BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Payment System Operator

Applicable to−

1 Approved operators of payment systems
2 Operators of designated payment systems

Issued on: 22 December 2022 BNM/RH/PD 029-54

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 An operator of a payment system (PSO) performs the role of processing, clearing and settlement of payment transactions. It facilitates public and private entities, as well as consumers to transfer funds either directly from one account to another, or through the use of a payment instrument. In Malaysia, PSOs consist of both domestic and foreign-owned entities. While each of these entities may have unique characteristics depending on their different market segments and operational setups, all PSOs are regulated by Bank Negara Malaysia.

1.2 A well-functioning payment system is crucial for the efficient operation of the financial system as well as to support the needs of the economy as any disruptions may have broader system-wide implications. Therefore, effective oversight of the PSOs to ensure the safety and efficiency of all payment systems in Malaysia is fundamental to promote financial stability.

1.3 This policy document outlines requirements aimed to–

(a) ensure the safety, efficiency and reliability of payment systems;

(b) preserve public confidence in the payment systems and the use of payment instruments; and

(c) ensure payment systems are aligned with relevant international standards, such as the Principles for Financial Market Infrastructures issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO).

2 Applicability

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

3 Legal provisions

3.1 The requirements in this policy document are specified pursuant to−

(a) sections 33(1), 47(1) and 143 of the Financial Services Act 2013 (FSA); and

(b) sections 43(1), 57(1) and 155 of the Islamic Financial Services Act 2013 (IFSA).

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

4 Effective date

4.1 This policy document comes into effect on 22 December 2022.

5 Interpretation

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

5.2 For the purposes of this policy document−

"S" denotes a standard, an obligation, 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;

"approved operator of a payment system" refers to a person approved under section 11 of the FSA or section 11 of the IFSA to operate a payment system set out in paragraph 1 of Division 1 of Part 1 of Schedule 1 of the FSA or paragraph 1 of Part 1 of Schedule 1 of the IFSA respectively;

"Bank" refers to Bank Negara Malaysia;

"Board" refers to the board of directors of a PSO, including a committee of the board where responsibilities of the board as set out in this policy document have been delegated to such a committee;

"business continuity management" or "BCM" refers to an enterprise-wide framework that encapsulates policies, processes and practices that ensure the continuous functioning of a PSO during an event of disruption. It also prepares the PSO to resume and restore its operations and services in a timely manner during an event of disruption, thus minimising any material impact to the PSO;

"business continuity plan" or "BCP" refers to a comprehensive action plan that documents the processes, procedures, systems and resources necessary to resume and restore the operations and services of a PSO in the event of a disruption;

"business risk" refers to risks related to the administration and operation of the PSO as a business enterprise, which result in the potential impairment[1] of the financial condition (as a business concern) of the PSO and require the losses to be charged against capital. This excludes risks relating to the default of participants or other relevant parties, such as settlement banks or other PSO;

"control function" refers to a function that has a responsibility independent from business lines to provide objective assessments, reporting and assurance on the effectiveness of a PSO's policies and operations, and its compliance with legal and regulatory obligations. This includes the risk management function, the compliance function and the internal audit function or equivalent functions that perform similar roles of risk management, compliance and internal audit, by whatever name called;

"critical business functions" refer to business functions undertaken by a PSO, where the failure or discontinuance of such business functions is likely to–
(a) critically impact the PSO financially or non-financially; and
(b) disrupt the provision of essential services to its participants;

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

"cyber resilience framework" or "CRF" refers to a framework that ensures the PSO's cyber resilience;

"cyber risk" refers to threats or vulnerabilities emanating from the connectivity of internal technology infrastructure to external networks or the Internet;

"direct participant" refers to a participant that has access to a PSO's payment, clearing or settlement facilities. For avoidance of doubt, a direct participant is directly bound by all the rules and procedures established by the PSO that is made applicable to the participant;

"disaster recovery plan" or "DRP" refers to a comprehensive action plan that documents the procedures and processes that are necessary to recover and restore information technology (IT) systems, applications and data of a PSO in the event of a disruption;

[1] Potential impairment may result from poor execution of business strategy, ineffective response to competition, adverse reputational effects, or other business factors.

