33, 10.34, 10.48, 11.1, 11.2, 11.5, 11.11, 11.12, 11.14, 11.15, 11.18, 11.20, 11.21, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, and 12.9 and their corresponding Appendices.

Are there any specific areas among the requirements in this ED that your institution may require additional time to implement? If yes, please provide:

(a) the relevant paragraphs on the requirements;

(b) strong justification for the additional time needed, with data or evidence or information on costs involved to support your justification, if any; and

(c) the projected time needed for your institution to achieve full compliance.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA or MSBA, as the case may be, unless otherwise defined in this policy document.

5.2 For purposes of this policy document:

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"affiliate" in relation to an entity, refers to any corporation that controls, is controlled by, or is under common control with, the entity;

"board" refers to the board of directors of a PSR, including any committee carrying out any of the responsibilities of the board under this policy document;

"critical system" refers to any application system that supports the provision of payment services, which includes services for issuing e-money, merchant acquiring and money services business, where failure of the system has the potential to significantly impair the PSR's provision of payment services to customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements;

"customer and counterparty information" refers to any information relating to the affairs or, in particular, the account of any customer or counterparty of a PSR in whatever form;

"cyber resilience" refers to the ability of people, processes, IT systems, applications, platforms or infrastructures to withstand adverse cyber events;

"digital services" refers to the provision of payment, remittance, delivered to customers via electronic channels and devices including Internet and mobile devices, self-service terminals, point-of-sale terminals or payment acceptance devices;

"disruption" refers to an unanticipated incident that causes degradation to the normal performance of a business function that would affect a PSR's ability to continue its operations and services to its customers;

"essential services" refers to financial services that are essential to support financial intermediation activities which must continue to be provided by a financial institution in the event of a disruption;

"payment services regulatee" (PSR) refers to:
(a) A non-bank e-money issuer as defined in the policy document on Electronic Money[5];
(b) A non-bank acquirer as defined in the policy document on Merchant Acquiring Services[6];
(c) A money services business licensed under the MSBA; and
(d) An operator of a designated payment system under the FSA and IFSA;

"material technology projects" refers to projects which involve critical systems, the delivery of essential services to customers or counterparties, or compliance with regulatory requirements;

"OTP or one-time password" refers to an alphanumeric or numeric code represented by a minimum of 6 characters or digits which is valid only for single use;

"senior management" refers to the Chief Executive Officer (CEO) and senior officers. This includes, the relevant paragraphs on their roles and responsibilities in the policy documents on "Electronic Money", "Merchant Acquiring Services" and "Governance, Risk Management, and Operations for Money Services Business (MSB)";

"senior officer" refers to a person, other than the CEO or a director, having authority and responsibility for planning, directing or controlling the activities of a PSR, including the Chief Operating Officer, Chief Financial Officer, members of decision-making committees and other persons performing key functions such as risk management, compliance or internal audit; and

"third party service provider" refers to an internal group affiliate or external entity providing technology-related functions or services that involve the transmission, processing, storage or handling of confidential information pertaining to the PSR or its customers. This includes cloud computing software, platform and infrastructure service providers.

[5] For ease of reference, a "non-bank e-money issuer" refers to an e-money issuer which is not a licensed bank, licensed Islamic bank, or a prescribed institution as defined under the Development Financial Institution Act 2002. Whereas "e-money issuer" refers to any person approved by the Bank under section 11 or section 15(1)(e) of the FSA or section 11 of the IFSA to issue e-money.

[6] For ease of reference, a "non-bank acquirer" refers to any person who is not a licensed bank, licensed Islamic bank or prescribed institution that is registered pursuant to sections 17(1) and 18 of the FSA to provide merchant acquiring services and fulfils the criteria under paragraph 2.1 of the policy document on Merchant Acquiring Services.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with any relevant legal instruments, policy documents, guidelines, circulars, and supplementary documents issued by the Bank, including any amendments and reissuances thereafter, in particular:

(a) Policy Document on Electronic Money (E-Money);
(b) Policy Document on Merchant Acquiring Service;
(c) Policy Document on Governance, Risk Management, and Operations for Money Services Business (MSB);
(d) Policy Document on Interoperable Credit Transfer Framework;
(e) Management of Customer Information and Permitted Disclosures (MCIPD);
(f) Policy Document on Fair Treatment of Financial Consumers;
(g) Guideline on Complaints Handling;
(h) Guidelines on Product Transparency and Disclosure;
(i) Policy Document on Risk-Based Authentication for Online Payment Card Transaction; and
(j) Policy Document on Payment Card Reform Framework.

7 Policy documents and circulars superseded

7.1 This policy document supersedes the IT requirements under the following policies:

(a) Paragraphs 30 to 34 of the Policy Document on Governance, Risk Management, and Operations for Money Services Business (MSB);
(b) Paragraphs 27 to 31 of the Policy Document on Electronic Money (E-Money); and
(c) Paragraphs 17 to 22 of the Policy Document on Merchant Acquiring Services.

The rest of the page is intentionally left as blank.

PART B POLICY REQUIREMENTS

8 Governance

Responsibilities of the Board of Directors

S 8.1 The board must establish and approve the technology risk appetite which is aligned with the PSR's risk appetite statement. In doing so, the board must:

(a) approve the corresponding risk tolerances for technology-related events considering potential impact on business operations as well as its customers;

(b) identify risk owner to ensure clear accountability and establish criteria and approving authority for the acceptance of residual risks by the institution;

(c) ensure key performance indicators are identified to monitor existing and emerging risks against PSR's risk tolerance;

(d) ensure sufficiency and appropriate deployment of resources; and

(e) conduct review of the technology risk appetite at regular intervals with sufficient deliberation to ensure such risk appetite remains relevant with changing risk environment.

S 8.2 In discharging its oversight responsibility, the board must:

(a) approve and review the adequacy of the PSR's IT and cybersecurity strategic plans to meet business objectives covering a period of no less than three years;

(b) endorse and oversee the effective implementation of a sound and robust technology risk management framework (TRMF) and cyber resilience framework (CRF), as required to be developed under paragraphs 9.1 and 11.2, for the continuity of operations and delivery of financial services;

(c) require senior management to continuously demonstrate that risk assessments undertaken in relation to critical IT systems and use of emerging technology are robust and comprehensive, supported with adequate control measures and resources to mitigate IT and cyber risks arising from the execution of IT strategic plans;

(d) ensure IT-related framework, policies and guidelines are reviewed at least once every three years (unless otherwise stated in this policy document) and apply the depth of review that is commensurate with the complexity of the PSR's operations and changes in the risk environment; and

(e) ensure robust risk assessments are undertaken in relation to material technology applications submitted to the Bank.

G 8.3 The board may designate a board-level committee[7] which shall be responsible for supporting the board in providing oversight over technology-related matters.

[7] 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

S 8.4 To promote effective discussions at the board level, the board must undertake appropriate awareness education and training on IT and cybersecurity matters and obtain regular updates on technology risk and cyber threat development.

G 8.5 In addition to paragraph 8.4, PSRs are encouraged to include at least a member with technology experience and competencies as part of the composition of its board or the designated board-level committee.

Question 4:
Designation of a board-level committee

(a) Does your institution anticipate any challenges in meeting the requirements outline in paragraphs 8.3 and 8.5 if such requirements are made mandatory (i.e. as "S" instead of "G")? If yes, please explain the challenges.

(b) What alternative measures could ensure effective board oversight over technology-related matters?

S 8.6 Given the rapidly evolving cyber threat landscape, the board shall allocate sufficient time to discuss cyber risks and related issues, including the strategic, reputational and liquidity risks[8] associated with extreme or adverse cyber-incident. This shall be supported by input from external experts as appropriate.

S 8.7 The board or the board audit committee (BAC), if a BAC is established, shall be responsible for ensuring the effectiveness of the internal technology audit function. This includes ensuring the adequate competence of the audit staff to perform technology audits. The board or BAC shall review and ensure appropriate audit scope, procedures and frequency of technology audits. The board or BAC shall also ensure effective oversight over the prompt closure of corrective actions to address technology control gaps.

Responsibilities of the senior management

S 8.8 The senior management shall bear primary responsibility for the day-to-day management of technology risk including cyber risks. In fulfilling its responsibilities, senior management must:

(a) implement board approved TRMF and CRF into specific policies and procedures that are consistent with the approved risk appetite and risk tolerance;

(b) assess and establish customer impact tolerance level for essential services disruption and consider it in the triggers for escalation in its crisis management plan, based upon:

(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.

[8] For instance, rapid outflow of funds following a major cyber incident.

(i) duration of disruption;
(ii) number of customers affected by a disruption; and
(iii) number and value of financial transaction impacted.

(c) allocate and prioritise skilled resources to mitigate high-impact risks to maintain robust technology systems and appropriately skilled and competent staff to support the effective management of technology;

(d) identify appropriate organization structure to support effective enterprise-wide oversight of technology risk. These arrangements must provide for designated staff responsible for the identification, assessment and mitigation of technology risks who do not engage in day-to-day technology operations to achieve practical level of independence; and

(e) provide regular updates to the board on the status of key performance indicators with pertinent information on the risk controls to facilitate informed performance review.

S 8.9 The senior management must establish a cross-functional committee to provide guidance on the PSR's technology plans and operations. The members of the committee must include senior management from both technology functions and major business units. The committee's responsibilities shall include the following:

(a) oversee the formulation and effective implementation of the strategic technology plan and associated technology policies and procedures;

(b) provide timely updates to the board on key technology matters[9];

(c) approve any deviation from technology-related policies after having carefully considered a robust assessment of related risks; and

(d) Report any material deviations to the board.

Question 5:
Cross-functional committee

Does your institution anticipate any challenges in fulfilling the requirement in paragraph 8.9? If yes, please explain:

(a) The potential challenges, with clear justification for such challenges; and

(b) Alternative control measures to ensure effective senior management oversight over technology-related matters, if any.

[9] Key technology matters include updates on critical systems' performance, significant IT and cyber-incidents, management of technology obsolescence risk, status of patch deployment activities for critical technology infrastructure, proposals for and progress of strategic technology projects, performance of critical technology outsourcing activities, utilisation of the technology budget and competencies for managing technology risks.

9 Technology Risk Management

Risk Management Framework

S 9.1 A PSR must ensure that the TRMF is an integral part of the PSR's enterprise risk management framework (ERM).

S 9.2 The TRMF must include the following:

(a) clear definition of technology risk;
(b) clear responsibilities assigned for the management of technology risk at different levels and across functions, with appropriate governance and reporting arrangements;
(c) the identification of technology risks to which the PSRs is exposed, including risks from the adoption of new or emerging technology (refer Appendix 7 on Guidance for Emerging Technologies);
(d) risk classification of all information assets/systems based on its criticality;
(e) risk measurement and assessment approaches and methodologies;
(f) risk controls and mitigations;
(g) continuous monitoring to timely detect and address any material risks;
(h) effective information system to ensure the technology risk profile remain accurate and up to date;
(i) identification of key resources and interdependencies (including critical third-party service providers and their connected parties) which support delivery of critical functions;
(j) undertake scenario analysis to strengthen capacity and readiness to resume critical services in the severe events; and
(k) effective incident management policies and procedures with the objective of restoring an affected IT services or system to a secure and stable state, as quickly as possible, so as to minimise impact to the PSR's business and customer.

S 9.3 A PSR must establish an enterprise-wide technology risk management function which is responsible for:

(a) implementing the TRMF and CRF;
(b) advising on critical technology projects and ensuring critical issues that may have an impact on the PSR's risk tolerance are adequately deliberated or escalated in a timely manner; and
(c) providing independent views to the board and senior management on third party assessments[10], where necessary.

S 9.4 The enterprise-wide technology risk management function shall be assigned to staff that are independent from the day-to-day operations and functions.

[10] Relevant third-party assessments may include the Data Centre Risk Assessment (DCRA), Network Resilience and Risk Assessment (NRA) and independent assurance for introduction of new or enhanced digital services.

Designated Chief Information Security Officer

S 9.5 A PSR must designate a Chief Information Security Officer (CISO), by whatever name called, to be responsible for the technology risk management function of the PSRs. The PSR must ensure that the CISO has sufficient authority and resources[11]. The CISO shall:

(a) apprise board and senior management of current and emerging technology risks which could potentially affect the PSR's risk profile;

(b) has the requisite technical skills in emerging and core technologies used by the institution, expertise and experience in audit, governance and risk management, strategic planning and execution of IT and cybersecurity programs, and third-party risk management; and

(c) be appropriately certified.

S 9.6 The PSR must ensure that the CISO shall be independent from day-to-day technology operations.

S 9.7 The CISO shall be responsible for ensuring that the PSR's information assets and technologies are adequately protected, which includes:

(a) formulating appropriate policies for the effective implementation of TRMF and CRF;

(b) enforcing compliance with these policies, frameworks and other technology-related regulatory requirements; and

(c) advising senior management on technology risk and security matters, including developments in the PSR's technology security risk profile in relation to its business and operations.

Question 6:
Independence of enterprise-wide technology functions and CISO

Would your institution be able to designate a staff/team who would be independent (i.e. does not engage in day-to-day technology operations, management or development), for the following functions:

(a) Enterprise-wide technology management function as per paragraph 9.4; and

(b) CISO as per paragraph 9.6.

If no, please provide the reasons with clear justification and the alternative control for the requirements in (a) and (b) above.

[11] A PSR's CISO may take guidance from the expertise of a group-level CISO, in or outside of Malaysia, and may also hold other roles and responsibilities provided these do not impair the CISO's independence or competence. Such designated CISO shall be accountable for and serve as the point of contact with the Bank on the PSR 's technology-related matters, including managing entity-specific risks, supporting prompt incident response and reporting to the PSR's board.

10 Technology Operations Management

Technology Project Management

S 10.1 A PSR must establish appropriate governance requirements commensurate with the risk and complexity[12] of technology projects undertaken. This shall include project oversight roles and responsibilities, authority and reporting structures, and risk assessments throughout the project life cycle.

S 10.2 The risk assessments shall identify and address the key risks arising from the implementation of technology projects. These include the risks that could threaten successful project implementation and the risks that a project failure will lead to a broader impact on the PSR's operational capabilities. At a minimum, due regard shall be given to the following areas:

(a) the adequacy and competency of resources including those of the vendor to effectively implement the project. This shall also take into consideration the number, size and duration of significant technology projects already undertaken concurrently by the PSR;

(b) the complexity of systems to be implemented such as the use of unproven or unfamiliar technology and the corresponding risks of integrating the new technology into existing systems, managing multiple vendor-proprietary technologies, large-scale data migration or cleansing efforts and extensive system customisation;

(c) the adequacy and configuration of security controls throughout the project life cycle to mitigate cybersecurity breaches or exposure of confidential data;

(d) the comprehensiveness of the user requirement specifications to mitigate risks from extensive changes in project scope or deficiencies in meeting business needs;

(e) the robustness of system and user testing strategies to reduce risks of undiscovered system faults and functionality errors;

(f) the appropriateness of system deployment and fallback strategies to mitigate risks from prolonged system stability issues; and

(g) the adequacy of disaster recovery operational readiness following the implementation of new or enhanced systems.

