BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Payment System Operator
Exposure Draft

Applicable to−
1 Approved operators of payment systems

Issued on: 15 December 2021 BNM/RH/ED 029-23

This exposure draft sets out Bank Negara Malaysia (the Bank)'s proposed requirements and guidance for payment systems' operators that have been approved under section 11 of the Financial Services Act 2013 or the Islamic Financial Services Act 2013.

The Bank invites written feedback on the proposals in this exposure draft, including suggestions on areas to be clarified or elaborated and any alternative proposals that the Bank should consider. The written feedback should be supported with clear rationale, accompanying with evidence or illustrations as appropriate, to facilitate the Bank's assessment.

Responses must be submitted to the Bank by **31 March 2022** to –

Pengarah
Jabatan Dasar Perkhidmatan Pembayaran
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: paymentpolicy@bnm.gov.my

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

In the course of providing your feedback, you may direct any queries to the following officers at 03-26988044 –

1. Safiyyah Mohsin (ext. 7805 or e-mail: safiyyah@bnm.gov.my)
2. Syafiqa Shamsul (ext. 8969 or e-mail: syafiqa@bnm.gov.my)
3. Puteri Aemelia Sophia (ext. 8338 or e-mail: aemeliasophia@bnm.gov.my)

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 An approved operator of a payment system (PSO) performs the roles of processing, clearing and settlement of payment transactions. It facilitates public and private entities, as well as consumers to transfer funds to one another.

1.2 A well-functioning payment system is crucial for the efficient operation of the financial market as well as to support the economy. Disruption could potentially lead to a systemic or system-wide impact to the financial system. Therefore, the safety and efficiency of payment systems are 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 by the Bank for International Settlements (BIS).

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 upon issuance of the final policy document.

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" or "PSO" means 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" means Bank Negara Malaysia;

"Board" means the Board of Directors of 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 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 operations of business functions 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 procedures, processes, systems and resources necessary to resume and restore the business functions 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

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

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 function" refers to operations, activities, or processes undertaken by a PSO, where failure or discontinuances is likely to –
(a) critically impact the PSO financially or non-financially; and
(b) disrupt the provision of essential services to the public;

"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;

"direct participant" refers to a participant that has access to a PSO's payment, clearing or settlement facilities. A direct participant is bound to the rules and procedures established by the PSO;

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

"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 during 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 be bound to 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;

"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];

"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 to be recovered and operationally ready to support critical business functions after a disruption. A recovery time objective has 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 operation.

"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

[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.

[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.

"tiered-participation arrangement" refers to an arrangement where indirect participant rely 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) Fit and Proper Criteria for Approved Person;
(b) Guidelines on Business Continuity Management (Revised);
(c) Interoperable Credit Transfer Framework;
(d) Management of Customer Information and Permitted Disclosures;
(e) Operational Risk Reporting (ORR);
(f) Payment Card Reform Framework; and
(g) Risk Management in Technology (RMiT).

[5] For the avoidance of doubt, where relevant, a PSO shall comply with the requirements of a policy document and any subsequent document issued thereafter which are more stringent.

PART B GOVERNANCE

7 Governance arrangement

S 7.1 A PSO shall establish adequate governance arrangements which are clear and transparent. To ensure resilient and efficient operations of the payment systems that support the stability of the broader financial system and other relevant public interest considerations, the governance arrangement should include, among others, the following –

(a) a Board of Directors (the Board) and senior management that consists 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 control arrangements to promote good corporate culture that reinforces ethical, prudent and professional behaviour, as well as reduce the chances of mismanagement and fraud.

8 Board of directors

S 8.1 The Board must have a board charter that sets out the mandate, responsibilities and procedures of the Board and its committees (if any), including the matters reserved for the Board's decision.

G 8.2 Board committees 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 8.3 The Board shall have the overall responsibility for promoting the safety, efficiency and reliability of the payment system which include –

(a) approving 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 overseeing the risk management function and material risk decisions, which include ensuring risk management policies, processes and infrastructure, and effective operationalisation of the risk controls to manage the various types of risks, are in place and effective;

(e) ensuring the independence and effectiveness of internal control functions;

(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, reliability and efficiency of the PSO; and
(h) ensuring compliance with supervisory and oversight requirements.