"essential services" refers to financial services that are essential to support the authorisation, clearing and/or settlement of payment transactions, which must continue to be provided by a PSO in the event of a disruption;

"executive director" refers to a director of a PSO who has management responsibilities in the PSO;

"independent director" refers to a director of a PSO who is independent in character and judgement, and free from associations or circumstances that may impair the exercise of his independent judgement;

"indirect participant" refers to a participant that has a contractual relationship with another entity (at times referred to as a sponsor institution) that is a direct participant of the PSO, and therefore has access to a PSO's payment, clearing or settlement facilities. An indirect participant may not be directly bound by certain rules and procedures established by the PSO;

"**maximum tolerable downtime" or "MTD**" refers to the timeframe allowable for a recovery to take place before a disruption compromises the critical business functions of a PSO;

"operator of a designated payment system" refers to a person who operates a payment system prescribed as a designated payment system under subsection 30(1) of the FSA or subsection 39(1) of the IFSA;

"operator of a payment system" or "PSO" refers to an approved operator of a payment system and operator of a designated payment system;

"outsourced service provider" refers to an internal group affiliate or external entity providing services to the PSO under an outsourcing arrangement. This could include, but is not limited to, technology-related functions or services that involve the transmission, processing, storage or handling of confidential information pertaining to the PSO;

"outsourcing arrangement" refers to an arrangement in which an outsourced service provider performs an activity on behalf of the PSO on a continuing basis[2], where the activity would otherwise be undertaken by the PSO[3];

[2] For the avoidance of doubt, an agreement which is time-bound does not preclude the activity from being considered as being performed on a continuing basis.

[3] For the avoidance of doubt, system or application leveraging, data center hosting, data center operations, data storage, cloud computing services and back-up location(s) are considered as outsourcing arrangements.

"outsourcing risk" refers to risk emanating from outsourcing arrangements that could result in a disruption to business operations, financial loss or reputational damage to the PSO[4];

"**recovery time objective" or "RTO**" refers to the timeframe required for systems and applications of a PSO to be recovered and operationally ready to support its critical business functions after a disruption. A recovery time objective has the following two components:

(a) the duration of time from the disruption to the activation of the BCP; and
(b) the duration of time from the activation of the BCP to the recovery of the business operations;

"senior management" refers to the Chief Executive Officer (CEO) and senior officers of the PSO;

"Technology Risk Management Framework" or "TRMF" refers to a framework that safeguards the PSO's information infrastructure, system and data; and

"tiered-participation arrangement" refers to an arrangement where an indirect participant relies on the services provided by the direct participant of a PSO in order to access the PSO's payment, clearing or settlement facilities.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with other relevant [5] legal instruments and policy document that have been issued by the Bank, and any subsequent review on such documents, in particular –

(a) Business Continuity Management;
(b) Fit and Proper Criteria for Approved Person;
(c) Interoperable Credit Transfer Framework;
(d) Management of Customer Information and Permitted Disclosures;
(e) Operational Risk Reporting;
(f) Payment Cards Framework; and
(g) Risk Management in Technology (RMiT).

[4] This includes strategic risk, reputational risk, compliance risk, operational risk, exit strategy risk, counterparty risk, country risk, contractual risk, information security risk and concentration risk.

[5] For the avoidance of doubt, where relevant, a PSO shall also comply with specific requirements of the Bank's policy document on areas such as Business Continuity Management, RMiT and any subsequent enhancements to these policy documents issued thereafter.

PART B GENERAL REQUIREMENTS

7 Demonstration of compliance

S 7.1 The requirements set out in this policy document shall apply to PSOs on an ongoing basis.

G 7.2 For PSOs that leverage on its parent and/or other foreign related entities to support the offering of its services in Malaysia, the PSO may demonstrate its compliance with the requirements in the policy document based on the existing arrangements/practices adopted by the PSO.

S 7.3 For purposes of paragraph 7.2, a PSO shall demonstrate its compliance with the requirements in the policy document by submitting relevant documentary evidence and justification[6] to the Bank which shall be signed off by a senior officer who is authorised by the PSO for the Bank's assessment. For the avoidance of doubt, submission of documentary evidence and justification alone does not automatically result in full compliance by the PSO.

S 7.4 A PSO shall notify the Bank and submit updated documentary evidence and justification, if relevant, as and when there are material changes that affect compliance with the requirements of this policy document.

S 7.5 In relation to paragraphs 7.3 and 7.4–

(a) a PSO shall submit additional information and/or documentary evidence to the Bank upon request to facilitate the Bank's review of the PSO's demonstration of its compliance; and

(b) the Bank reserves the right to review and assess whether the documentary evidence submitted by the PSO adequately fulfils the expectations of the policy document.

8 Submission requirements

S 8.1 The following information[7] shall be made available to the Bank upon request to facilitate the Bank's ongoing supervisory oversight–

(a) incident reports;

(b) system and service availability reports;

(c) audit reports[8];

[6] Documentary evidence may include audit reports, assessments from home regulators, attestation of compliance and any other relevant documents.

[7] Subject to the Bank's approval, a PSO may submit relevant attestation in lieu of the information requested.

[8] Refer to both internal and external audit reports.

(d) annual audited financial statements[9]; and
(e) any other information as may be required by the Bank.