S 10.3 The board and senior management must receive and review timely reports on the management of these risks on an ongoing basis throughout the implementation of significant projects.

System Development and Acquisition

S 10.4 A PSR must establish a framework to guide the design, planning, implementation and governance of an enterprise technology architecture. A technology architecture serves as a foundation on which PSRs plan and

[12] For example, large-scale integration projects or those involving critical systems should be subject to more stringent project governance requirements such as more frequent reporting to the board and senior management, more experienced project managers and sponsors, more frequent milestone reviews and independent quality assurance at major project approval stages.

structure system development and acquisition strategies to meet business goals and thus, the PSR must ensure the framework carries out these functions:

(a) provides a comprehensive view of technology throughout the PSR, baseline architecture components and key rationale for their use;

(b) is an overall technical design and high-level plan that describes the PSR's technology infrastructure, systems' inter-connectivity and dependencies (e.g. fallback facility), and security controls. These outlined information are critical to support identification of single point of failure (SPOF);

(c) contains mapping to supported business functions, organisation units, applications, and data to enable business impact analysis (BIA);

(d) defines principles and guideline to govern the design and maintenance of the network infrastructure, related technology controls and IT security policies; and

(e) outline longer-term priorities to guide its evolution.

S 10.5 A PSR must adopt a methodology for an effective and secure implementation of IT systems. Key phases of System Development Life Cycle (SDLC) shall include requirement, design, development, testing, deployment, change management, maintenance, and decommissioning, and integrate with:

(a) enterprise architecture to ensure successful execution of business strategy;

(b) risk management policies and practices to achieve business objectives; and

(c) security principles[13] and requirements to ensure confidentiality, integrity, and availability of customer information.

S 10.6 A PSR must meet enterprise security, governance and compliance requirements when using rapid system development methodology[14]. Given the dynamic environment can increase likelihood of errors, a PSR shall automate the IT security compliance review to prevent unauthorised access as well as the discovery, remediation and testing of security vulnerabilities, to ensure secure release of new IT services.

S 10.7 A PSR shall segregate the production environment from the development and testing environment to mitigate risk of unauthorised changes to the production systems. Where a PSR is relying on a cloud environment, the PSR shall ensure that these environments are not running on the same virtual host.

[13] The security considerations shall include ensuring appropriate segregation of duties throughout the SDLC.

[14] Such as DevOps which is a set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the systems development life cycle and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives.

S 10.8 A PSR must establish a sound methodology for rigorous system testing prior to deployment. The testing shall ensure that the system meets user requirements and performs robustly. Where sensitive test data is used, the PSR must ensure proper authorisation procedures and adequate measures to prevent their unauthorised disclosure are in place.

G 10.9 The scope of system testing referred to in paragraph 10.8 may include unit testing, integration testing, user acceptance testing, application security testing, stress and load testing, and exception and negative testing, where applicable.

S 10.10 A PSR must ensure any changes to the source code of critical systems are subject to adequate source code reviews to ensure code is secure and was developed in line with recognised coding practices prior to introducing any system changes.

S 10.11 A PSR must establish appropriate procedures to independently review and approve system changes. The PSR must also establish and test contingency plans in the event of unsuccessful implementation of material changes to minimise any business disruption.

S 10.12 In relation to critical systems that are developed or maintained by third party service provider, a PSR must, through contractual obligations, require third party service provider to:

(a) provide sufficient notice to the PSR before any changes are undertaken that may impact the IT system;

(b) demonstrate that it adopts secure by design principles in IT system development methodology to mitigate cyber risks from propagating across the supply chain; and

(c) ensure the source code continues to be readily accessible for business continuity.

S 10.13 When decommissioning critical systems, a PSR must ensure minimal adverse impact on customers and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

G 10.14 A PSR may deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to facilitate timely security assessment of critical systems in keeping with growing complexity in IT systems and emerging cyber threats.

S 10.15 Where third-party software is used, a PSR shall consider the potential risks and impacts a cyber supply chain incident may pose to its overall business operations and services. A PSR shall consider, at the minimum:

(a) adopting Software-Bill-of-Material (SBOM)[15] to automate the identification and continuous monitoring of potential security vulnerabilities including security issues associated with third-party software components; and

(b) establishing open-source software security policy and procedures. This includes ensuring secure access to source code repositories in third-party platforms, regular monitoring to prevent data leakages, adoption of secure coding practices, robust testing of open-source software and timely vulnerability assessment to mitigate security vulnerabilities and propagation of malwares across supply chain.

Question 7:
Cyber supply chain

(a) Does your institution anticipate any challenges in meeting the requirements outlined in paragraph 10.15 (in particular 10.15(a))? If yes, please describe the challenges and the potential costs involved.

(b) Instead of the requirements in paragraph 10.15(a), what alternative proposals could ensure effective:
- software component management?
- visibility into your institution's environment?

S 10.16 A PSR must identify and reduce shadow IT[16] risks and commit to a plan to ensure all technology use and IT system development are governed in its technology risk management framework.

Patch and End-of-Life System Management

S 10.17 A PSR must ensure that all systems including digital services are not running with known security vulnerabilities[17], on outdated platform or end-of-life (EOL) technology systems. In this regard, a PSR must:

(a) maintain current security baseline for the security hardening of technology components and ensure the security baseline is accurate and up to date;

[15] Software Bill of Material (SBOM) refers to a formal record containing the details, and the various components used in building a software product including its related supply chain relationships. SBOM provides increased transparency, provenance, and speed at which vulnerabilities can be identified and remediated across the SDLC.

[16] Shadow IT refers to unauthorised use of hardware, software, or other systems and services within a company, commonly without the information technology (IT) department's approval, knowledge, or oversight.

[17] Known security vulnerability refers to a documented flaw or weakness in a system that are publicly disclosed or catalogued in databases such as the National Vulnerability Database (NVD) or Common Vulnerabilities and Exposures (CVE) list.

(b) continuously monitor and implement latest patch releases in a timely manner;
(c) identify, plan and implement remedial action for technology systems that are approaching EOL; and
(d) obtain management approval for any exception permitting the continued use of unsupported or outdated technology. This exception must be substantiated by a thorough risk assessment with clear timeline for phasing out the outdated technology and are regularly reviewed at least on annual basis to ensure associated risks are effectively managed.

S 10.18 A PSR must establish a patch and EOL management framework which addresses among others the following requirements:
(a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;
(b) formulation of criteria, priority and turnaround time for patch deployment according to the severity of the vulnerabilities identified;
(c) conduct of compatibility testing prior to the deployment of patches to minimize disruption to connected systems;
(d) adherence to the workflow for end-to-end patch deployment processes including approval, testing, monitoring and tracking of activities; and
(e) end-user awareness for orderly transition.

S 10.19 A PSR must continually monitor the effectiveness and security of the technology in use, incorporating developments in technology that may disrupt existing security controls[18]. A PSR must:
(a) ensure its board receives sufficient advice on the potential impact to business operation arising from evolving technology landscape;
(b) formulate long-term strategy to address anticipated changes with allocation of competent resources to manage associated risks, including new cyber adversary tactics and techniques; and
(c) establish roadmap for system migration to preserve security and reliability of the technology infrastructure in an orderly manner.

Cryptography

S 10.20 A PSR must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. This policy, at a minimum, shall address requirements for:
(a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;
(b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;

[18] Such as quantum computing.

(c) the periodic review, at least annually, of all cryptographic standards and algorithms currently in use for critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols;
(d) the expansion of IT asset inventory to include all cryptographic tools and algorithms in use with pertinent information on the rationale for each cryptographic method employed and its mapping to supported application systems; and
(e) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

S 10.21 A PSR must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Additionally, a PSR must ensure the following:
(a) except for non-critical systems or applications that do not contain customer data, the PSR must retain ownership and control of the encryption keys (themselves or with an independent key custodian) to minimize the risk of unauthorised access to the data;
(b) where the PSR does not generate its own encryption keys, the PSR shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys securely including adhere to relevant industry standard;
(c) where this involves a reliance on third party assessments[19], the PSR shall consider whether such reliance is consistent with the PSR's risk appetite and tolerance; and
(d) the PSR must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.

Question 8:
Ownership and control of encryption keys

Does your institution anticipate any challenges in fulfilling the requirement set out in paragraph 10.21(a)? If yes, please explain:

(a) the challenges, with clear justification for such challenges; and
(b) alternative control measures, if any.

S 10.22 A PSR must ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols shall include secret and public cryptographic key protocols, both of which shall reflect a high degree of protection to the applicable secret or private

[19] For example, where the PSR is not able to perform its own validation on embedded cryptographic controls due to the proprietary nature of the software or confidentiality constraints.

cryptographic keys. The selection of such protocols must be based on recognised international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation must be undertaken in a protected environment, supported by a hardware security module (HSM), trusted execution environment (TEE) or similarly secured devices.

S 10.23 A PSR shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The PSR must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications.

Question 9:
Cryptographic controls

Does your institution anticipate any challenges in fulfilling the requirement set out in paragraphs 10.22 and 10.23? If yes, please explain:

(a) the challenges, with clear justification for such challenges; and
(b) alternative control measures, if any.

Data Centre[20] Resilience

S 10.24 A PSR must specify the resilience and availability objectives of its data centres to effectively support its business recovery objectives.

S 10.25 A PSR must ensure data centres have redundant capacity components and multiple distribution paths serving the computer equipment to eliminate any single point of failure for effective achievement of the identified business recovery objectives.

S 10.26 A PSR shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area. A PSR must also ensure there is no single point of failure in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure. A PSR must also ensure adequate maintenance, and holistic and continuous monitoring of these

[20] Server rooms in office spaces are not to be equated as data centers (DC) as they do not meet the criteria of a DC.

critical components with timely alerts on faults and indicators of potential issues.

S 10.27 A PSR must establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions.

S 10.28 A PSR must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity[21]. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.

Service Availability

S 10.29 A PSR must ensure its system capacity needs are well-planned and managed with due regard to peak processing period, business growth plans and technology architecture changes.

S 10.30 A PSR must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services[22]. These monitoring mechanisms shall be capable of providing actionable alerts to administrators to enable timely detection and resolution of service interruptions. The monitoring scope, metrics and thresholds shall be updated periodically to ensure they remain effective.

G 10.31 A PSR may strive to ensure disruption to essential services caused by technology failures or cyber incidents does not exceed 4 hours on a rolling 12-months basis and a maximum tolerable downtime of 120 minutes per incident. For avoidance of doubt, disruption of payment services affecting more than 1% of daily average transactions for the current month or at least 10,000 failed transactions, whichever is higher shall be classified as unplanned downtime.

S 10.32 A PSR shall prioritise diversity[23] in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

S 10.33 A PSR shall review the effectiveness of system design, capacity management, identification of single point of failure and contingency arrangement whenever there is a material change to the risk environment, such as arising from:

[21] For example, system development activities must be segregated from data centre operations.
[22] For example, batch runs and backup processes for the PSR's application systems and infrastructure.
[23] Diversity in technology may include the use of different technology architecture designs and applications, technology platforms and network infrastructure.

(a) material changes in the IT system;
(b) system faults identified in service disruptions; and
(c) security vulnerabilities identified in cyber incidents.

S 10.34 A PSR shall implement robust incident response plan to contain the impact of technical failures which includes but not limited to timely and effective communications to customer and other stakeholders to manage their expectations and preserve public confidence.

Network Resilience

S 10.35 A PSR must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.

S 10.36 A PSR must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.

G 10.37 The control measures to prevent from network faults as referred to in paragraph 11.36 are expected to include component redundancy, service diversity and alternate network paths.

S 10.38 A PSR must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.

Question 10
Network Resilience

Does your institution anticipate any challenges in fulfilling the requirement set out in paragraph 10.38, in particular on the real-time network bandwidth? If so, please explain:

(a) the challenges and clear justification for such challenges; and
(b) countermeasures in place if real-time network bandwidth monitoring processes and corresponding network service resilience metrics is not implemented.

S 10.39 A PSR must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.

S 10.40 A PSR must establish and maintain a network design blueprint identifying all its internal and external network interfaces and connectivity. The blueprint must highlight both physical and logical connectivity between network components and network segmentations.

S 10.41 A PSR must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.

S 10.42 A PSR must implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the PSR from other entities within the group.

System backup and restoration

S 10.43 A PSR must establish a robust backup strategy and procedures to meet business recovery objectives. At minimum, a PSR shall:

(a) establish backup and restoration procedures to effectively manage the backup data life cycle;

(b) maintain an adequate number of backup copies of all critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes;

(c) backup media must be stored in an environmentally secure and access-controlled backup site;

(d) secure the storage and transportation of sensitive data in removable media to meet minimum controls as specified in Appendix 1 or equivalent;

(e) test backup and restoration procedures periodically to validate recovery capabilities. Remedial actions shall be taken promptly by the PSR to fix root cause of unsuccessful backups; and

(f) undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times.

G 10.44 A PSR is encouraged to establish tamper-proof backup arrangement and an isolated recovery environment to enable timely resumption of essential payment services within its tolerable level in the event of destructive cyber-attacks such as widespread data loss caused by ransomware.

Question 11:
Backup strategy for destructive cyber attacks

(a) What would be the anticipated challenges that your institutions may face in fulfilling the requirement set out in paragraph 10.44? Please provide clear justifications to support your response.

(b) Please list and explain any other aspects of backup approaches that should be considered.

Third Party Service Provider Management

S 10.45 The board and senior management of the PSR must exercise effective oversight and address associated risks when engaging third party service providers[24]. The PSRs remain accountable for managing all risks that arise from engagement of third-party service providers, to ensure security and reliability of technology services in compliance with all relevant regulatory requirements specified in this policy document.

S 10.46 A PSR must conduct due diligence on the third-party service prior to its on-boarding engagement and throughout the service engagement to ensure achievement of business performance and recovery objectives remain unimpaired, considering the latest risk environment. At minimum, a PSR must consider the range of risks outlined in Appendix 6.