S 8.4 The Board shall be composed of suitable members with appropriate mix of skills, experience and knowledge of the PSO.

S 8.5 The Board shall include non-executive directors, including independent directors.

S 8.6 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.

9 Senior management

S 9.1 The senior management shall be responsible for ensuring the following –
(a) establish and implement effective policies and procedures, among others, in the following areas –
(i) risk management and appropriate controls to manage and monitor risks;
(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;
(b) implement business and risk strategies and other strategic plans, such as technology plan and the associated technology policies and procedures, in accordance with the direction given by the Board; and
(c) conduct a robust assessment on any deviation [6] from policies and procedures. Material deviations shall be reported to the Board.

S 9.2 The senior management shall consist of individuals with the appropriate skill set and experience to adequately support the operation and risk management of the PSO. This includes individuals with technology background to provide guidance on the PSO's technology plans and operations.

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

S 9.3 For the purpose of paragraph 9.2, a PSO shall ensure that a designated staff who does not engage in day-to-day technology operations shall be responsible for the identification, assessment and mitigation of technology risks.

10 Control functions

G 10.1 The Board and senior management should create an environment which:

(a) ensures the PSO and its officers comply with legal and regulatory requirements;

(b) adopt relevant risk management practices; and

(c) encourages ethical conduct that underlies such requirements.

S 10.2 The Board is responsible for the effectiveness of a PSO's control functions. The Board shall –

(d) ensure clear, documented and effective risk management framework that is appropriate to the nature, scale and complexity of its activities is in place;

(e) ensure the establishment of control functions and the position of the relevant officers, and ensure that the said functions and officers are provided with appropriate standing, authority and independence;

(f) ensure the appointment of officers who have adequate working knowledge in payment system business and the legal and regulatory framework, and can effectively support the PSO's internal control framework;

(g) provide the relevant officers with direct and unimpeded access to the Board; and

(h) ensure the PSO's risk profile is consistent with the business strategy and risk appetite.

S 10.3 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 risk appetite statement. In doing so, the Board shall approve the corresponding risk tolerances 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 the 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 and oversee the adequacy of the PSO's information technology (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 resources. The plans shall be commensurate with the complexity of the PSO's operations, changes

in the risk profile and business environment and shall be periodically reviewed.

G 10.4 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 cyber-incident. This should be supported by input from external experts where relevant. The Board should also ensure its continuous engagement in cybersecurity preparedness, education and training.

S 10.5 The senior management is collectively 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 10.6 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 10.7 A PSO shall organise its control function in a manner that allows compliance and risk management to be managed effectively, taking into account the size, nature of operations and complexity of the PSO's business.

S 10.8 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 10.9 The compliance function shall identify and assess the compliance risk associated with the PSO's activities. The compliance officer must 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 regulatory authorities upon request.

S 10.10 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.

11 Fit and proper

S 11.1 A PSO shall ensure its directors and CEO are persons with calibre, integrity, and fulfil the fit and proper criteria as stipulated in the policy document on Fit and Proper Criteria for Approved Person issued on 24 December 2018 and any subsequent review on such policy document.

[The remainder of this page is intentionally left blank]

PART C RISK MANAGEMENT AND OPERATIONAL REQUIREMENTS

12 Risk management framework

S 12.1 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[7] as a result of interdependencies.

S 12.2 In establishing the risk management framework, the PSO shall –

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

(b) assign responsibilities and accountability for risk decisions; and

(c) address efficient decision making in crises.

S 12.3 The framework shall be periodically reviewed for continued effectiveness and be supported by a robust management information system that facilitates the timely and reliable reporting of risks.

S 12.4 A PSO shall establish risk monitoring and reporting requirements, which include periodic reporting to board and senior management on the assessment of the 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 regulatory authorities upon request.

13 Business risk

S 13.1 A PSO shall establish robust management and control systems to identify, monitor and manage its business risk and hold adequate capital and liquid net assets[8] which are commensurate with its business risk profile and is sufficient to support its operations as a going concern under normal or stress scenarios.