[The remainder of this page is intentionally left blank]

[9] Annual audited financial statements may be prepared in accordance with accounting standards applied in the respective home jurisdiction of a PSO.

PART C GOVERNANCE

9 Governance arrangement

S 9.1 A PSO shall establish appropriate governance arrangements which are clear and transparent. To ensure resilient and efficient operations of the payment systems that support overall financial stability and other relevant public interest considerations, governance arrangements shall include, among others, the following–

(a) board of directors (the board) and senior management that consist of persons with calibre, credibility and integrity;

(b) clearly defined and documented organisational and operational arrangements, such as reporting lines between management and the board, ownership, management structure and control functions; and

(c) segregation of duties and internal controls to promote good corporate culture that reinforces ethical, prudent and professional behaviour, as well as reduces the chances of mismanagement and fraud.

10 Board of directors

S 10.1 The board must have a board charter that sets out the mandate, responsibilities and procedures of the board and its committees (if any), including matters reserved for the board's decision.

G 10.2 Board committees[10] should be established to assist the board in executing its duties and responsibilities. A board is encouraged to have, among others, a risk committee, an audit committee and a remuneration committee, or equivalents.

S 10.3 The board shall have the overall responsibility for promoting the safety, efficiency and reliability of the payment system which include–

(a) approving the strategic objectives, business plans and significant policies, including its risk appetite;

(b) overseeing the selection, performance, remuneration and succession plans of senior management, such that the board is satisfied with the collective competence of senior management to effectively lead the operations of the PSO;

(c) ensuring clear lines of responsibility and accountability are established and communicated throughout the organisation;

(d) establishing and providing oversight to the risk management function and material risk decisions, which include ensuring appropriate risk

[10] Board committees should be composed mainly of, and led by, non-executive or independent directors.

management policies, processes and infrastructure to manage the various types of risks, are in place and effectively implemented;

(e) ensuring the independence and effectiveness of internal control functions (refer to detailed requirements in paragraph 12);

(f) oversee and approve business continuity plans and ensure such plans are updated, particularly as and when there are material changes to the size, nature and complexity of the PSO operations that can significantly affect the said plans;

(g) promote timely and effective communication between the PSO and the Bank on matters affecting or that may affect the safety, efficiency and reliability of the PSO; and

(h) ensuring compliance with legal and regulatory obligations, including institution-specific supervisory requirements and expectations.

S 10.4 The board shall be composed of suitable members with appropriate mix of skills, experience and knowledge to effectively carry out their responsibilities.

S 10.5 The board shall include non-executive directors, including independent directors.

S 10.6 The board must be able to devote sufficient time to their roles and maintain a sound understanding of the business of the PSO as well as relevant market and regulatory developments.

11 Senior management

S 11.1 The senior management shall be responsible for the following–

(a) implement business and risk strategies and other strategic plans, such as technology plans and the associated technology policies and procedures, in accordance with the direction given by the board;

(b) establish and implement effective policies and procedures, among others, in the following areas–

(i) risk management and appropriate controls to manage and monitor risks (refer to detailed requirements in paragraph 12);

(ii) due diligence and oversight to manage outsourced arrangements supporting the payment system operations; and

(iii) sufficient and timely reporting or escalation of issues to the Board; and

(c) ensure a robust assessment is conducted on any deviations[11] from legal and regulatory requirements as well as internal policies and procedures. This includes addressing any supervisory concerns and the progress of

[11] For avoidance of doubt, the requirement is applicable to both internal policies and procedures as well as policy documents issued by the Bank.

remedial actions taken to address them, with material information to be reported to the board in a timely manner.

S 11.2 The senior management shall consist of individuals with the necessary skill set, competencies and experience to adequately support the operation and risk management of the PSO. This shall include individuals with appropriate technology background to provide guidance on the PSO's technology plans and operations.

S 11.3 For the purpose of paragraph 11.2, a PSO shall ensure that a designated staff who does not engage in the day-to-day technology operations shall be responsible for the identification, assessment and mitigation of technology risks.

12 Control functions

G 12.1 The board and senior management should create an environment which:
(a) ensure the PSO and its officers comply with legal and regulatory requirements that are applicable;
(b) adopt appropriate risk management practices; and
(c) encourage ethical conduct that underlies the above-mentioned requirements.

S 12.2 The board is responsible for the effectiveness of a PSO's control functions. The board shall–
(a) ensure the PSO's overall risk profile is consistent with the business strategy and risk appetite;
(b) ensure a clear, well-documented and effective risk management framework that is appropriate to the nature, scale and complexity of its activities is in place;
(c) ensure the internal control functions are established and allocated with sufficient resources, and ensure that the said functions and officers are provided with appropriate stature, authority and independence;
(d) ensure the internal control functions are resourced by officers who have appropriate skills and knowledge to effectively support the PSO's internal control framework; and
(e) provide relevant officers with direct and unimpeded access to the board.