S 10.47 A PSR must establish Service Level Agreements (SLA) when engaging third party service providers. At a minimum, the SLA shall contain the following:

(a) access rights for the regulator and any party appointed by the PSR to examine any activity or entity of the PSR. This shall include access to any record, file or data of the PSR, including management information and the minutes of all consultative and decision-making processes;

(b) requirements for the third-party service provider to provide sufficient prior notice to PSRs of any sub-contracting which is substantial;

(c) a written undertaking by the third-party service provider on compliance with secrecy provisions under relevant legislation. The SLA shall further clearly provide for the third-party service provider to be bound by integrity and confidentiality provisions stipulated under the contract even after the engagement has ended;

(d) arrangements for disaster recovery and backup capability, where applicable;

(e) critical system availability;

(f) arrangements to facilitate an orderly exit in the event of exit or termination of the third-party service provider, which includes ensuring data residing in third party service providers are recoverable in a timely manner;

(g) responsibility of third-party service providers to promptly disclose and notify the PSR of any service disruptions or cyber incidents that affect PSR or customer data that occur within the service providers' or sub-contractors' environment. This enables PSRs to provide timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident; and

(h) requirements for the third-party service providers to comply with the relevant internationally recognised standards and ensure their key staff obtain the relevant certifications.

[24] PSR must adhere to the requirements in the "Outsourcing" section in MA and GRMO PD and "Outsourcing Risk Management" Section for E-Money PD for engagements with third party service providers that meet the definition of outsourcing arrangement as specified in these PDs.

S 10.48 A PSR shall formulate a roadmap to achieve continuous monitoring of third-party service provider's cyber security posture to obtain real-time insights for effective incident management. A PSR shall undertake the following:

(a) measure the IT infrastructure footprint and the customer information accessible to third parties, and regularly manage this external stress state exposures to mitigate cyber-attack surface;
(b) adopt leading security policies and controls to mitigate third-party risks that are product-specific;
(c) ensure incident response plans incorporate protocols with service providers to detect and contain adverse impact of security vulnerabilities resulting from software updates;
(d) define a priority set of security controls that require more frequent assurance assertion from the third-party service providers;
(e) monitor technology and cyber incidents information disclosed by third-party service providers at a higher frequency;
(f) implement technology solutions to automate metric testing; and
(g) establish processes to respond to breached thresholds, including investigating failed assertions and remedying control gaps.

Question 12:
Continuous monitoring of third-party service provider

Does your institution currently implement any continuous monitoring of your third-party service provider's cyber security posture?

(a) If yes, please elaborate on how continuous monitoring is implemented in your institution.

(b) If no, please provide view on the practical timeline and cost involved in this implementation.

Cloud Services

S 10.49 A PSR must fully understand the inherent risk of adopting cloud services. In this regard, a PSR is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment must specifically address risks associated with the following:

(a) sophistication of the deployment model;
(b) migration of existing systems to cloud infrastructure;
(c) location of cloud infrastructure including potential geo-political risks and legal risks that may impede compliance with any legal or regulatory requirements;
(d) multi-tenancy or data co-mingling;
(e) vendor lock-in and application portability or interoperability;
(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;
(g) exposure to cyber-attacks via cloud service providers;

(h) termination of a cloud service provider including the ability to secure the PSR's data following the termination;
(i) demarcation of responsibilities, limitations and liability of the cloud service provider; and
(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

G 10.50 For critical systems hosted on a public cloud[25], a PSR is expected to consider common key risks and control measures as specified in Appendix 8. A PSR that relies on alternative risk management practices that depart from the measures outlined in Appendix 8 is expected to be prepared to explain and demonstrate to the Bank that these alternative practices are at least as effective as, or superior to, the measures in Appendix 8.

S 10.51 A PSR must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.

Access Control

S 10.52 A PSR must implement an access control policy for the identification, authentication, and authorisation of all users to its IT assets and data. The level of granularity defined in the access control policy shall be commensurate with the level of risk of unauthorised access to its IT assets.

S 10.53 A PSR shall implement the following:
(a) adopt a "deny all" access control policy for users by default because all access to IT assets must be explicitly authorised;
(b) employ "least privilege" access rights to ensure IT assets are accessed on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;
(c) employ time-bound access which restrict access to a specific period based on the nature of work;
(d) employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as:
    (i) system development and technology operations;
    (ii) security administration and system administration;
    (iii) network operation and network security; and
    (iv) IT operations environment.
(e) establish criteria for activities that require dual authorization control; and

[25] Refer the Special Publication 800-145 on Definition of Cloud Computing issued by the National Institute of Standards and Technology, U.S. Department of Commerce.

(f) adopt robust user authorization and authentication based on criticality of IT assets:
  (i) stronger authentication for critical activities and higher-risk environment such as remote access;
  (ii) ensure user credentials provisioned with robust identity verification method to prevent impersonation risks; and
  (iii) ensure online credential is uniquely linked to a single user to ensure clear accountability in access to confidential IT assets.

S 10.54 A PSR must employ strong authentication method such as multi-factor authentication (MFA) that can defend against social engineering attacks for authenticating user access, to critical systems. The authentication method may combine two or more of knowledge factors, inherent factors (e.g. biometric characteristics) or possession factors (e.g. security keys, tokens).

Question 13:
Strong authentication method

Would your institution be able to implement MFA if it is made a mandatory requirement under paragraph 10.54? If no, please provide:

(a) The challenges, with clear justification for such challenges; and
(b) Alternative risk mitigation measures in place if MFA is not implemented.

S 10.55 A PSR must establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.

S 10.56 A PSR must ensure:
(a) access controls to enterprise-wide systems are effectively managed and monitored;
(b) anomalies are flagged for prompt investigations to contain any cyber incidents; and
(c) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.

11 Cybersecurity Management

Cyber Risk Management

S 11.1 A PSR must ensure that there is an enterprise-wide focus on effective cyber risk management to reflect the collective responsibility of business and technology lines for managing cyber risks.

S 11.2 A PSR must develop a CRF which clearly articulates the institution's governance for managing cyber risks, its cyber resilience objectives and its risk tolerance, with due regard to the evolving cyber threat environment. Objectives of the CRF shall include ensuring operational resilience against extreme but plausible cyber-attacks. The framework must be able to support the effective identification, protection, detection, response, and recovery (IPDRR) of systems and data hosted on-premises or by third party service providers from internal and external cyber-attacks.

S 11.3 The CRF must consist of, at a minimum, the following elements:

(a) development of an institutional understanding of the overall cyber risk context in relation to the PSR's business and operations, its exposure to cyber risks and current cybersecurity posture;

(b) identification, classification and prioritisation of critical systems, information, assets and interconnectivity (with internal and external parties) to obtain a complete and accurate view of the PSR's information assets, critical systems, interdependencies and cyber risk profile;

(c) identification of cybersecurity threats, vulnerabilities and countermeasures to secure digital services delivery against cyber-attacks and contain reputational damage that can undermine confidence in the PSR;

(d) enhancing layers of cyber defence with reference to the latest international standards and sound practices such as zero-trust principles[26], defense-in-depth through micro-segmentation and security by design, to protect its data, infrastructure and assets against evolving cyber threats;

(e) timely detection of cybersecurity incidents through continuous surveillance and monitoring;

(f) detailed incident handling policies and procedures and a crisis response management playbook to support the swift recovery from cyber-incidents and contain any damage resulting from a cybersecurity breach; and

(g) policies and procedures for timely and secure information sharing and collaboration with other PSRs and participants in financial market infrastructure to strengthen cyber resilience and fraud prevention.

[26] Zero-trust principles is a security paradigm designed to prevent data breaches and limit internal lateral movement of threat actors by requiring all users, whether in or outside the organization's network, to be authenticated, authorised, and validated before being granted the access.

G 11.4 In addition to the requirements in paragraph 11.3, a PSR is encouraged to implement a centralised automated tracking system to manage its technology asset inventory.

S 11.5 A PSR shall establish a dedicated in-house cyber risk management function to manage cyber risks or emerging cyber threats. The cyber risk management function shall include performing detailed analysis on cyber threats, provide risk assessments on potential cyber-attacks and ensuring timely review and escalation of all high-risk cyber threats to senior management and the board.

Question 14:
Dedicated in-house cyber risk management function

(a) What is the current set-up in your institution (i.e. fully outsourced, hybrid or fully in-house) for the following functions:
- Cyber risk management function as described in paragraph 11.5?
- The Security Operations Centre (SOC) as described in paragraph 11.10(a)?
- If fully outsourced or hybrid for the cyber risk function and/or the SOC, please provide the name of the outsourced service provider and some description for the hybrid arrangement.

(b) Does your institution anticipate any challenges in fulfilling the requirement for in-house cyber risk management function as set out in paragraph 11.5? If so, please explain:
- the challenges, with clear justification for such challenges; and
- countermeasures in place if the dedicated in-house cyber risk management function is not established.

S 11.6 A PSR must adopt robust control measures as outlined in Appendix 5 to enhance its resilience to cyber-attacks.

G 11.7 A PSR is encouraged to conduct a comprehensive "Red Team" simulation attack on its infrastructure at least once every three years to proactively identify and manage potential vulnerabilities. The scope of the simulation shall include the FI technology infrastructure as well as infrastructure managed by third party service providers.

G 11.8 A PSR is encouraged to implement crowdsourced security testing programs as a complement to existing security assessments, in order to thoroughly test the security of their IT environment. The PSR must engage reputable and credible service providers to facilitate the program.

Cybersecurity Operations

S 11.9 A PSR must establish clear responsibilities for cybersecurity operations which shall include implementing appropriate mitigating measures in the PSR's conduct of business that correspond to the following phases of the cyber-attack lifecycle:

(a) reconnaissance;
(b) weaponisation;
(c) delivery;
(d) exploitation;
(e) installation;
(f) command and control; and
(g) exfiltration.

S 11.10 A PSR must ensure continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure to prevent potential compromise of its security controls or weakening of its security posture. This shall include:

(a) establishing a Security Operations Center (SOC) supported by competent resources and equipped with the necessary tools and technologies for proactive monitoring of its technology security posture;
(b) ensuring the scope of monitoring must cover all critical systems including the supporting infrastructure; and
(c) conducting regular review of its security posture via the conduct of a vulnerability assessment and penetration testing.

S 11.11 PSRs must establish a process to collect, analyse and evaluate cyber threat information in relation to the PSR's environment ("cyber threat intelligence") to promptly detect cyber threats, including data breach incidents and spread of misleading information in relation to the PSR over the Internet[27].

S 11.12 A PSR must establish appropriate response to investigate and respond to flagged anomalous activities based on their level of complexity.

Cyber Response and Recovery

S 11.13 A PSR must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident.

[27] This includes the capability to collect and correlate such information from sources such as social media and dark web.

S 11.14 A PSR must establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP must address the following:

(a) **Preparedness**
Establish a clear governance process, reporting structure and roles and responsibilities of the Cyber Emergency Response Team (CERT) as well as invocation and escalation procedures in the event of an incident.

(b) **Detection and analysis**
Ensure effective and expedient processes for identifying points of compromise, assessing[28] the extent of damage and preserving sufficient evidence for forensics purposes.

(c) **Containment, and eradication**
Identify and implement remedial actions to prevent or minimise damage to the PSR, contain and remove the known threats and resume business activities.

(d) **Recovery**
Implement multiple strategies including contingency plans as part of incident recovery to swiftly resume business operations and significantly enhance redundancy and resilience.

(e) **Post-incident activity**
Conduct post-incident review incorporating lessons learned and develop long-term risk mitigations.

S 11.15 A PSR must ensure that relevant CERT members are conversant with the incident response plan and handling procedures and remain contactable at all times.

S 11.16 A PSR shall establish a secure and reliable out-of-band communication method for both internal and external stakeholders to ensure continued coordination and communication if the primary channel is rendered unavailable during a crisis.

S 11.17 A PSR must conduct an annual cyber drill exercise to test the effectiveness of its CIRP including the out-of-band communication methods, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third-party service providers. The result of the annual cyber drill exercise must be reported to the Board in a timely manner. The out-of-band communication method must be tested regularly as part of the institutions cyber drill exercises. The test scenarios must include scenarios designed to test:

[28] This includes competency in handling threat actor claims by confirming the legitimacy and extent of the incident and uncover more details on the threat actor.

(a) the effectiveness of escalation, internal and external communication and decision-making processes that correspond to different impact levels of a cyber-incident; and
(b) the readiness and effectiveness of CERT and relevant third party service providers in supporting the recovery process.

Question 15:
Cyber drill exercise

Tier-2 PSRs must ensure fulfilment of the requirements under paragraph 11.17. For clarity, this does not include any cyber drills conducted by the Bank for the industry.

(a) Does your institution currently conduct cyber drill exercise and what is the frequency of such exercise?
(b) Please provide views and comments to this requirement, if any.

S 11.18 A PSR shall review its loss provision arrangements to ensure its adequacy to cover cyber incidents based on its scenario analysis of extreme adverse events. Where cyber insurance is adopted to mitigate impact of cyber incidents, the PSR shall:
(a) ensure that the scope of the insurance policy adequately covers the information security events and types of liability that the PSR is exposed to;
(b) understand the terms and conditions of the insurance policy in relation to warranties, attestations or any responsibilities of the PSR to ensure that any changes to IT services and control measures do not result in unintended exclusions of cover; and
(c) ensure that any obligations imposed by the insurance policy (such as in relation to appointment of experts and accepting their recommendations during a cyber incident) do not impair its ability to act in the best interest of the PSR and its customers. The PSR shall anticipate and adequately manage any conflict of interest that may arise from the insurer's objective to minimise the cost of its liability under the insurance policy.

Cyber Reporting and Threat Information Sharing

S 11.19 A PSR is required to notify the Bank of cyber incidents in adherence to the Bank's policy documents and any requirements as specified[29] by the Bank.

S 11.20 Subject to the applicable data protection laws, a PSR must share cyber threat intelligence information with the industry on timely basis via the relevant sharing platforms developed by the Bank, the industry, or law enforcement

[29] In addition to the email communique issued to all PSRs on 14, December 2022, PSRs are required to also refer to paragraph 19.25 of the Merchant Acquiring Services policy document (PD), paragraph 29.23 of the E-Money PD, paragraph 31.9 of the Governance, Risk Management and Operations PD, and Operational Risk Reporting (ORR).

authorities. In addition, PSRs must allocate resources to participate in any industry-wide initiatives aimed at improving collective threat intelligence capabilities.

S 11.21 A PSR shall collaborate and cooperate closely with relevant stakeholders and authorities in combating cyber threats.

The rest of the page is intentionally left as blank.