G 13.2 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 13.3 A PSO shall, at a minimum, maintain liquid net assets equal to at least six months of current operating expenses.

[7] This may include other PSO, settlement banks, liquidity providers, and service providers.

[8] For avoidance of doubt, liquid net assets are derived from assets which can be easily and immediately converted into cash at little or no loss of value, less current liabilities.

G 13.4 In determining the appropriate threshold of liquid net assets, a PSO should consider its general business risk profile and the length of time required for a recovery or orderly wind-down that is appropriate to the critical business function of the PSO in the event such action is taken.

14 Liquidity risk

S 14.1 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 14.2 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 stress scenarios.

G 14.3 In determining the type, amount and assessing the sufficiency of liquid resources, as well as the adequacy of its liquidity risk management framework, a PSO should regularly conduct stress testing which considers a range of relevant scenarios. Results should be reported to the board and senior management to facilitate effective decision making on timely basis.

G 14.4 A PSO may, as appropriate, conduct reverse stress testing[9] or simulations to identify scenarios or conditions, which may include extreme default scenarios and/or extreme market conditions, in which a PSO's liquid resources would be insufficient. The results may be used by a PSO, among others, to inform and validate its risk mitigation plans and prepare for these severe conditions.

S 14.5 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.

15 Credit risk

S 15.1 A PSO shall establish a credit risk management framework to effectively measure, monitor and manage its credit exposures to participants and other relevant parties from its payment, clearing and settlement processes as well as maintain sufficient financial resources to cover its credit exposure to each participant.

[9] For avoidance of doubt, reverse stress testing commences from a known adverse outcome and deduces the possible different forward-looking scenarios that could lead to such an outcome materialising for a PSO.

G 15.2 A PSO may, as appropriate, establish adequate processes to effectively manage its credit concentration risks, including establishment of exposure limits where the potential losses can jeopardise the solvency of, or public confidence in, the PSO.

G 15.3 In determining the amount and assessing the sufficiency of financial resources, a PSO should regularly conduct stress testing which considers a range of relevant scenarios. Results should be reported to the board and senior management to facilitate effective decision making on timely basis.

G 15.4 A PSO may, as appropriate, 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 risk. The results may be used by a PSO, among others, to inform and validate its risk mitigation plans and to prepare for these severe conditions.

S 15.5 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 15.6 A PSO shall establish appropriate collateral management practices which includes processes and procedures to support robust and reliable valuation, adequate monitoring of collateral's condition and timely liquidation.

G 15.7 For purposes of paragraph 15.6, a PSO may, as appropriate –

(a) establish concentration limits for holdings of certain collateral as part of its collateral management practices, such as for collateral with value which is likely to be volatile; and

(b) regularly mark collateral to market and develop haircuts that are regularly tested, taking into account stressed market conditions to ensure adequate assurance of the collateral's value in the event of liquidation.

G 15.8 A PSO should be supported with a robust collateral management system to facilitate ongoing monitoring and management of collateral.

16 Operational risk

S 16.1 A PSO shall establish a robust management and control systems to identify, measure, monitor and manage its sources of operational risk.

S 16.2 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 on timely basis.

S 16.3 A PSO shall ensure sufficient resources with appropriate competencies and experience are employed to operate its systems safely and efficiently during normal and stressed periods.

System and service availability

S 16.4 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 system and service high availability.

S 16.5 For purposes of paragraph 16.4, the PSO shall define the service level objectives and set minimum service-level targets for the operation of the payment system.

S 16.6 A PSO shall ensure that the payment system have adequate capability and capacity to process and manage stressed scenarios[10] at all times.

S 16.7 A PSO shall regularly monitor and test the actual capacity and performance of the payment system, as well as, plan for changes in volumes or business pattern. The PSO shall also regularly conduct stress tests to verify whether the payment system can handle abnormally huge volume of transaction under extreme circumstances.

G 16.8 In conducting the stress testing as specified under the paragraph 16.7, 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) participant's 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 its relevancy and effectiveness.

17 Technology risk and information security

S 17.1 A PSO shall establish the 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.

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

S 17.2 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[11] and retention of all information including sensitive data.