S 12.3 In managing the technology and cybersecurity risks, the board shall–
(a) establish and approve the technology risk appetite which is aligned to the PSO's overall risk appetite statement. The board shall approve the corresponding risk tolerance for technology-related events and ensure key performance indicators are in place to monitor the PSO's technology risk against its approved risk tolerance;

(b) ensure senior management provides regular updates on the status of these indicators, key technology risks and critical technology operations to facilitate strategic decision-making; and

(c) ensure the adequacy of the PSO's IT and cybersecurity strategic plans. These plans shall address the PSO's requirements on infrastructure, control measures to mitigate IT and cyber risk as well as financial and non-financial resource needs. The plans shall be commensurate with the complexity of the PSO's operations and may require refinements in response to changes in the risk profile and business environment. These plans shall be periodically reviewed.

G 12.4 Given the rapidly evolving cyber threat landscape, the board should allocate sufficient time to discuss cyber risks and related issues, including the strategic and reputational risks associated with such cyber-incidents. The board should ensure it is kept abreast of developments on cyber threats and cybersecurity preparedness through on-going education and training. The PSO should ensure that these efforts are also supported by engagements with external experts where relevant.

S 12.5 The senior management is responsible for the effective management of a PSO's internal control framework. In discharging its responsibility, senior management shall–

(a) establish a control function commensurate with the size, nature of operations and complexity of the PSO;

(b) provide sufficient resources for the control function, including officer(s) with appropriate competencies and experience;

(c) report periodically to the board on compliance or risk issues and promptly on any material incidents of non-compliance; and

(d) report periodically to the board on the effectiveness of the PSO's overall management of compliance and risk management.

S 12.6 The board and senior management shall ensure that the risk management and control framework is periodically reviewed for continued effectiveness. This includes ensuring an audit by an independent party is conducted with reasonable frequency to detect weaknesses and enable corrective measures to be taken in a timely manner.

S 12.7 The control function must be independent of the business lines in order to carry out its role effectively. As such, a PSO must ensure that the control function is not placed in a position where there are real or potential conflicts in respect of, amongst others, scope of responsibilities, reporting lines or compensation.

S 12.8 The compliance function shall identify and assess the compliance risk associated with the PSO's activities. A designated compliance officer shall report to senior management on a regular basis the findings and analyses of compliance risk. The reports must be readily available to internal audit function of the PSO, the Bank and other relevant authorities upon request.

S 12.9 The internal audit function shall inform senior management, including the risk or compliance officer (or equivalent), of any incidents of non-compliance or material risks that it discovers.

[The remainder of this page is intentionally left blank]

PART D RISK MANAGEMENT AND OPERATIONAL REQUIREMENTS

13 Risk management framework

S 13.1 A PSO shall establish a risk management framework, which includes policies, procedures and systems, that enables the identification, measurement, control and continuous monitoring of all relevant and material risks, including risks that a PSO bears from and poses to its participants and other relevant parties[12] as a result of interdependencies.

S 13.2 In establishing the risk management framework, the PSO shall–

(a) align the framework with the PSO's risk appetite;

(b) clearly assign responsibilities and accountabilities for risk decisions; and

(c) ensure the framework facilitates efficient decision making in crises.

S 13.3 The framework shall be periodically reviewed for continued effectiveness and be supported by a robust management information system that facilitates the timely and reliable monitoring and reporting of risks.

S 13.4 A PSO shall establish risk monitoring and reporting requirements, which include periodic reporting to the board and senior management on the assessment of material risks affecting the PSO, to ensure risks are managed and mitigated in a timely manner. The reports must be readily available to the internal audit function of the PSO, the Bank and other relevant authorities upon request.

14 Business risk

S 14.1 A PSO shall establish robust management and control systems to identify, monitor and manage its business risk and hold adequate liquid net assets funded by equity[13] which are commensurate with its business risk profile and is sufficient to support its operations as a going concern under normal and stressed operating conditions.

G 14.2 A PSO may consider using a combination of tools such as risk management and internal control assessments, scenario analysis, and sensitivity analysis to identify business risks that may affect the PSO.

S 14.3 A PSO shall, at a minimum, maintain liquid net assets funded by equity equal to at least six months of current operating expenses.

[12] This may include other PSOs, settlement banks, liquidity providers, and service providers.
[13] This may include ordinary shares, disclosed reserves, and retained earnings.

G 14.4 In determining the appropriate level of liquid net assets funded by equity to be maintained internally, a PSO should consider its general business risk profile and the length of time required for a recovery or orderly exit that is appropriate to the critical business functions of the PSO in the event such action is taken.