12 Digital Services

Security of Digital Services

S 12.1 Securing digital services is an integral part of PSR's risk management. A PSR must expand its CRF to implement robust technology security controls in providing digital services which assure the following:

(a) adopt and regularly assess the minimum-security controls for respective delivery channels to ensure confidentiality and integrity of customer and counterparty information and transactions. (Refer to Appendices 2, 3, 4, 9, 10[30] and 11);

(b) proper authentication of users or devices and authorization of transactions to mitigate impersonation and fraud risk. Refer the minimum-security controls in Appendix 3 (Customer Authentication); and

(c) strong physical control and logical control measures.

S 12.2 In the event that a PSR has not yet implemented the digital services security controls stipulated in this policy requirement, the PSRs must be ready to provide documented explanation of how alternative measures or mitigations achieve equivalent or superior effectiveness, and to assume the liability of any fraud that occurs due to the gaps that arise from the absence of the stipulated control.

Digital Fraud Management and Customer Awareness

S 12.3 The complex and fast evolving digital fraud require PSRs to be vigilant against new fraud techniques and proactive in strengthening its cyber defence for customer protection. In line with paragraphs 11.2 and 11.3 (a) through (g) of this policy document, a PSR must enhance its CRF as follows:

(a) expand the scope of identification of cybersecurity threats and countermeasures to include customers' mobile devices and access points;

(b) adopt layered (defense-in-depth) security controls to protect the digital service application deployed to customers' mobile devices and the relevant customer data contained in it;

(c) perform continuous surveillance and monitoring to detect any exploitation of the digital service application deployed to customers' mobile devices and ensure the swift upgrade of security controls to mitigate new vulnerabilities;

(d) establish clearly defined and effective incident handling procedures to assist customers to contain the potential damage resulting from a cybersecurity breach involving digital services;

(e) formalise operational arrangement to enable swift coordinated response and rapid upgrade of countermeasures to defend against advanced fraud tactics if a PSR relies on multiple business functions;

[30] Appendix 10 is only applicable to MAs.

(f) conduct regular review by Senior Management to ensure the effectiveness of digital fraud management and define threshold for escalation of countermeasures considering the actual impact to victims of digital fraud and emerging fraud environment; and
(g) apprise the Board on the outcome of management reviews to preserve public confidence in the security of digital services and mitigate reputation-risk to the industry.

S 12.4 A PSR must ensure that its fraud detection rules are updated in a timely manner upon detection of new fraud modus operandi in order to prevent fraudulent transactions or account takeover using stolen customer credentials. This must be supported by appropriate risk analytics to improve the accuracy of fraud detection, that includes continuous upgrade of fraud detection capability as specified in Appendix 9 on Fraud Detection Standards.

S 12.5 A PSR must mitigate attendant risk arising from its delivery of digital services. This shall include:
(a) adopt secure communication channel to mitigate risk of phishing. Compensating controls shall be adopted when using communication channel prone to phishing exploits[31];
(b) all customers must be properly informed in advance of new controls to ease adoption and minimise inconvenience; and
(c) practical ways for customers to verify the authenticity of calls made by the PSRs or its appointed outsourced service providers.

S 12.6 A PSR shall empower customer to mitigate digital fraud risks where it is reasonably practical. This shall include offering customer solutions to manage de-activation of payment card for overseas and card-not-present transactions. This does not absolve a PSR from its liabilities, responsibilities and duty of care to ensure the security of digital services.

S 12.7 Consumer competency is essential to strengthening the security of digital services. A PSR must maintain continuous efforts to review and enhance the effectiveness of its awareness programmes, ensuring customers understand the risks of digital services fraud. This shall include:
(a) continuous and timely updates of practical information on how to identify potential fraud or scams, including specific information about new or common modus operandi;
(b) clear explanation about new and existing security measures, such as how to verify genuine PSR's websites and mobile applications;
(c) real-time alerts of possible risks when security measures are absent or have not yet been implemented; and
(d) potential measures to further improve customer understanding and familiarisation, such as through interactive simulations of security features, phishing exercises, etc.

[31] A PSR must remove any clickable hyperlinks in SMS messages to customers and create awareness on this change to mitigate risk of phishing.

S 12.8 A PSR must provide convenient means for customers to report, suspend and re-activate their account swiftly in the event of a suspected fraud. This shall require the PSRs to:

(a) offer a secure self-service "kill switch" solution;
(b) ensure that its contact centre is adequately resourced and operating effectively to provide prompt and adequate assistance to customers in distress; and
(c) restore customer access to digital services within a reasonable timeframe upon validation.

S 12.9 In addition to effective incident handling procedures, a PSR must adopt additional measures to protect customers in response to any data breach. This shall include:

(a) heightening monitoring of affected customer accounts;
(b) notifying affected customers and provide them with the necessary information to apply mitigating measures and reduce the risk of fraud; and
(c) revoking and re-issuing affected user credentials or designated payment instruments, where there is potential fraud risk involving the exploit of the compromised data.

Question 16:
Digital services

(a) Do you foresee any operational challenges in implementing the requirements in this section (paragraph 12.9), including paragraph 12.3(b) on adoption of layered (defense-in-depth) security controls, 12.7(c) on real-time alerts, 12.8(a) on "kill-switch" solution and 12.8(b) on contact centre requirements.

- Please describe the specific requirements in this section and the corresponding appendices that would be of significant challenge to be implemented by your institution, with clear justification for such challenges.
- What are your plans to address these challenges?

(b) What is your internal arrangement to coordinate various teams effectively for fraud management?

(c) Are there any other areas that TR policy document should address to mitigate fraud risks?

13 Technology Audits

Audit function

S 13.1 A PSR must ensure that the scope, frequency, and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.

S 13.2 A PSR must establish annual technology audit plan that provides appropriate coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation review of new or material enhancements of technology services.

S 13.3 A PSR must ensure the internal audit function would have dedicated technology audit resources with specialized competencies and professionally certified. The technology audit resources shall be adequately conversant with the developing sophistication of the PSR's technology systems, delivery channels and have sound knowledge in the areas audited.

S 13.4 Tier-3 PSRs shall ensure the internal audit function must be established with a minimum of an internal IT Audit head or personnel with specialized competencies and professionally certified. The IT Audit head or personnel shall be adequately conversant with the developing sophistication of the PSR's technology systems, delivery channels and have sound knowledge in the areas audited. In addition, in the event where an external IT audit is appointed, the PSR shall ensure that the key staff in the external IT audit team is adequately competent, have the appropriate experience and be professionally certified.

Question 17:
Technology Audits

(a) What are the challenges for your institution to establish dedicated resources for technology audit?

(b) What is the risk your institution foresee and compensating controls that would need to be put in place to manage the identified gaps if external IT auditors are engaged?

S 13.5 The internal technology audit staff must be enlisted to provide advice on compliance with and adequacy of control processes during the planning and development phases of new major products, systems, adoption of third party service providers or technology operations. In such cases, the technology auditors participating in this capacity must carefully consider whether such an advisory or consulting role can materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.

14 External Party Assurance

S 14.1 A PSR shall appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA). The assessment must consider all major risks and determine the current level of resilience of the production data centre. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.24 to 10.28 have been adhered to. For data centres managed by third party service providers, a PSR shall rely on independent third party assurance reports provided such reliance is consistent with the PSR's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment.

S 14.2 A PSR shall appoint a technically competent external service provider to carry out regular network resilience and risk assessments (NRA) and set proportionate controls aligned with its risk appetite. The assessment must be conducted at least once in three years or whenever there is a material change in the network design. The assessment must consider all major risks and determine the current level of resilience. This shall include an assessment of the PSR's adherence to the requirements in paragraphs 10.35 to 10.42. The designated board-level committee must deliberate the outcome of the assessment.

Question 18:
External Party Assurance

Does your institution anticipate any challenges in fulfilling the requirement set out in paragraphs 14.1 and 14.2? If yes, please explain the challenges with clear justifications for such challenges.

15 Internal Awareness and Training

S 15.1 A PSR must provide adequate and regular technology and cybersecurity awareness education for all staff and third party service providers in undertaking their respective roles and measure the effectiveness of its education and awareness programs. This cybersecurity awareness education must be conducted at least annually and must reflect the evolving cyber threat landscape and emerging risks.

S 15.2 A PSR must provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent and suitably certified to effectively perform their roles and responsibilities.

S 15.3 A PSR must provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

16 Simplified Approach

Technology risk management

S 16.1 A PSR shall establish a sound internal technology risk framework, IT policies and procedures including the governance arrangements and oversight on the IT system operations, business continuity management, and all relevant security controls that commensurate with its risk profile.

S 16.2 A PSR shall establish controls to mitigate technology risk to systems, online portals and/or mobile applications. At a minimum, a PSR's technological eco-system shall be equipped with the following controls to manage the risks from malware, phishing or data leakage:

(a) its internal network, if any, is protected by a firewall;
(b) all servers and workstations are installed with anti-virus with the latest virus signature update;
(c) the system uses the latest and most secure encryption communication channel;
(d) effective security patch management[32] to safeguard its system from intrusion and data loss, which includes regular updates of all types of IT inventories with the latest security patches;
(e) implement a sound user access management policy including that only authorised system administrators are provided access to its database for administrative duties, segregation of data access between user profiles and documented procedures for access control and authorization;
(f) ensure proper controls over the management of user IDs, whereby each user ID shall be unique and passwords must not be shared among staff;
(g) implement appropriate physical access control to the PSR's IT equipment (e.g. physical access controls to its servers, firewalls, routers and switches). The access control should include identification, authentication and authorization of the user (internal and external users[33]) accessing IT equipment;
(h) conduct continuous training and awareness programmes to promote cyber hygiene[34] and understanding on cyber security risks[35];

[32] A PSR shall consider leveraging on effective IT inventory management system to ensure it is able to record and monitor the security patch versions for all its IT peripherals.
[33] External users include service providers, auditors, etc.
[34] Examples of good cyber hygiene includes usage of strong password, ensuring user's password are not written and posted on the workstations, sharing of IDs and passwords, etc.
[35] Examples of cyber security risk includes phishing attacks, malware attacks, social engineering, ransomware, trojan viruses, etc.

(i) for the PSRs who subscribe to services offered by a third-party service provider, the following controls to safeguard themselves in the service level agreement (SLA) should be established:
  (i) clearly defined roles and responsibilities between the PSR and the service provider;
  (ii) arrangements for disaster recovery and backup capabilities, where applicable;
  (iii) written undertaking by the service provider on compliance with secrecy provisions under relevant legislation. The SLA shall clearly provide that the service provider is bound by confidentiality provisions stipulated under the contract even after the engagement has ended;
  (iv) clearly affirm the PSR's ownership of its data stored on the service provider's system; and
  (v) arrangements to secure business continuity in the event of exit or termination of the service provider.

(j) for online portal and mobile platform, at a minimum, the following controls to safeguard the system and the customers must be established:
  (i) mechanism to authenticate system users based on the PSR's technology risk appetite (e.g. login authentication);
  (ii) mechanism to notify customers (e.g. via secured communication channel) of all online transactions performed and completed;
  (iii) mechanism to clear the web-browser cache used by the user when logging out from the account of the PSR's website for online transactions;
  (iv) ensure the PSR's core system(s), including the online portal, mobile application and network system are equipped with audit trail capabilities. This includes tracking the IP address source for data movement through the online portal as well as IP address and geo-location sources for data movement via a mobile device;
  (v) mechanism to prevent sensitive information from being stored on the user's mobile device;
  (vi) provide sufficient information to customers to create awareness on risks associated with online and mobile application transactions; and
  (vii) multi-factor authentication for online transactions.

Maintenance of Robust and Reliable Management Information System

S 16.3 A PSR shall establish a secure and robust management information system to support the PSR's business operation. The system shall have the capability to perform at minimum, the following functions:
(a) detect and capture any alterations made to the information maintained in the system;

(b) record details of transactions and generate reports on transaction value and volumes for purposes of identifying, monitoring, and reporting suspicious transactions; and

(c) for PSR with branches and agents, the system must be able to record business transactions on a real-time basis and facilitate the aggregation of business transactions undertaken at all its offices including agents, either at customer level or PSR level, for purposes of monitoring compliance with internal and regulatory limits.

S 16.4 Upon commencement of the operation, a PSR shall ensure the system is continuously operating in a sound and robust manner with at a minimum the following controls:

(a) ensure the PSR's customer information is appropriately encrypted at all times;

(b) ensure the use of updated and secured encryption standards for all forms of data (i.e. data-at-rest, data-in-use and data-in-motion);

(c) ensure data backup and restoration tests are performed frequently; and

(d) ensure all business transaction records conducted by the PSR are readily available upon request by the Bank.

17 Assessment and Gap Analysis

S 17.1 A PSR must perform a gap analysis of existing practices in managing technology risk against the requirements in this policy document and highlight key implementation gaps. The PSR must develop an action plan with a clear timeline and key milestones to address the gaps identified. The gap analysis and action plan must be submitted to the Bank no later than 90 days after the issuance date of this policy document.

Question 19:
General Comments

The requirements in this ED is a significant step-up from the technology requirements under current E-Money PD, MA PD and GRMO PD given the higher level of risks including increasing cyber threat and fraud risk. Therefore, other than the specific questions asked throughout this ED, the Bank would like to seek further feedback on the following areas:

(a) Overall key challenges or constraints to comply with the requirements in the ED;
(b) Estimation of the overall implementation cost / investment and recurring cost involved for the new requirements outlined in the ED (in RM), indicating key areas that will incur the most investment cost to your institution;
(c) Impact, if any, on your business operations and strategic objectives; and
(d) Any other comments or views.

To facilitate the Bank's assessment, please clearly specify which area or paragraph in this ED each comment is related to.

Appendix 1 Storage and Transportation of Sensitive Data in Removable Media

PSRs must ensure adequate controls and measures are implemented for the storage and transportation of sensitive data in removable media, which includes:

1. Deploying the latest industry-tested and accepted encryption techniques;
2. Implementing authorised access control to sensitive data (e.g. password protection, user access matrix);
3. Prohibiting unauthorised copying and reading from the media;
4. Where there is a need to transport the removable media to a different physical location, PSRs must:
   (a) strengthen the chain of custody process for media management which includes:
      (i) the media must not be under single custody at any point of time;
      (ii) the media must always be within sight of the designated custodians; and
      (iii) the media must be delivered to its target destination without unscheduled stops or detours.
   (b) use secure and official vehicle for transportation;
   (c) use strong and tamper-proof containers for storing the media with high-security lock (e.g. dual key and combination lock); and
   (d) implement location tracking functionality for each media container.
5. Ensuring third party service providers comply with the requirements in paragraphs 1 to 4 of this Appendix, in the event third party services are required in undertaking the storage management or transportation process of sensitive data.