S 17.3 In relation to paragraph 17.2, the PSO shall also ensure their relevant stakeholders put in place appropriate controls in safeguarding the confidentiality, integrity and availability of sensitive data.

G 17.4 In ensuring the confidentiality, integrity and availability of information held within the system, the PSO should ensure the following –

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

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

(c) ensure that the information contained in the system are not disclosed or accessible to any unauthorised 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 proper mitigation measures where the scope of the assessment should include but 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 assessment and penetration test on the infrastructure and technology ecosystem and ensure any material findings identified in such testing are rectified prior operationalisation;

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

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

G 17.5 As part of effective management of sensitive data, the PSO may implement the following –

(a) conduct periodic review of privileged users[12] and the access rights given;

(b) ensure technology networks are segregated into multiple zones according to risk profile;

[11] From data input into real-time backup.
[12] Including outsourced service providers.

(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 ensure no data leakage occurs;
(g) establish audit trail capabilities; and
(h) practise timely security patches for operating systems and application systems.

18 Cybersecurity

S 18.1 A PSO shall also 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 includes ensuring operational resilience against extreme but plausible cyber-attacks.

G 18.2 As part of the CRF specified under paragraph 18.1 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 appropriate access control policy including explicitly verifying user access by adopting the principles of least privilege and separation of duties for staff, outsourced service providers, as well as related parties in outsourcing arrangements and related connected 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 profiles 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 management and rapid patching of critical vulnerabilities;
(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 avoid 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 education that reflects the current cyber threat landscape for all staff.

19 Business continuity management

S 19.1 A PSO shall ensure an effective and comprehensive BCP and DRP for all the critical business functions to ensure continuity and timely recovery of operations in the event of contingencies.

G 19.2 In relation to paragraph 19.1, the PSO should ensure the following:

(a) detailed contingency plans are established for a variety of plausible scenarios [13] 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 [14] to have effective BCP and DRP which are sufficiently/regularly tested and covering 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 relevancy and effectiveness.

S 19.3 A PSO shall determine the maximum tolerable downtime (MTD) and recovery time objectives (RTO) for all critical business functions.

S 19.4 A PSO shall conduct an independent assessment on the adequacy and effectiveness of its BCM framework, policies and procedures including testing of BCP and DRP.

S 19.5 A PSO shall ensure adequate organisational understanding and training on BCM such that all levels of staff are well trained to perform their roles.

20 Outsourcing arrangement

S 20.1 A PSO shall remain responsible and accountable for any services performed by an outsourced service provider.

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

G 20.2 A PSO should conduct appropriate due diligence of the outsourced service provider, at the point of considering new service-level arrangement (SLA), and renewing or renegotiating existing SLA.

S 20.3 A PSO shall identify and have in-depth understanding of potential risks[15] arising from the SLA. The scope and nature of services and operations to be performed by the outsourced service provider should not compromise the controls and risk management of the PSO's system.

S 20.4 In relation to the requirement specified in paragraph 20.3, the PSO shall ensure that the SLA are conducted in a manner which does not affect –

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

(b) the PSO's prompt recovery of data in the event of the outsourced service provider's failure, having regard to the laws of the particular jurisdictions 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 relating to the outsourced service provider arrangement.

G 20.5 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 SLA with the outsourced service provider to ensure the integrity and quality of work conducted by the outsourced service provider is maintained;

(b) ensure controls are in place and effective in safeguarding the confidentiality, integrity and availability of any information shared with the outsourced 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 period review of the 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 updates to the Bank and other relevant regulatory bodies in the event of cyber-incident; and

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

(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 in using the services.

S 20.6 A PSO shall ensure any critical system hosted by the outsourced service provider have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by such provider.

S 20.7 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[16]. The contingency plan shall be reviewed from time to time to ensure that the plan is current and ready for implementation.

G 20.8 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[17], provided such reliance is supported by an adequate understanding and review of the scope of the audits and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit.

21 Interlinkages

S 21.1 For the purposes of paragraphs 21.2 and 21.3, the requirements shall be applicable to a PSO that establishes a link arrangement with other counterparties[18].