15 Liquidity risk

S 15.1 A PSO shall establish a liquidity risk management framework to effectively identify, measure, monitor and manage liquidity risks faced by the PSO, including risks from its participants and other relevant parties.

S 15.2 A PSO shall measure and monitor its settlement and funding flows as well as maintain adequate liquid resources in all relevant currencies to ensure smooth settlement under normal or stressed operating conditions.

G 15.3 In determining the sufficiency of liquid resources including in terms of type and amount, a PSO should regularly conduct stress testing[14] which considers a range of relevant scenarios. Stress test results should be reported to the board and senior management to facilitate effective decision making on a timely basis and these results may also be used to validate the risk mitigation plans of a PSO, where relevant.

S 15.4 A PSO shall establish clear rules and procedures to address any unforeseen and potentially uncovered liquidity shortfalls, including the process of replenishing liquidity resources it may employ during a stress event, in order to continue operating in a safe and sound manner.

16 Credit risk

S 16.1 A PSO shall establish a credit risk management framework to effectively measure, monitor and manage its credit exposures to participants and other relevant parties[15] from its payment, clearing and settlement processes as well as to maintain sufficient financial resources[16] to cover its credit exposure to each participant.

G 16.2 A PSO should establish adequate processes to effectively manage its credit concentration risks, including through the establishment of exposure limits which

[14] A PSO may also conduct reverse stress testing or simulations to identify scenarios and/or extreme market conditions in which a PSO's liquid resources would be insufficient. For the avoidance of doubt, reverse stress testing is derived from a known adverse outcome and deduces possible forward-looking scenarios that could lead to such an outcome materialising for a PSO.

[15] Other relevant parties may include settlement banks and custodians.

[16] Financial resources may include collateral and other equivalent financial resources.

are determined based on potential losses that can jeopardise the solvency of, or public confidence in, the PSO.

G 16.3 In determining the amount and assessing the sufficiency of financial resources, a PSO should regularly conduct stress testing[17] which considers a range of relevant scenarios. Stress test results should be reported to the board and senior management to facilitate effective decision making on a timely basis and the results may also be used to validate the risk mitigation plans of a PSO, where relevant.

S 16.4 A PSO shall establish clear rules and procedures to address any credit losses as a result of default among its participants with respect to their obligations to the PSO. This includes the process a PSO must employ to replenish financial resources during a stress event, for it to continue operating in a safe and sound manner.

S 16.5 A PSO shall establish appropriate collateral management practices which include processes and procedures to support robust and reliable valuation, adequate monitoring of the collateral's condition and timely liquidation.

G 16.6 For purposes of paragraph 16.5, a PSO may, as appropriate–

(a) establish concentration limits for holdings of certain collateral, such as for collateral which are susceptible to high price volatility; and

(b) regularly mark-to-market the collateral and develop appropriate haircuts that are regularly validated, taking into account stressed market conditions to ensure sufficiency of collateral in the event of liquidation.

G 16.7 A PSO should be supported with a robust collateral management system to facilitate ongoing monitoring and management of collateral.

17 Operational risk

S 17.1 A PSO shall establish a robust management and control systems to identify, measure, monitor and manage sources of operational risk.

S 17.2 A PSO shall identify and assess the potential vulnerabilities from the operational risk it faces on an ongoing basis and ensure appropriate mitigation measures are implemented to address such risks on a timely basis.

S 17.3 A PSO shall ensure sufficient resources with appropriate competencies and experience are employed to effectively manage the operational risk of a PSO,

[17] A PSO may also conduct reverse stress testing or simulations to identify scenarios and/or extreme market conditions in which a PSO's financial resources would be insufficient to cover tail risks.

which include operating its systems safely and efficiently during normal and stressed periods.

System and service availability

S 17.4 A PSO shall establish adequate controls and measures to ensure the reliability, efficiency and smooth operation of the payment system with minimal disruption and to achieve high availability of the payment system and service.

S 17.5 For purposes of paragraph 17.4, the PSO shall define the service level objectives and set minimum service-level targets for the operation of the payment system.

S 17.6 A PSO shall ensure that the payment system has adequate capability and capacity to effectively manage its operations at all times including under stressed scenarios[18].

S 17.7 A PSO shall regularly monitor and test the actual capacity and performance of the payment system[19], as well as, plan for changes in volume or business patterns. The PSO shall also regularly conduct stress testing to verify whether the payment system can handle huge volumes of transactions under extreme circumstances.

G 17.8 In conducting stress testing as specified under paragraph 17.7, a PSO should ensure at minimum, the following–

(a) detailed approach and methodology of stress testing scenarios are adequately established and tested to ensure comprehensive coverage;

(b) participants' involvement in stress testing to identify weak system linkages and bottlenecks; and

(c) stress testing results are reviewed and updated as and when is required to ensure continued relevance and effectiveness of approach and scenarios.