Appendix 2 Control Measures on Self-service Terminals (SSTs)

Cash SST

Cash SSTs are computer terminals provided by PSRs that provide cash transactions or cash acceptance for customers. PSRs must ensure the adequacy of physical and logical security and controls implemented on the Cash SST, which include:

1. Enforcing full hard disk encryption;
2. Deploying Anti-virus (AV) solution for Cash SST, ensure full virus scanning on all Cash SSTs is performed periodically and ensure timely update of signatures;
3. Implementing a centralised management system to monitor and alert any unauthorised activities on Cash SST such as unauthorised shutting-down of operating system or deactivation of the white-listing programme;
4. Ensuring effective control over the Cash SST lock and key by using a unique and non-duplicable key to open the Cash SST PC Core compartment as well as ensure proper safekeeping and custody of the key;
5. Installing alarm system with triggering mechanism connected to a centralised alert system to detect and alert PSR's staff of any unauthorised opening or tampering of the physical component of the Cash SST;
6. Securing physically the Cash SST PC Core by enclosing the CPU in a locked case;
7. Enforcing pairing authentication for key Cash SST components, particularly between cash dispenser and Cash SST controller;
8. Enforcing Basic Input Output System (BIOS) lock-down including enabling unique password protection and disabling external input device;
9. Ensuring proper configuration and hardening of the Operating System (OS) and application system including disabling default program system (such as Notepad, Internet Browser, Windows Shortcut, etc), concealing Start Bar or Tray Menu and enabling cache auto deletion;
10. Enforcing secure system parameter setting, which includes:
    (a) changing default passwords and other system security parameters setting of the Cash SST;
    (b) using a unique system administrator password for all Cash SSTs; and
    (c) using lowest-level privileges for programmes and users' system access.
11. Enforcing and monitoring Cash SST end-point protection such as installing white-listing programmes. The end-point protection programme, at a minimum, shall ensure only authorised Cash SST system processes and libraries are installed and executed;
12. Enforcing strict control procedures over installation and maintenance of Cash SST operating system and application systems; and
13. Installing closed-circuit cameras and/or transaction triggered cameras at strategic locations with adequate lighting to ensure high quality and clear closed-

circuit television images of customer performing a transaction as well as any suspicious activities.

Non-Cash SST

Non-cash SSTs are computer terminals such as desktops, laptops, tablets, kiosks or machines that provide non-cash transactions such as balance enquiries, fund transfers, account updates, utilities bill payments, etc.

PSRs must ensure the adequacy of physical and logical security and controls implemented on the self-service terminals, which include:

1. Enforcing the use of lock and key on the computer terminal's central processing unit (CPU) at all times;
2. Deploying closed-circuit television to monitor the usage of self-service terminals;
3. Disabling the use of all input devices (such as USB, CD and DVD), application system (such as Notepad, Microsoft Word, and Microsoft PowerPoint) and file download as well as command prompt on the kiosk;
4. Disabling browser scripting, pop-ups, ActiveX, Windows shortcut;
5. Concealing Start Bar or Tray Menu;
6. Enabling cache auto-deletion;
7. Disabling key combinations and right-click mouse functions; and
8. Restricting use of Internet browser i.e. only to be used to access the PSR's internet website.

Question 20:
Cash and non-cash SST

Does your institution have in place any cash and/or non-cash SST? If yes, please describe:

(a) the services offered by such cash and/or non-cash SST; and
(b) views or comments regarding the requirements in this appendix.

Appendix 3 Control Measures for Digital Services

1. A PSR must ensure the adequacy of security controls implemented for digital services, which include the following, where relevant:
   (a) ensuring registration or enrolment in digital services is subject to robust authentication and verification;
   (b) ensuring transactions are performed over secured channels such as the latest version of Transport Layer Security (TLS);
   (c) ensuring that both client and host application systems must encrypt all confidential information prior to transmission over the network;
   (d) implementing strong mutual authentication between the users' end-point devices and PSRs' servers, such as the use of the latest version of Extended Validation SSL certificate (EV SSL);
   (e) ensuring secure user and session handling management;
   (f) ensuring sufficient and relevant digital service logs are retained for investigation and forensic purposes for at least three years;
   (g) putting in place additional authentication protocols to enable customers to identify the PSR's genuine website such as deploying image or word verification authentication or similar controls. The system shall require the customer to acknowledge that the image or word is correct before the password box is displayed to the customer;
   (h) ensuring resilience against brute-force attacks[36];
   (i) for new customers, the default transfer limit shall be set at a conservatively low level (such as RM1,000 per day). However, customers shall be provided with the option to change the limit via secure channels (e.g. online with MFA or at branches); and
   (j) applying appropriate verification or cooling-off period for first time enrolment in digital services or secure device, transaction limit increase or other activities which are deemed necessary.

2. A PSR must ensure the technology used in identity proofing and authentication methods are:
   (a) secure, highly resistant to cyber threats[37] affecting customer devices;
   (b) accurate, have a minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions; and
   (c) compliant with internationally recognised standards where available.

3. A PSR must strengthen security controls for registration and update of mobile device and customer details (such as mobile number, postal and email address) used for authentication of digital service transactions to prevent fraudsters from initiating funds transfers using stolen credentials. This shall include:

[36] A brute-force attack is a method used by attackers to gain unauthorised access to a system by systematically trying possible combinations or attempting to guess passwords or encryption keys.
[37] This includes but not limited to malware, phishing, transaction fraud or data leakage.

(a) consideration to restrict authentication of digital service transactions by default to one mobile device or secure device per account holder (or to designated devices in the case of joint or business accounts), except when specifically requested by customers who understand and accept the risks of dispensing with this control;
(b) ensuring all customers are immediately alerted upon detecting access to the customer's account from a new device, or when customer details are changed;
(c) ensuring that the registration of a new mobile phone number or replacement of an existing mobile phone number is only processed after applying robust verification methods to confirm the authenticity of the customer;
(d) adopting efficient measures to promptly verify and assist customers who need to change devices or update their personal details; and
(e) applying appropriate verification or cooling-off period for first time enrolment of digital services or secure device and multiple successive high-volume transactions or other abnormal transaction patterns. Transaction limit increase must also be subject to appropriate verification.

Question 21:
Authentication to one mobile device or secure device per account holder

Does your institution anticipate any challenges in fulfilling the requirement set out in paragraph 3(a) of this appendix, if the requirement is made mandatory? If so, please explain:

(a) the challenges, with clear justifications; and
(b) countermeasures in place if authentication to one mobile or secure device is not in place.

4. A PSR must implement controls to authenticate devices and users, authorise transactions, and support non-repudiation and accountability for transactions performed via digital services. These measures must include, at minimum, the following:
(a) adopting a strong authentication method such as MFA for financial and high-risk non-financial transactions. This includes when registering an account as a "favourite" beneficiary and, for all subsequent funds transfer to the favourite beneficiary. The deployment of authentication technology and channels, including for MFA, shall be more secured than unencrypted short messaging services;
(b) requesting users to verify details of the transaction prior to execution; and
(c) providing timely notification to customers that is sufficiently descriptive of the nature of the transaction.

5. A PSR must ensure the MFA solution used to authenticate financial transactions are adequately secure and resistant to phishing attacks, which includes the following:
(a) activation of MFA must be subject to robust verification by the PSR; and

(b) timely notification to customers of any activation and changes to the MFA solution via the customers' verified communication channel.

6. A PSR must ensure that the security controls of MFA solutions include adherence to the following requirements:
   (a) the MFA solution is resistant to interception or manipulation by any third party throughout the authentication process;
   (b) payer/sender must be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction;
   (c) authentication code must be initiated and generated locally by the payer/sender using MFA;
   (d) authentication code generated by payer/sender must be specific to the confirmed identified beneficiary and amount;
   (e) secure underlying technology must be established to ensure the authentication code accepted by the PSR corresponds to the confirmed transaction details; and
   (f) notification must be provided to the payer/sender of the transaction.

Question 22:
MFA as a strong authentication method for digital services

Would your institution be able to implement MFA for digital services, if it is made a mandatory requirement under paragraph 4 of this Appendix? If no, please provide:

(a) The challenges, with clear justification for such challenges; and
(b) Alternative risk mitigation measures in place if MFA is not implemented.

7. Where a PSR deploys OTP as a factor of authentication, the following features must be implemented:
   (a) OTP must be dynamic where it changes each time it is required and time-bound;
   (b) binding of the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction); and
   (c) generation of the OTP from the customer's device and not from the PSR's server to mitigate the risk of manipulating OTP in the PSR's infrastructure and increase customer control over authentication process.

8. A PSR must implement MFA to authenticate devices and users, authorise transactions and support non-repudiation and accountability for high-risk transactions or transactions RM10,000 and above (including open third party fund transfer and open payment transactions).

9. Where a PSR decides not to adopt MFA for financial transactions below RM10,000 to customer's own account, the PSRs must implement adequate safeguards to protect customer from digital fraud. This shall include:

(a) setting SLA of T+3 calendar days (or less), T being the date of event reported by customer, for reversal of any unauthorised first-party transactions reported by customer;
(b) setting appropriate limits on a per-transaction basis, and on a cumulative basis;
(c) providing a convenient means for customers to reduce the limits described in paragraph (b) or to opt for MFA; and
(d) providing its customers with adequate notice of the safeguards set out in paragraphs (a) to (c).

10. A PSR may consider where possible, to offer to customer a robust cryptographic key based authentication[38] such as digital certificate or passwordless as alternative to existing authentication methods to mitigate the risk of credentials of password being compromised or stolen. The enrolment of this method must be subject to robust verification and resilient against cyber threats and fraud techniques.

Question 23:
Passwordless authentication

(a) If paragraph 10 of this appendix is to be made mandatory, what would be your strategy in implementing such authentication solution? Please choose one (1) of the options below:
- Option 1: Deploy in-house infrastructure or leverage on third-party solutions to offer to your customers.
- Option 2: Establish a consortium among PSRs to manage standardized cryptographic key based authentication model.
- Option 3: Leverage on the government initiatives, such as MyDigital ID to support the implementation.
- Option 4: Other methods, please explain.

(b) For any of the strategy selected above, please describe:
i) the authentication mechanism to offer to customer? Such as passkey, virtual token, hard token, smart card, hybrid approach etc;
ii) the estimated timeline and cost for this implementation;
iii) any anticipated challenges in implementing this requirement; and
iv) any other aspects to ensure smooth implementation of this strategy.

[38] Cryptographic-key-based authentication is a method used to verify the identity of a user or system through the use of cryptographic keys, typically involving a challenge-response handshake to prove one's identity.

Appendix 4 Control Measures for Mobile Applications and Devices

1. A PSR that offers digital services must be aware of the risks associated with mobile applications. To mitigate these risks, a PSR is expected to continuously assess and perform risk assessment to ensure that the threats associated with mobile applications/devices and payment acceptance devices are addressed.

2. A PSR must ensure digital services involving sensitive customer and counterparty information offered via mobile devices are adequately secured. This includes the following:
   (a) enforcing the mobile application to only operate on a secure version of operating systems which have not been compromised, jailbroken or rooted;
   (b) designing the mobile application to operate in a secure and tamper-proof environment within the mobile devices to protect users against cyber threats such as malware and unauthorised access;
   (c) prohibiting the mobile application from storing customer and counterparty information used for authentication with the application server such as PIN and passwords. Authentication and verification of unique key and PIN must be centralised at the host;
   (d) ensuring activation of the mobile application is subject to robust authentication by the PSR;
   (e) ensuring secure provisioning process of mobile application in the customer's device is in place by binding the mobile application to the customer's profile such as device ID and account number;
   (f) undertaking proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;
   (g) ensuring proper controls are in place to access, maintain and upload the mobile application on application distribution platforms; and
   (h) monitoring the application distribution platforms to identify and address the distribution of fake applications in a timely manner.

3. A PSR must also ensure the following measures are applied specifically for applications running on mobile devices used by the PSR, appointed agents or intermediaries for the purpose of processing customer and counterparty information:
   (a) mobile device to be adequately hardened and secured;
   (b) ensure there is the capability to automatically wipe data stored in the mobile devices, in the event the device is reported stolen or missing;
   (c) comply with industry standards processed in card payments to mitigate risks of unauthorised data access, identity theft and fraud[39]; and
   (d) enforce the masking of sensitive customer and counterparty information when displayed on mobile devices.

[39] Such as have not been compromised, jailbroken or rooted.

Appendix 5 Control Measures on Cybersecurity

A PSR must adopt robust control measures to enhance its network resilience against cyber threats.

Part A: Network Security

1. A PSR must ensure technology networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including firewall and Intrusion Prevention System (IPS). This must include a network for delivery of digital services and wireless networks as well.

2. A PSR must ensure security controls for server-to-server external network connections include the following:
   (a) use of PKI based authentication method or equivalent alternatives;
   (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and
   (c) deploying staging servers with adequate perimeter defenses and protection such as firewall, IPS and antivirus.

3. A PSR must ensure security controls for remote access to server include the following:
   (a) restricting access to only hardened and locked down endpoint devices;
   (b) using secure tunnels such as TLS and VPN IPSec;
   (c) deploying ‘gateway’ server with adequate perimeter defenses and protection such as firewall, IPS and antivirus; and
   (d) closing relevant ports immediately upon expiry of remote access.

4. A PSR must ensure overall security controls are implemented including the following:
   (a) dedicated firewalls at all critical segments. All external-facing firewalls must be deployed on High Availability (HA) configuration and “fail-close” mode activated;
   (b) IPS at all critical network segments with the capability to inspect and monitor encrypted network traffic;
   (c) web and email filtering systems such as web-application firewalls, web-proxy, URL filtering, sandboxing features, spam filter and anti-spoofing controls;
   (d) end-point protection solution to detect and remove security threats such as malware;
   (e) enforcing full hard disk encryption for all endpoints and systems as required;
   (f) solution to mitigate advanced persistent threats including zero-day and signatureless malware; and
   (g) capturing the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.

5. A PSR must synchronise and protect the Network Time Protocol (NTP) server against tampering.

6. A PSR must ensure its technology systems and infrastructure, including critical systems outsourced to or hosted by third party service providers, are adequately protected against all types of Distributed Denial of Service (DDoS) attacks (including Domain Named Service (DNS) based, volumetric, protocol and application layer attacks) through the following measures:
   (a) subscribing to DDoS mitigation services, which include automatic 'clean pipe' services to filter and divert any potential malicious traffic away from the network bandwidth; and
   (b) regularly assessing the capability of the provider to expand network bandwidth on-demand including upstream provider capability, adequacy of the provider's incident response plan and its responsiveness to an attack.