S 21.2 A PSO shall conduct appropriate due diligence and assessment on the potential risk that could arise from the link arrangement prior to entering into an arrangement with other counterparties. This shall include the risk associated to the different legal requirements in the case where the counterparties are located in different jurisdictions from the PSO.

S 21.3 A PSO shall ensure that its agreement with the counterparties clearly indicates the right and responsibilities of each party, which at minimum, shall include the following –

(a) safeguarding the confidentiality, integrity and availability of any information shared;

[16] Including insolvency or resource issue.
[17] For avoidance of doubt, such certifications or reports should not substitute the PSO's right to conduct on-site inspections where necessary.
[18] E.g. Cross-border links with another PSO.

(b) ensure proper controls for all established interlinkages to external systems;
(c) 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 enhancement or changes associated with the link arrangements does 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 immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of cyber-incident.

22 Recovery and orderly wind-down

S 22.1 A PSO shall continuously identify plausible scenarios that may prevent its ability to provide its critical operations and services as a going concern and assess the effectiveness of options for recovery or orderly wind-down under these scenarios.

S 22.2 A PSO shall establish appropriate plans for its recovery or orderly wind-down, including its communication strategy with the Bank and other relevant stakeholders to mitigate any unintended consequences. The plans shall be reviewed and updated, where necessary, to ensure it remains relevant.

[The remainder of this page is intentionally left blank]

PART D OTHER POLICY REQUIREMENTS

23 Access and participation

S 23.1 A PSO shall establish fair and open access criteria to its payment system that are objective, transparent and risk-based to commensurate the risk profile of the participants.

G 23.2 For purposes of paragraph 23.1, the PSO may set reasonable risk-related participation requirements to mitigate potential risks posed by the participants to the payment system.

S 23.3 For tiered-participation arrangement, the PSO shall ensure the following:

(a) establish rules, procedures and arrangement with the direct participants to enable 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[19] the PSO; and

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

S 23.4 A PSO shall put in place measures to monitor the compliance of its participants with the participation requirements on an ongoing basis.

S 23.5 A PSO shall clearly outline and disclose the procedures on the suspension or orderly exit of a participant in the event its participant has breach or is no longer able to meet the participation requirements.

24 Efficiency

S 24.1 A PSO shall ensure the payment system offered meets the needs of its participants and the market it serves, in respect to, among others, the clearing and settlement arrangement, operating structure[20], and the use of technology and communication procedure.

G 24.2 In meeting the requirement specified in paragraph 24.1, the PSO is advised to consider relevant factors such as the practicality and cost structure for its participants and other relevant stakeholders.

[19] For example, exposure that could arise from credit and liquidity risk.

[20] For example, where the PSO involved in a cross-border links or outsourced arrangement with service providers.

G 24.3 In addition to paragraph 24.2, A PSO is encouraged to put in place a mechanism to facilitate continuous feedback from its participants and other relevant stakeholders in ensuring it meets the needs of its participants and the market.

S 24.4 A PSO shall establish a clearly defined, measurable and achievable objective to ensure it remains effective in the manner that the PSO is operated and the resources required to perform its functions.

S 24.5 A PSO shall regularly review the progress against its targeted objectives to ensure the efficiency and effectiveness of its payment system.

25 Transparency

S 25.1 A PSO shall ensure rules and procedures established are clear, comprehensive, up-to-date and fully disclosed to its participants.

S 25.2 A PSO shall ensure the processes for proposing and implementing changes to its rules and procedures as well as communication of these changes to its participants and relevant authorities are clear and fully disclosed.

G 25.3 A PSO is encouraged to provide participants with the relevant documentation, training and information, including the risks participants may face from participating in the payment system to facilitate their understanding on the rules and procedures.

S 25.4 A PSO shall publicly disclose its fees and relevant information that would allow participants to assess the total cost of participating in the payment system and/or the services offered by the PSO.

S 25.5 A PSO shall ensure that it provides a timeline notice to its participants of any changes to the fees made.

26 Submission requirements

S 26.1 The following information shall be made available to the Bank upon request –

(a) incident reports;
(b) system and service availability reports;
(c) audit reports;
(d) annual audited financial statements; and
(e) other information as required by the Bank.

[End of exposure draft]

Issued on: 15 December 2021