18 Technology risk and information security

S 18.1 A PSO shall establish a technology risk management framework, to safeguard the PSO's information infrastructure, systems and data, which shall be an integral part of the PSO's risk management framework.

[18] E.g. high volume or erratic transaction, and prolonged disruption.

[19] For the avoidance of doubt, this should include monitoring and testing of the backup or recovery system, to ensure that the system is able to resume operations in the event of main system outage.

S 18.2 A PSO shall ensure confidentiality, integrity and availability of information held within the payment system by putting in place adequate controls to safeguard the information[20] and retention of all information including sensitive data.

S 18.3 In relation to paragraph 18.2, the PSO shall also ensure their relevant stakeholders, including outsourcing service providers, put in place appropriate controls to safeguard the confidentiality, integrity and availability of sensitive data.

G 18.4 In ensuring the confidentiality, integrity and availability of information held within internal systems, the PSO should undertake the following–

(a) develop a comprehensive data management framework that includes collection, identification, classification, handling, retention and disposal of data;

(b) ensure there is sufficient back-up mechanism in place to facilitate access to all data and information, including critical data and information at all times;

(c) ensure that information maintained in the system are not disclosed or accessible to any unauthorised users or third parties, and any changes or revision to the data and the system can only be made with proper authorisation;

(d) ensure that there are sufficient controls put in place to minimise human error, mishandling or any other potential gaps;

(e) conduct an IT risk assessment and identify appropriate mitigation measures to address risks identified through this assessment. The scope of the assessment should include but is not limited to the risk assessment on data security, business continuity management and fraud management;

(f) conduct periodic review on the configuration and rules settings for all security devices. Automated tools shall be used to review and monitor changes to the configuration and rules settings;

(g) perform regular vulnerability assessments and penetration tests on the infrastructure and technology ecosystem and ensure any material findings identified in such testing are rectified prior to operationalisation;

(h) implement a fraud detection system to monitor suspicious or fraudulent transactions; and

(i) implement an appropriate intruder detection and prevention system to monitor, detect and prevent any abnormal or suspicious network traffic within the PSO's internal network.

G 18.5 As part of effective management of sensitive data, the PSO may implement the following–

[20] From data input into real-time backup.

(a) conduct periodic review of privileged users[21] and the access rights given;
(b) ensure technology networks are segregated into multiple zones according to their risk profile;
(c) implement multi-layer network security and devices;
(d) implement end-to-end encryption for external communication;
(e) ensure protection of important data and information in use, in storage and in transit by adopting industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;
(f) establish proper controls to limit risk of potential data leakage;
(g) establish audit trail capabilities; and
(h) practise timely security patches for operating systems and application systems.

19 Cybersecurity

S 19.1 A PSO shall develop a CRF which articulates the PSO's governance for managing cyber risks, its cyber resilience objectives and risk tolerance, with due regard to the evolving cyber threat environment. Objectives of the CRF include ensuring operational resilience against extreme but plausible cyber-attacks.

G 19.2 As part of the CRF specified under paragraph 19.1 and in ensuring proper cybersecurity controls are in place, a PSO should undertake the following:
(a) actively manage software and hardware inventories and ensure updated records are adequately maintained;
(b) adopt an appropriate access control policy including explicitly verifying user access by adopting the principles of least privilege[22] and separation of duties for staff, outsourced service providers, as well as related parties in outsourcing arrangements and related counterparties;
(c) ensure critical systems, applications and data are backed up and protected from deliberate erasure or encryption;
(d) ensure micro segmentation of networks based on criticality and risk profile of assets;
(e) perform continuous and integrated security monitoring of IT infrastructure (network, systems and endpoints) including effective collection, analysis and retention of audit logs;
(f) adopt multi-factor authentication for all access;
(g) perform regular vulnerability assessment and rapid patching of critical vulnerabilities;

[21] Including outsourced service providers.
[22] This refers to having access on a 'need-to-have' basis where only the bare minimum permissions are granted to legitimate users so that they can effectively perform their roles.

(h) establish and periodically test incident response programs to prepare, detect and rapidly respond to cyber-attacks;
(i) periodically test the effectiveness and resiliency of IT systems and networks by adopting intelligence-led penetration testing;
(j) strengthen security configurations by minimising security misconfigurations and avoiding use of default security settings of software and hardware – include periodic security reviews and whenever material changes are made to IT systems/networks;
(k) implement the use of endpoint malware defence tools including rapid detection and response; and
(l) provide adequate and regular technology and cybersecurity awareness training programmes that reflect current cyber threats for all staff, including the board.