Part B: Data Security

1. A PSR must ensure that all data-at-rest of personal identifiable information (PII) and transaction data are securely protected and rendered unreadable to unauthorised access through the implementation of robust encryption mechanisms or equivalent capabilities.

2. A PSR must design internal control procedures and implement appropriate technology in all applications and access points to enforce Data Loss Provision (DLP) policies and trigger any policy violations. The technology deployed must cover the following:
   (a) data in-use – data being processed by IT resources;
   (b) data in-motion – data being transmitted on the network; and
   (c) data at-rest – data stored in storage mediums such as servers, backup media and databases.

3. A PSR must implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorised access to data.

4. A PSR must establish a clear DLP strategy and process to ensure that proprietary, customer and counterparty information is identified, classified and secured. At minimum, a PSR must:
   (a) ensure that data owners are accountable and responsible for identifying and appropriately classifying data;
   (b) undertake a data discovery process prior to the development of a data classification scheme and data inventory; and
   (c) ensure that data accessible by third parties is clearly identified and policies must be implemented to safeguard and control third party access. This includes adequate contractual agreements to protect the interests of the PSR and its customers.

5. A PSR must ensure adequate security controls are in place to safeguard against customer information breach (CIB)[40], which include:
   (a) conducting continuous review to ensure that CIB does not occur in the IT environments of the PSR, its intermediaries, or third-party service providers. The PSRs shall also incorporate scanning or screening of customer information into the scope of periodic security assessments (e.g., penetration testing, red teaming, or other security validation exercises);
   (b) enhancing cybersecurity operations to promptly detect and strengthen the safeguards against CIB;
   (c) ensuring that the scope of PSRs' internal audit reviews encompass the management and security controls pertaining to CIB; and
   (d) conducting a thorough investigation to identify the technical root cause(s) of all CIBs with appropriate action and consequence management to mitigate recurrence.

Part C: Security Operations Centre (SOC)

1. A PSR must ensure its SOC has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the PSR to detect anomalous user or network activities, flag potential breaches and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts. The outcome of the SOC activities shall also inform the PSR's reviews of its cybersecurity posture and strategy.

2. The SOC must be able to perform the following functions:
   (a) log collection and the implementation of an event correlation engine with parameter-driven use cases such as Security Information and Event Management (SIEM);
   (b) incident coordination and response;
   (c) vulnerability management;
   (d) threat hunting;
   (e) remediation functions including the ability to perform forensic artifact handling, malware and implant analysis;
   (f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations and monitoring Indicators of Compromise (IoCs). This includes advanced behavioral analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers; and
   (g) has a well-documented and standardized playbook that covers common and plausible cyber threat scenarios, such as ransomware attacks.

3. A PSR must ensure that the SOC provides monthly threat assessment report, which shall include, at minimum, the following:

[40] This is also applicable to the PSRs intermediaries as well as their third-party service providers.

(a) trends and statistics of cyber events and incidents categorised by type of attacks, target and source IP addresses, location of data centres and criticality of applications; and
(b) intelligence on emerging and potential threats including Tactics, Techniques and Procedures (TTP).

4. A PSR must subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and support the implementation of countermeasures.

5. A PSR must ensure the following:

(a) the SOC is located in a physically secure environment with proper access controls;
(b) the SOC operates on a 24x7 basis with disaster recovery capability to ensure continuous availability; and
(c) the SOC has a holistic and end-to-end view of the PSR's infrastructure including internal and external facing perimeters.

Part D: Vulnerability Assessment and Penetration Test (VAPT)

1. A PSR must establish standard operating procedures (SOP) for VAPT activities to continuously identify vulnerabilities, assess potential risks and remediate the identified gaps. The SOP must outline the relevant control measures including but not limited to ensuring that the activities of external penetration testers are within the defined scope and are always subject to continuous oversight, validating the event logs and ensuring data purging.

2. A PSR shall perform a quarterly vulnerability assessment of external and internal network components that support all critical systems.

3. A PSR must conduct annual intelligence-led penetration tests on its internal and external network infrastructure, critical systems as well as digital services including web, mobile and all external-facing applications. The penetration testing must reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. A PSR must engage suitably accredited penetration testers and service providers to perform this function.

4. In addition to the periodic testing, a PSR must conduct intelligence-led penetration tests prior to introducing new systems for the new products or services to ensure that the IT infrastructure is not accidently exposed due to unchecked network configuration.

5. A PSR must ensure the outcome of the penetration testing exercise is properly documented and escalated in a timely manner to senior management to identify and monitor the implementation of relevant remedial actions.

6. A PSR must undertake an independent compromise assessment on the technology infrastructure of its critical systems at least once every three years and to ensure that the results of such assessments are escalated to senior management and the board in a timely manner.

Part E: Application Programming Interface (API) Security

1. A PSR must ensure that the level of API security implemented commensurate with the potential risks involved. At minimum, PSRs is required to implement the following measures to mitigate cybersecurity risks associated with APIs:

   (a) implement and maintain a centralized API inventory. The inventory must comprehensively encompass identification, classification and prioritization of all associated API connections and dependencies;
   (b) ensure availability of API service by designing APIs to be scalable for handling high level of traffic and implementing measures to mitigate denial of service attacks;
   (c) undertake secure coding practices during API development, which shall include but not be limited to validating security of third-party code and libraries, implementing robust error handling, input validation and appropriate security headers;
   (d) employ robust encryption standards and effective key management controls;
   (e) deploy anti brute-force mechanisms such as rate limiting, account lockout, captcha challenges, and others;
   (f) implement strong and robust authorization and authentication protocols that commensurate with the risks presented by the APIs;
   (g) consider utilizing an API gateway to manage access, authentication, and authorization of the APIs;
   (h) conduct periodic security assessments on APIs, including penetration testing and static / dynamic security testing;
   (i) continuous monitoring for APIs to ensure visibility into the utilization and performance of the APIs, for prompt identification and detection of potential suspicious activities; and
   (j) establish process to effectively revoke access token or API keys in the event of a compromise.

Question 24:
Enhanced requirements in the control measures on cybersecurity

The requirements in this Appendix 5 is an overall enhancement on cybersecurity controls compared to the requirements in current E-Money, MA and GRMO PD, which is needed given the escalation of cyber threats in the industry. Therefore, please provide:

(a) Specific requirements which your institution would anticipate to have significant challenges to implement. Please also provide clear justification on the reasons for such challenges; and

(b) Please provide your views and comments on the frequency of assessment as described in paragraphs 2, 3 and 6 of Part D of this appendix.

The rest of the page is intentionally left as blank.

Appendix 6 IT and Cyber Risks associated with third party service providers

1. Operational performance and capacity (including staff competency and bench strength to mitigate key-man risks, system infrastructure reliability and IT operation management for service quality, strong recovery and resumption capability for business continuity).
2. Security requirements to mitigate information security risks relating to secure handling of confidential information pertaining to the PSR, its customers or counterparty during transmission, process or storage of such information:
   (a) security governance;
   (b) IT asset management and protection against evolving cyber threats. This includes ensuring the storage of its data is at least logically segregated from the other clients of the third-party service provider;
   (c) secure system development lifecycle;
   (d) physical security;
   (e) personnel security;
   (f) access management; and
   (g) incident management.
3. Cyber supply chain risks:
   (a) vetting of personnel;
   (b) vetting of third-party or open source software and system interdependence;
   (c) third-party risk management for key sub-contractors; and
   (d) concentration and geopolitical risk.

Appendix 7 Guidance on Emerging Technologies

1. As the landscape of emerging technologies is dynamic and evolving, a PSR shall ensure TRM is effective in monitoring the build-up of risks at the enterprise level arising from the use of new technologies. A PSR must provide clarity in its governance arrangement relating to new technologies as follows:
   (a) appropriate level of caution, factoring the unintended consequences such as fairness, ethics, legal liability exposures and frictions to vulnerable customers in the risk assessment and tolerance level;
   (b) acceptance criteria for introduction of new technology and reporting structure and oversight mechanism to uphold accountability throughout the lifecycle of adoption;
   (c) enhancement of technology and cybersecurity operation controls to mitigate attendant risks; and
   (d) evaluation and improvement of operating control effectiveness on on-going basis.

2. A PSR must only allow the use of emerging technology in a production environment when, at minimum, the following requirements are met:
   (a) IT system using the new technology is adequately tested to meet the service quality, resiliency, and information security objectives of the institution with residual risk that remains within the PSR's risk tolerance level;
   (b) availability of industry standards and best practices to effectively test the operation risk controls and cyber defence. Where this cannot be met, additional margin of conservatism shall be applied in the risk assessment and the scope of provision to customers;
   (c) prepare to suspend the use of emerging technology applications when extreme events such as adversarial attacks arises;
   (d) implement regular monitoring to assess consistency in the quality of the solution, security and compliance, enabling timely identification and mitigation to any emerging risks or issues; and
   (e) disclose to users that emerging technology is utilized in the system, providing adequate information about associated risks to enable them to make an informed decision before using the service.

Appendix 8 Key Risks and Control Measures for Cloud Services

This appendix provides additional guidance to PSRs for the assessment of common key risks and considerations of control measures when PSRs adopt public cloud for critical systems. The guidance is broadly applicable across various cloud service models and PSRs are expected to apply a risk-based approach in implementing the guidance.

The guidance consists of two (2) parts:

- **Part A: Cloud governance** – describes the considerations governing the cloud usage policy, and technology skills capacity to implement cloud services securely and effectively.
- **Part B: Cloud design and control** – describes the considerations related to designing robust cloud infrastructure and in operationalising the cloud environment. This places emphasis on cloud architecture, cloud application delivery model, high velocity software development, user access management, data protection, key management, cloud backup and recovery, business continuity management and cybersecurity management.

Part A: Cloud Governance

A PSR is expected to ensure robust cloud governance processes are established prior to cloud adoption and are subject to on-going review and continuous improvement. This should cover the following areas:

1. Cloud risk management

(a) The board of a PSR is expected to promote and implement sound governance principles throughout the cloud service lifecycle in line with the PSR's risk appetite to ensure safety and soundness of the PSR.

(b) The senior management of a PSR is expected to develop and implement a cloud risk management framework that integrates with existing outsourcing risk management framework, technology risk management framework (TRMF) and cyber resilience framework (CRF), for the board's approval, proportionate to the materiality of cloud adoption in its business strategy, to assist in the identification, monitoring and mitigating of risks arising from cloud adoption.

(c) Common cloud service models[41] are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), wherein each presents a different set of capabilities offered to the PSR

[41] Cloud service models consist of SaaS, PaaS and IaaS. For SaaS, PSRs, as a consumer, uses the cloud service provider's applications running on a cloud infrastructure. PaaS is a service model where PSRs deploy application onto cloud infrastructure using the platform capabilities e.g., programming languages, libraries services and tools supported by the cloud service provider. IaaS is a service model where cloud service provider offers fundamental computing resources such as compute, network, or storage, where PSRs can deploy application and operation systems.

as the cloud consumer, and hence a different set of shared responsibilities. In view of this, the cloud risk management framework of the PSR is expected to:

i) be an integral part of the PSR's enterprise risk management framework (ERM);

ii) be tailored to the cloud service models, both currently in use or being considered for use; and

iii) specify the scope of the PSR's responsibility under each shared responsibility model, as the associated risks may vary.

(d) A PSR is responsible for the protection of data stored in cloud irrespective of cloud service models and the cloud service providers. Therefore, the PSR's understanding of the specific details of the cloud arrangement, particularly what is or is not specified in the terms of the contract with the cloud service providers is essential.

(e) Regardless of the cloud arrangement with cloud service providers, the onus remains on the PSR to satisfy the Bank that it is protecting customer information and ensuring service reliability.

(f) The use of cloud services may represent a paradigm shift in technology operation management as compared to on-premises IT infrastructure. Business processes may change and internal controls on compliance, business continuity, information and data security may be overlooked due to the ease of subscribing to cloud services. Therefore, the cloud risk management framework should also clearly articulate the accountability of the PSR's board and senior management, and the process involved in approving and managing cloud service usage, including the responsibility of key functions across the enterprise in business, IT, payment services, legal, compliance and audit, over the lifecycle of cloud service adoption.

(g) As the cloud landscape rapidly evolves, a PSR's cloud risk management framework is expected to undergo periodic review (at least once every three years to ensure its adequacy and effectiveness to manage new service models over time), or immediately upon any major cyber security incidents involving the cloud services.

2. Cloud usage policy

(a) The PSR's senior management is expected to develop and implement internal policies and procedures that articulate the criteria for permitting or prohibiting the hosting of information assets on cloud services, commensurate with the level of criticality of the information asset and the capabilities of the PSR to effectively manage the risks associated with the cloud arrangement.

(b) A PSR is expected to expand the scope of its current technology assets inventory to include critical systems hosted on the cloud services, with a clear assignment of ownership, and to be updated upon deployment and changes of IT assets to facilitate timely recalibration of cybersecurity

posture in tandem with an evolving threat landscape. Having visibility on the latest view of the technology asset would enable effective triaging, escalation and response to information security incidents.

(c) A PSR is expected to regularly review and update the cloud usage policy at least once every three years. However, where any material changes arise, including but not limited to adoption of new cloud service deployment model, or adoption of cloud service for IT systems with higher degree of criticality, the PSR is expected to review and update its cloud usage policy immediately.

3. Due diligence

Due diligence on the prospective cloud service providers are expected to be risk-based and conducted to a level of scrutiny that is commensurate with the criticality of the information and technology assets to be hosted on the cloud in compliance with relevant requirements and guidance as stipulated in the Third Party Service Provider Management section of this policy document and the relevant paragraphs in the E-Money, MA and GRMO policy documents.

4. Access to cloud service providers' certifications

A PSR is expected to review their cloud service providers' certifications prior to entering into any cloud arrangement or contract with such cloud service providers. At a minimum, a PSR is expected to:

(a) seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider's action plans for mitigating any non-compliance; and

(b) obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. The PSR's risk assessment is expected to address all the requirements and guidance as stipulated in the Cloud Services section of this policy document.

5. Contract management

A PSR is expected to set out clearly and where relevant, measurable, contractually agreed terms and parameters on the information security and operational standards expected of the cloud service providers. Such contract terms and parameters are expected to be aligned with the PSR's business strategy, information security policies and regulatory requirements.

(a) The terms of the contracts between the PSR and cloud service providers is expected to address the risks associated with cloud services and third-party service providers;

(b) Jurisdiction risk may arise because cloud service providers operate regionally or globally in nature and may be subject to the laws and regulatory requirements of its home country, the location of incorporation, and the country where the client receives the service. Therefore, a PSR is expected to:

i) identify and address potential jurisdiction risks by adopting appropriate mitigating measures, where practically possible, to ensure the use of cloud services does not impair its ability to comply with local law and regulatory requirements; and

ii) understand the scope of local customer protection legislation and regulatory requirements as well as to ensure that the PSR receives adequate protection and recourse for the benefit of its customers, in the event of a data breach or fulfilment of a legal data request by the cloud service provider.

(c) A PSR is expected to assess the potential impact and formalise arrangements with cloud service providers to comply with local laws and regulatory requirements for incident investigation and law enforcement purposes. This would include adhering to data retention requirements and data access procedural arrangements to ensure the confidentiality and privacy of the customers are protected; and

(d) The provision of cloud services by the primary cloud service provider may interconnect with multiple layers of other fourth party service providers (such as sub-contractors), which could change rapidly. For example, customer data could be leaked due to exposure caused by fourth party service providers. To mitigate the risks associated with such fourth party service providers, PSRs are expected to:

i) understand the scope of customer information shared across the supply chain and ensure that relevant information security controls can be legally enforced by the PSR; and

ii) ensure Service Level Agreement (SLA) negotiations and contractual terms cover the performance matrix, availability, and reliability of services to ensure that the cloud service providers agree and are formally aligned on the requirements and standard of cloud services provided. In addition, cloud service providers are expected to be accountable to the PSR for the SLA, performance matrix, availability and reliability of cloud services rendered by its service providers (i.e. subcontractors).

6. Oversight over cloud service providers

A PSR is expected to ensure effective oversight over cloud service providers taking into account the fact that the cloud service providers may engage sub-contractor(s) to provide cloud services. This includes, at minimum, the following:

(a) establish and define a continuous monitoring mechanism with alignment to the enterprise outsourcing risk management framework (or equivalent) to ensure adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis;
(b) identify, assign and document the key responsibilities within the PSR for continuous monitoring of cloud service providers to ensure accountabilities are clearly defined;
(c) perform assessments of the outsourcing arrangement involving cloud service providers periodically in accordance with the PSR's internal policy to achieve business resilience with emphasis on data security and ensure prompt notification to the Bank of the developments that may result in material impact to the PSR (such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development), in particular, provisions relating to outsourcing of cloud services outside Malaysia including the relevant paragraphs in the E-Money, MA and GRMO policy documents; and
(d) promptly review or re-perform risk assessment upon any material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development.

7. Skilled personnel with knowledge on cloud services

(a) The adoption of cloud services requires commensurate changes to the PSR's internal resources and process capabilities. In this regard, a PSR is expected to:
    i) equip its board and senior management with appropriate knowledge to conduct effective oversight over the cloud adoption; and
    ii) ensure its IT and security operations or relevant personnel are appropriately skilled in the areas of cloud design, migration, security configurations, including administrative, monitoring and incident response.
(b) The effective management of cloud services is not purely the responsibility of the PSRs' IT function. Therefore, a PSR is expected to ensure relevant internal resources in business operations, payment services, procurement, legal, risk and compliance are also adequately skilled and engaged to manage the change in risk profile arising from cloud adoption. This should also enable PSRs to respond effectively to operational incidents.
(c) A PSR is expected to equip internal audit and personnel undertaking the risk management and compliance functions with relevant cloud computing

and cloud security skills to be able to verify the effectiveness of the information security controls in alignment with the PSR's cloud usage policy and information security objectives.

(d) A PSR is expected to ensure that its staff receive adequate training to understand their responsibilities in complying with internal cloud usage policies and are prepared to effectively respond to a range of security incident scenarios developed on a risk-based approach.

(e) A PSR is expected to expand the scope of the formal consequence management process to govern the use of cloud services to ensure the cloud usage policy is effectively enforced given that cyber hygiene is critical to ensure the continued security of cloud service usage.

Part B: Cloud Design and Control

A PSR is expected to design its adoption of cloud services with a degree of portability, scalability and fault tolerance that is proportionate to the materiality of the cloud service to its business operation. It is expected to also ensure robust operational controls are in place to manage its ongoing cloud operations.

1. Cloud architecture

(a) A PSR is expected to design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application.

(b) A PSR is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an “assume breach” mindset, layering defence-in-depth through micro-segmentation, “deny-by-default“, “least privilege” access rights, and conducting deep inspection and continuous validation where applicable.

(c) A PSR is expected to use the latest network architecture approach and appropriate network design concept and solutions for managing and monitoring granular network security and centralized network provision in managing complexity of the cloud network environment.

(d) A PSR is expected to establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms.

(e) For PSRs leveraging on their financial group’s cloud infrastructure, the PSRs is expected to consider an appropriate level of network segregation (e.g., logical tenant isolation in the shared environment of the cloud) to mitigate the risk of cyber-attacks from propagating cross-border or cross-entity and affecting the Malaysian PSR’s operations.

(f) The increasing use of application programming interfaces (API) by PSR to interconnect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface, and any mismanagement may amplify the impact of an information security incident. A PSR is expected to ensure its APIs are subject to rigorous management and control mechanisms which include the following:

i) APIs are expected to be designed for service resilience to avoid the risk of single points of failure and configured securely with appropriate access controls; and

ii) APIs are expected to be tracked and monitored against cyber-attacks with adequate incident response measures and are de-commissioned on a timely basis when no longer in use.

2. Cloud application delivery models

(a) Cloud application delivery models may evolve to support faster time-to-market in response to consumer demand. Currently, DevOps and Continuous Integration / Continuous Development (CI/CD)[42] are amongst the prevailing practices and processes for cloud application delivery. For instance, the ability to enforce segregation of duties for CI/CD where application developers may require access to the management plane for service configuration. A PSR is expected to ensure CI/CD pipelines are configured properly to enhance security of automated deployments and immutable infrastructure[43].

(b) A PSR is expected to continuously leverage enhanced cloud capabilities to improve the security of the cloud services and PSRs are, among others, encouraged to:

i) adopt industry best practices such as infrastructure-as-code (IaC)[44] to automate the provisioning of IT infrastructure in a consistent, scalable and secure manner; and

ii) use immutable infrastructure practices for deployment of services to reduce the risk of failure by creating a new environment with the latest stable version of the software. The on-going monitoring of the cloud environment should include automating the detection of changes to immutable infrastructure to improve compliance review and combat evolving cyber-attacks.

(c) Where relevant, a PSR is expected to implement appropriate controls on the IaC process to minimise the risk of misconfiguration and reduce the cyber- attack surface. This includes the following measures that is expected to be taken by the PSR:

i) conduct vulnerabilities scanning as part of IaC automation steps and ensure issues are remediated prior to the provisioning of IT infrastructure;

ii) ensure virtual machine images (VMI) or container images of IaC templates are trusted and digitally signed; and

iii) implement appropriate access control to prevent unauthorised changes to IaC templates.

[42] CI/CD is a set of methods that enables developers to deliver code changes more frequently using automation.

[43] Immutable infrastructure is an approach to managing and deploying infrastructure where components, such as virtual servers and networks, are created once and then never modified. If a new version of a service or application requires changes to the underlying infrastructure components, new instances of those components are created and the old instances are replaced.

[44] The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools. - NIST Special Publication 800-172, U.S. Department of Commerce, February 2020

3. Virtualization and containerization management

The guidance provided in this paragraph is applicable to PSRs which use or plan to use PaaS and IaaS cloud service models only.

(a) A PSR is expected to ensure virtualization services are configured in line with the prevailing guidance from the cloud service providers and industry best practices, commensurate with the evolution of cloud computing technologies.

(b) A PSR is expected to ensure virtual machine and container images are configured, hardened, and monitored appropriately. This includes the following:

i) use stable images and keep images up to date;
ii) store and use images from trusted repositories or registries;
iii) scan images for vulnerabilities, remediate any vulnerabilities prior running in production;
iv) enforce “least privilege” access;
v) harden images based on industry best practices; and
vi) stored images are subjected to security monitoring from unauthorised access and changes.

4. Change management

(a) A PSR is expected to establish a process to systematically assess and take appropriate action to manage the impact of the releases by cloud service providers in relation to existing infrastructure, network, upstream and downstream systems to minimize the impact of any service disruption.

(b) A PSR is expected to ensure its existing change management process is extended to cover cloud services where appropriate to promote effective and secure system development. The escalation process and approving authority should be clearly defined to ensure critical changes can be implemented and risk of service disruptions are mitigated promptly.

(c) All critical changes deployed to the production environment should also be timely applied across environments such as disaster recovery site or supported cloud regions and availability zones where appropriate.

5. Cloud backup and recovery

(a) As part of an effective recovery capability, PSRs are expected to ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following:

i) define and formalise backup and recovery strategy at the planning stage of cloud adoption;

ii) conduct periodic reviews of the cloud service providers' restoration and recovery capabilities; and

iii) conduct testing of recovery strategy prior to deployment of the system.

(b) A PSR should is expected to ensure backup and restoration procedures are periodically tested to validate recovery capabilities. The frequency of backup procedures should be commensurate with the criticality of the system and recovery point objective (RPO) of the system. Remedial actions should be taken promptly by the PSR for unsuccessful backups.

(c) A PSR is expected to ensure sufficient backup and recovery of virtual machine and container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following:

i) ensure the capability to restore a virtual machine and container at point-in-time[45] as per the business recovery objectives; and

ii) make virtual machine and container images available in a way that would allow the PSRs to replicate those images at alternate sites or recovery sites[46].

(d) A PSR is expected to assess the resilience requirements of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. PSRs are expected to consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentration risk. Amongst the viable options are:

i) leverage cloud services' high availability and redundancy features to ensure production data centres have redundant capacity in different availability zones;

ii) achieve geographical redundancy by having data centres in different geographical regions;

iii) adopt hybrid cloud (combination of on-premises and public cloud setup);

iv) establish back-up cloud service providers and identify appropriate arrangement for porting of data and application to ensure timely service resumption; and

v) adopt multi-cloud strategy, with the use of services from different cloud service providers to mitigate concentration risks and geopolitical risks.

[45] Point-in-time refers to the ability to preserve and retrieve the state of a virtual machine or system at a specific moment.

[46] The alternate sites and recovery sites could either be in-house arrangements, or available through agreement with third-party recovery facility provider, or a combination of both options.

6. Interoperability and Portability

Interoperability standards for cloud services continue to evolve such that porting data, related configuration and security logging across different cloud service providers may be challenging. To facilitate the smooth process of interoperability and portability between on-premise IT systems or alternate cloud service providers, PSRs are encouraged to:

(a) assess technical requirements for interoperability and portability prior to entering into an agreement or arrangement with the cloud service providers to avoid vendor lock-in;
(b) maintain a list of third party service providers and tools that are needed to facilitate a smooth transition;
(c) ensure usage of standardized network and communication protocols for ease of interoperability and portability with on-premise IT systems or alternate cloud platforms;
(d) ensure the use of common electronic data formats, where applicable, to ease the movement of data between cloud service providers or to on-premises IT system; and
(e) extend patch and EOL management to ensure technology solutions employed remain effective and protected against system vulnerabilities.

7. Exit strategy

(a) A PSR is expected to establish a robust cloud exit strategy as part of its cloud risk management framework to prepare for extreme adverse events such as the unplanned failure or termination of cloud service providers. The exit strategy is expected to:
    i) be developed during the cloud deployment planning phase rather than on an ex-post basis;
    ii) identify alternative cloud service providers (multi-cloud approach) or third-party solutions, or other such means to ensure no business recovery objectives disruption or vendor lock-in;
    iii) be properly documented including details on the various exit trigger scenarios, roles and responsibilities, and sufficient resources to manage exit plans and the transition activities; and
    iv) be updated in a timely manner to reflect any material developments.

(b) A PSR's exit strategy is expected to be supported by an appropriate and proportionate exit plan that establishes the operational arrangements to facilitate an orderly exit from an agreement or arrangement with cloud service provider, including the following:

i) conduct impact assessment to determine potential costs, resources, and timing implications of transferring cloud services to an alternative cloud service providers or rely on the in-house arrangement at the PSR;
ii) identify appropriate methods to port data and applications to an alternative arrangement;
iii) to obtain written confirmation or attestation from the cloud service providers or independent external service providers that all sensitive data has been securely deleted from the cloud service provider's system upon completion of the exit process; and
iv) conduct testing to validate the effectiveness of the exit plan, to obtain a reasonable degree of assurance of its effectiveness.

8. Cryptographic key management

(a) A PSR is expected to implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud.
(b) A PSR is expected to ensure its policies and procedures on cryptography are extended to cover cloud services where relevant, to promote the adoption of strong cryptographic controls.
(c) Where appropriate and feasible, PSRs are expected to retain ownership and control of the encryption keys (themselves or with an independent key custodian), independent from the cloud service provider, to minimize the risk of unauthorised access to the data hosted on the cloud.
(d) As the usage of cloud adoption increases, managing many encryption keys used for protecting data has become more complex and may introduce new challenges for PSRs. A PSR is expected to adopt a comprehensive and centralized approach to key management including the use of centralised key management system that can handle generations, storage and distribution of keys in a secure and scalable manner.

9. Access Controls

(a) The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, PSRs are expected to ensure the use of strong controls for accessing the management plane which may include the following:
i) allocate dedicated and effectively hardened endpoints and up to date patching of software to access the management plane;

ii) implement “least privilege” and strong multi-factor authentication (MFA) e.g., strong password, soft token, privileged access management tool and maker-checker functions;
iii) employ granular entitlement allocation for privileged users;
iv) conduct continuous monitoring of the activities performed by privileged users; and
v) ensure secure communication protocols are in place for accessing the management plane. e.g., secure end-to-end communication channels, whitelisting of IP addresses, etc.

(b) A PSR is expected to extend its user access matrix to cover user access rights for both the PSR and its cloud service providers where relevant for the ongoing access to cloud services.

(c) A PSR is expected to ensure their tenant access controls to all hypervisor management functions or administrative consoles for systems hosting virtualized systems are effectively implemented in accordance with the requirements and guidance under the Access Control section of this policy document. These controls should mitigate the risk of any unauthorised access to the hypervisor management functions and virtual machine.