20 Business continuity management

S 20.1 A PSO shall ensure an effective and comprehensive BCP and DRP for all critical business functions to ensure continuity and timely recovery of operations in the event of contingencies.

G 20.2 In relation to paragraph 20.1, the PSO should ensure the following:
(a) detailed contingency plans are established for a variety of plausible scenarios [23] and fully operational back-up arrangements for critical communication and IT systems, crucial data and key personnel are in place;
(b) ensure the PSO, its participants, outsourced service providers and other relevant counterparties[24] have effective BCP and DRP which are regularly tested and cover appropriate test scenarios, to ensure their reliability and effectiveness of the recovery strategies and procedures; and
(c) the BCP and DRP are reviewed and updated on a regular basis to ensure its continued relevancy and effectiveness.

S 20.3 A PSO shall determine the MTD and RTO for all critical business functions.

S 20.4 A PSO shall conduct an independent assessment on the adequacy and effectiveness of its BCM framework, policies and procedures including the testing of BCP and DRP.

[23] For the avoidance of doubt, this should include extreme plausible scenarios such as all systems down.
[24] E.g. onshore settlement institution or cross-border links.

S 20.5 A PSO shall ensure adequate organisational understanding and training on BCM such that all levels of staff are well equipped to effectively perform their roles.

21 Outsourcing arrangement

S 21.1 A PSO shall remain responsible and accountable for any services performed by an outsourced service provider.

G 21.2 A PSO should conduct appropriate due diligence of the outsourced service provider, at the point of considering new service-level arrangements (SLA), and when renewing or renegotiating existing SLAs.

S 21.3 A PSO shall identify and have an in-depth understanding of potential risks[25] arising from the SLA. The scope and nature of services and operations to be performed by the outsourced service provider should not compromise the risk management and internal controls of the PSO.

S 21.4 In relation to the requirement specified in paragraph 21.3, the PSO shall ensure that the SLA are established in a manner which do not affect–

(a) the PSO's ability to effectively monitor the outsourced service provider and execute its BCP;

(b) the PSO's ability to promptly recover data in the event of the outsourced service provider's failure that would critically impact or disrupt the PSO's Malaysian operations, having due regard to the laws of the particular jurisdiction in the case where the outsourced service provider is located in a different jurisdiction from the PSO; and

(c) the Bank's ability to exercise its regulatory or supervisory powers, in particular the Bank's timely and unrestricted access to systems, information or documents from the PSO relating to the outsourced service provider arrangement in the event that such service would critically impact or disrupt the PSO's Malaysian operations.

G 21.5 A PSO should exercise effective oversight on the outsourced service provider, as would have been the case if they were performed in-house which includes the following–

(a) conduct regular review and monitoring of contracts and SLAs with the outsourced service provider to ensure the integrity and quality of work conducted by the outsourced service provider is maintained;

(b) ensure effective controls are in place to safeguard the confidentiality, integrity and availability of any information shared with the outsourced

[25] Including operational, financial and IT related risk.

service provider including proper escalation and resolution in handling disputes or complaints raised by the relevant stakeholders;

(c) ensure the storage of its data is at least logically segregated from the other clients of the outsourced service provider with appropriate controls and periodic review of user access;

(d) ensure data residing in the outsourced service provider are recoverable in a timely manner;

(e) ensure clearly defined arrangements with the outsourced service provider are in place to facilitate the PSO's immediate notification and timely update to the Bank and other relevant authorities in the event of a cyber-incident; and

(f) ensure proper communication procedures and processes are in place where the participants or related stakeholders clearly understand the roles and responsibilities of the outsourced service provider to enable them to adequately manage their risks related to using their services.

S 21.6 A PSO shall ensure any critical systems hosted by the outsourced service provider have strong recovery and resumption capabilities, and can facilitate an orderly exit in the event of failure or unsatisfactory performance by such provider.

S 21.7 A PSO shall have a contingency plan or arrangements to secure business continuity in the event the arrangement with the outsourced service provider is suddenly terminated or fails to provide necessary support[26]. The contingency plan shall be periodically reviewed to ensure that the plan is current and remains appropriate for timely implementation.

G 21.8 For outsourcing involving cloud services, the PSO may rely on third party certification and reports made available by the cloud service provider for the audit[27], provided such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and timely access to the third party and service provider to clarify matters relating to the audit.

22 Interlinkages

S 22.1 For the purposes of paragraphs 22.2 and 22.3, the requirements shall be applicable to a PSO that establishes a link arrangement with other counterparties[28].

[26] Including insolvency or lack of resources issue.

[27] For the avoidance of doubt, such certifications or reports should not substitute the PSO's right to conduct on-site inspections where necessary.