(d) Point-to-point connections with cloud services may proliferate with the ease of cloud adoption, resulting in fragmentation of identity and access management and the risk of unsanctioned data being migrated to the cloud. In view of this, rigorous planning is recommended for the design of identity and access management as it is inherently complex. PSRs are encouraged to:
i) where appropriate and commensurate with the size and complexity of the cloud adoption, implement a federated[47] approach for identity and access management to mitigate risks of identities in cloud services being disjointed from the internal identities, unauthorised access and to ease user access management; and
ii) consider additional attributes in context-aware decisions for identity and access management such as pattern of access to further mitigate the risks associated with remote access.

10. Cybersecurity Operations

(a) A PSR is expected to ensure the governance and management of cybersecurity operations is extended to cover cloud services, with appropriate control measures to prevent, detect, and respond to cyber

[47] Federated approach for identity and access management is a process / arrangement between multiple systems or enterprises that enables users to use the same identification data to access all related networks.

incidents in the cloud environment to maintain the overall security posture of the institution.

(b) The interconnected cloud service supply chain could become a source of cyber risk. A PSR is expected to ensure integrated monitoring and full visibility of cloud services are established. This should include the following:

i) continuous monitoring of system communications between the cloud service provider, on-premise IT systems and other service providers to ensure the security perimeter is not breached; and

ii) ensuring that third party service providers, including those providing ancillary functions, have adequate capabilities to monitor, detect and respond to anomalous activities, with timely communication to the PSR of relevant cyber incidents.

(c) A PSR is expected to understand the segregation of responsibility in security management, which varies across the cloud service models. A PSR should manage the sources of vulnerabilities appropriately including by:

i) proactively seeking assurance of their cloud service providers to conduct periodic VAPT on the cloud infrastructure to ensure tenant isolation and overall security posture remains healthy; and

ii) understanding the cloud service provider's VAPT policy for the PSR on cloud infrastructure for IaaS model given the varying degree of the PSR's access to the cloud environment and establish a VAPT arrangement with cloud service providers upfront which commensurate with the complexity of the cloud environment.

11. Distributed Denial of Service (DDoS)

(a) A PSR is expected to ensure that its DDoS mitigation service is commensurate with the size and complexity of the cloud adoption.

(b) The risk of a SPOF may surface when a PSR leverages solely on a cloud-based solution to mitigate DDoS attacks. As such, a PSR is encouraged to engage alternative DDoS mitigation providers or establish circuit breakers to avoid service disruption when the main DDoS mitigation provider is disrupted.

12. Data Loss Prevention (DLP)

(a) A PSR is expected to protect the data hosted in cloud services as required under the Data Security of Appendix 5 of this policy document, including the expansion of the endpoint footprint if the PSR allows its staff to use their own devices to access the sensitive data.

(b) As it becomes increasingly easy to distribute digital content to customers via cloud services, a PSR is expected to adopt the appropriate digital rights management mechanism to preserve the confidentiality of its proprietary and customer information.

13. Security Operations Centre (SOC)

(a) A PSR is expected to understand the scope of cloud service providers' responsibility for cybersecurity monitoring and adapt its SOC strategy and processes to ensure proactive and holistic monitoring of its cybersecurity posture. This adaptation should include the ability to effectively improve cybersecurity telemetry and analysis to detect and respond to cyber threats.

(b) Where applicable, the responsibilities of cloud service providers with respect to SOC operations should be formalised in the agreement or arrangement between the PSR and the cloud service providers, including the retention period required for relevant logs needed for forensic purposes and the right of the PSR to access the logs for quick restoration as and when needed, in accordance with the requirements and guidance under the Access Control section and Part C of Appendix 5 of this policy document.

14. Cyber response and recovery

(a) A PSR is expected to enhance existing cyber crisis management policies and procedures to remain in a state of readiness to respond to cyber threats in a cloud environment.

(b) A PSR is expected to extend its Cyber Incident Response Plan (CIRP) to include adverse scenarios that may affect cloud services and establish clear roles and responsibilities between the PSR and cloud service providers for incident response and remediation. The incident escalation process and turnaround time should be established with cloud service providers and periodically reviewed, to achieve an effective incident response.

(c) A PSR is expected to consider the following additional measures in the development of its CIRP:

i) enhancing its ability to detect security breach incidents to achieve effective incident management, including the ability to detect data leakage on the dark web;

ii) providing adequate assistance to customers in the event of a security breach in view that the complexity of cloud arrangements and sophistication of cyber-attacks often exceed the response range reasonably expected of customers; and

iii) ensuring CIRP is ready to manage cross-border incidents where the data resides in a foreign jurisdiction.

(d) A PSR is expected to ensure that relevant Cyber Emergency Response Team (CERT) members are conversant with the CIRP covering cloud services to effectively activate the CIRP when incidents occur.

(e) A PSR is expected to extend its existing incident reporting requirements to include cloud services.

(f) A PSR is expected to enter into agreements or arrangements with its cloud service providers to regularly conduct integrated business continuity testing and cyber drill in accordance to the cyber response and recovery section under this policy document to test the effectiveness of the PSR's CIRP and recovery plan.

(g) A PSR is expected to review its loss provision arrangements to ensure its adequacy to cover cyber incidents in accordance with the requirement on paragraph 11.17 of this policy document.

Appendix 9 Fraud Detection Standards

PSRs are required to adhere to the requirements specified. While compliance with the minimum standards is essential, PSRs are encouraged to exceed these standards to stay ahead of emerging threat. PSRs shall continuously upgrade and refine their fraud detection capability to ensure it remains robust against the anticipated level of threat.

1. A PSR must establish detailed and comprehensive risk profiles for each customer as a reference point when performing fraud detection based on behavioural analysis of the PSR's customer and fraud profiles.

   Examples of relevant factors to be considered may include:

   (a) demographics information e.g. age, gender, race, occupation, salary, language, etc;
   (b) geographical information e.g., city, state, countries, IP address;
   (c) historical transactional patterns e.g. monetary transfer amount, time of transaction, velocity, new beneficiaries/favourite transfer; and
   (d) behavioural patterns e.g., time taken to make transfer, typing speed, mouse hovering pattern.

2. A PSR must be able to detect and block suspicious or fraudulent transactions on a real-time basis based on individual customer risk profiles established in accordance with paragraph 1 through the fraud risk analytics. At minimum, the fraud risk analytics must include the parameters or indicators outlined below:

   (a) Access to or conduct of a digital account by a customer for a period of time following specific activities which could indicate elevated risk of identity theft or fraud, such as:
      i) newly enrolled digital account;
      ii) activation of digital account access for existing customer;
      iii) registration of multi-factor authentication method on a new device;
      iv) increase in transaction limit;
      v) password reset;
      vi) change of personal information such as phone number, email, and postal address; and
      vii) registration of third-party details (e.g. favourite accounts or beneficiary name), if applicable.
   (b) Transaction pattern(s) observed in a customer's account, which could indicate elevated risk of identity theft or fraud, such as:
      i) high volume of transaction or fund transfer in a short period to new beneficiaries within a day or next few days following such activities as specified in paragraph 2(a) of this Appendix;
      ii) sudden change in transaction patterns (e.g. for EMI businesses, increases in frequency or cumulative value over a short period, or

large withdrawals resulting in low account balance inconsistent with the customer's normal transaction patterns);

iii) activities that may be inconsistent with a customer's risk profile or history (e.g. transaction time, high transactions or fund transfer from a previously inactive account);

iv) large transaction value or fund transfer made into a newly opened account and withdrawn in a short period (e.g. within a few days);

v) transactions or fund transfer initiated from an unusual geographical location (not the customer's typical location) or consecutive transactions or fund transferred from different locations within a short period of time;

vi) transactions or fund transfer initiated from an account or device that was previously reported for fraud by various sources of fraud intelligence (e.g. upon investigation by a PSR, reports from customers or law enforcement agencies, industry threat intel sharing, etc.);

vii) transactions or fund transferred from a digital account that was previously inactive for a period of time; and

viii) transactions or fund transferred to suspected financial mules detected by your institution or any other fraud repositories developed by the Bank, the industry, or law enforcement authorities.

(c) Changes in a device fingerprint, such as the location, IP address, device MAC, operating system and other device profile. This must include the ability to detect and block attempts to defeat or bypass device fingerprinting methodologies;

(d) Account takeover and identity fraud using advanced artificial intelligence tools, techniques, and procedures to defeat or bypass the authentication controls of digital services or contact centre;

(e) Higher risk scoring must be applied for vulnerable customers (e.g. senior citizens, younger customers, previous victims of fraud, customers with lower literacy on the safety of electronic banking, electronic payment services facilities or awareness level, etc); and

(f) A PSR must expand risk parameters when detecting changes in biometric credentials registered in a device, where biometric technologies are solely used for financial transaction authentication purposes. This includes the scenario where a mobile digital application relies on the biometric verification function of the device, mobile operating system, or a third-party application.

Question 25:
Detecting and blocking suspicious or fraudulent transactions

(a) Would your institution face significant challenges in implementing real-time detection and blocking of suspicious or fraudulent transactions as required under paragraph 2 of this appendix? If yes, please provide clear justifications.
(b) What would be the appropriate timeline for detection and blocking of suspicious or fraudulent transaction that your institution may be able to implement?

3. A PSR must implement measures to promptly detect and terminate hijacked sessions to prevent unauthorised access to customer accounts. PSRs must notify customers on elevated cyber risk caused by the presence of risky apps such as apps downloaded outside official app stores, detected to contain security vulnerabilities or exhibit suspicious activities, with option for customer to accept the risk and associated risk mitigating measures if they wish to proceed.

4. When customers' mobile application access is restricted, PSRs must promptly notify customers with appropriate guidance to enable customers to restore access to their account subject to robust verification. To mitigate privacy concerns, a PSR must seek consent from the customers prior to effecting the customer device profiling.

5. A PSR must investigate suspicious transactions based on pre-determined priority levels and conduct the necessary verification (such as call-backs or other effective methods) with the customer prior to releasing any flagged transactions. To ensure acceptable customer experience, PSRs must notify the affected customer immediately upon the blocking of each suspicious transaction (e.g. via secured communication channel). Sufficient resources should be deployed to contact the affected customer in a timely manner after the transaction, including during peak periods. The verification procedures must consider and include ways to help detect circumstances where scam victims may be responding under the influence or threat of fraudsters. PSRs must also establish a robust process to minimize risk to the customer in the event the customer cannot be contacted due to their unavailability.

6. A PSR must ensure that its various touch points such as contact centres are easily accessible and sufficiently resourced to provide customers with prompt advice or to connect customers with the fraud investigation team, if necessary.

7. A PSR must continuously update its system to ensure fraud detection rules remain effective to combat new fraud modus operandi via the following:
   (a) enhancing its fraud detection rules promptly upon detection of new fraud techniques that have evaded its fraud detection system. The enhancements must be timely upon being notified by its internal fraud team or upon receiving such intelligence from external sources such as other PSRs, industry group, public-private partnership and other intelligence sharing platform; and
   (b) reviewing the effectiveness of its fraud detection parameters and thresholds in a timely manner, taking into consideration recent typologies in relation to fraudulent transactions and financial mule accounts, including new digital fraud techniques and modus operandi in other jurisdictions.

8. In order to effectively address the wide range of fraud alerts that can arise from various fraud modus operandi and techniques, it is important to have clear and detailed procedures for managing suspected fraud cases.

9. Therefore, PSRs must develop a comprehensive fraud management playbook, as a point of reference for the relevant staff to promptly identify, confirm, and respond effectively to various scenarios. The playbook must be updated and validated at least once a year, or more frequently if needed, to ensure it remains relevant in the evolving fraud landscape. This includes reflecting insights from assessments of confirmed fraud cases and lessons learnt from incidences in which the PSR was unable to detect the fraudulent activities or transactions.

Question 26:
Enhanced requirements in fraud detection standards

The requirements in this Appendix 9 is an overall enhancement on cybersecurity controls compared to the requirements in current E-Money, MA and GRMO PD, which is needed given the escalation of fraud and scam cases in the industry. Therefore, please provide areas of specific requirements which your institution would anticipate to have significant challenges to implement. Please also provide clear justification on the reasons for such challenges.

Appendix 10 Control Measures on Payment Acceptance Device

PSRs who are acquirers should ensure all relevant risks associated to the use of merchant's payment acceptance device are mitigated, including the following:

1. ensuring the payment acceptance devices are:
   (a) adequately hardened and securely configured using methods that ensure its integrity and authenticity;
   (b) protected from tampering and cyber threats such as malware attacks, key logger, and etc;
   (c) designed for the protection of PIN data;
   (d) certified to be fully compliant with applicable security standards, e.g. PCI PIN Transaction Security (PCI PTS), Software-based PIN Entry on COTS (PCI SPoC), etc.; and
   (e) used solely as the payment acceptance device.

2. ensuring PIN entry process and cardholder verification method (CVM) applications are secured and protected against manipulation or sabotage;

3. providing guidance for merchants to ensure the PIN is entered in a way that it cannot be observed by an unauthorised party;

4. PIN data must be encrypted upon entry and remain encrypted when transmitted to protect against malicious activity and attacks;

5. ensuring data is protected at all times to prevent data leakage and no data is stored on the payment acceptance devices;

6. ensuring only dedicated merchant staff are allowed to perform system administration functions (e.g. performing correction) of the payment acceptance device; and

7. for PIN Entry on COTS:
   (a) ensuring PIN CVM applications run only on secured and supported versions of operating systems which have not been compromised, jailbroken or rooted i.e. the security patches are up-to-date; and
   (b) (use of automated monitoring and attestation system to detect potential compromise of payment acceptance devices and ensuring that all components in the payment acceptance devices are always in a secure state.

Appendix 11 Control Measures on Quick Response Code

1. Ensure QR code authenticity which among others include:
   (a) QR codes are securely generated by host server, unique for each merchant/user/transaction, where dynamic QR codes should have reasonable expiry time;
   (b) block QR code application from operating on unsecured (e.g. rooted or jail-broken) devices;
   (c) any fake QR code shall be rejected upfront and the merchant/user shall be automatically notified of the authenticity of the scanned QR code; and
   (d) bind the QR code to the respective user or merchant ID and transaction amount.

2. Ensure QR codes do not contain any confidential data and are not stored in endpoint devices.

3. Ensure all relevant risks associated with the use of static QR codes at participating merchants are mitigated, including the following:
   (a) all information from the scanned QR codes shall be transmitted to payment instrument's host server for authentication;
   (b) educate merchants on fraud risk related to static QR codes and the preventive measures to effectively mitigate such risk (e.g. merchants shall regularly inspect the displayed static QR code to ensure it has not been tampered with); and
   (c) enforce masking of sensitive customer and counterparty information when displayed on mobile devices.