[28] E.g. Cross-border links with another payment system, either directly or through intermediaries.

S 22.2 A PSO shall conduct appropriate due diligence and assessment on the potential risks that could arise from the link arrangement prior to entering into an arrangement with other counterparties. This shall include the risks associated with the different legal requirements in the case where the counterparties are located in different jurisdictions from the PSO.

S 22.3 A PSO shall ensure that its agreement with the counterparties clearly indicates the rights and responsibilities of each party, which at minimum, shall include the following–

(a) safeguarding the confidentiality, integrity and availability of any information shared;
(b) ensure appropriate controls for all established interlinkages to external systems;
(c) ensure appropriate controls are in place to ensure the reliability, efficiency and smooth operation of the interlinkages system with minimal disruption and to achieve system and service high availability;
(d) proper escalation and resolution in handling disputes or complaints raised by the relevant stakeholders;
(e) ensure any enhancements or changes associated with the link arrangements do not pose significant operational risk to the other counterparties; and
(f) ensure clearly defined arrangements with the counterparties are in place to facilitate the PSO's ability to immediately notify and provide timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.

23 Recovery and orderly exit

S 23.1 A PSO shall continuously identify plausible scenarios that may prevent its ability to provide its critical operations and services as a going concern or in the event a PSO exits[29] the market and assess the effectiveness of options for recovery or orderly exit under these scenarios.

S 23.2 A PSO shall establish appropriate plans for its recovery or orderly exit, including its communication strategy with the Bank and other relevant stakeholders to mitigate any unintended consequences. The plans shall be periodically reviewed and updated, where necessary, to ensure it remains relevant.

[29] A PSO may exit the market either by (i) revocation of approval to operate in Malaysia by the Bank; or (ii) voluntary exit of a PSO from the market.

24 Access and participation

S 24.1 A PSO shall establish fair and open access criteria for participants of its payment system that are objective, transparent and risk-based to commensurate with the risk profile of the participants.

G 24.2 For purposes of paragraph 24.1, the PSO may set reasonable risk-related participation requirements to mitigate potential risks posed by the participants to the payment system.

S 24.3 For tiered-participation arrangements, the PSO shall ensure the following:

(a) establish rules, procedures and arrangements with the direct participants to enable the PSO to obtain information on indirect participants for the purpose of risk identification and monitoring;

(b) identify the significant dependencies between direct and indirect participants that may adversely affect[30] the PSO; and

(c) regularly review the risks associated with the tiered-participation arrangements and institute appropriate mitigating measures.

S 24.4 A PSO shall put in place measures to monitor the compliance of its participants with the participation requirements on an ongoing basis.

S 24.5 A PSO shall clearly outline and disclose the procedures on the suspension or orderly exit of a participant in the event its participant has breached or is no longer able to meet the participation requirements.

25 Efficiency

S 25.1 A PSO shall ensure the payment system offered meets the needs of its participants and the market it serves, with respect to, among others, clearing and settlement arrangements, operating structure[31], and the use of technology and communication procedures.

G 25.2 In meeting the requirement specified in paragraph 25.1, the PSO is advised to consider relevant factors such as the practicality and cost structure for its participants and other relevant stakeholders.

G 25.3 In addition to paragraph 25.2, a PSO is encouraged to put in place a mechanism to facilitate continuous engagement with its participants and other relevant

[30] For example, exposures that could arise from credit risk and liquidity risk.

[31] For example, where the PSO is involved in cross-border links or outsourced arrangements with service providers.

stakeholders to receive feedback such that the PSO continues to meet the needs of its participants and the market.

S 25.4 For the purposes of paragraph 25.1, a PSO shall establish a clearly defined, measurable and achievable efficiency objective[32] to ensure it remains effective in the manner that the PSO operates.

S 25.5 A PSO shall regularly review the progress against its targeted objectives to ensure the efficiency and effectiveness of its payment system.

26 Transparency

S 26.1 A PSO shall ensure that the established rules and procedures for its participants are clear, comprehensive, up-to-date and fully disclosed to its participants.

S 26.2 A PSO shall ensure the processes for proposing and implementing changes to its rules and procedures as well as the communication of these changes to its participants and relevant authorities are clear and fully disclosed.

G 26.3 A PSO is encouraged to provide participants with all relevant documentation, training and information, including the risks that participants may face from participating in the payment system to facilitate their understanding on the rules and procedures.

S 26.4 A PSO shall disclose its fees and relevant information to its participants, including prospective participants, to allow participants to assess the total cost of participating in the payment system and/or the services offered by the PSO.

S 26.5 A PSO shall ensure that it provides sufficient advance notice to its participants of any changes to the fees made.

[32] For example, in the areas of minimum service level targets, risk management expectations and business priorities.