BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Electronic Money (E-Money)

Exposure Draft

Applicable to: Approved issuers of e-money

Issued on: 11 June 2021

BNM/RH/ED 029-20

This exposure draft sets out Bank Negara Malaysia (the Bank)'s proposed requirements and guidance for issuers of electronic money (e-money) approved pursuant to section 11 of the Financial Services Act 2013 (FSA) or the Islamic Financial Services Act 2013 (IFSA).

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

Responses must be submitted to the Bank by **31 July 2021** to–

Pengarah
Jabatan Pemantauan 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. Nor Azlina Abdul Wahid (ext. 8036 or e-mail: norazlina@bnm.gov.my)
2. Ira Zalis Ismail (ext. 8226 or e-mail: irazalis@bnm.gov.my)
3. Mohd Idham Harith Suhaimi (ext. 8159 or e-mail: idhamharith@bnm.gov.my)

Issued on: 11 June 2021

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 E-money is a payment instrument that stores monetary value that is paid in advance by the user to the issuer of e-money (EMI). E-money can be used to make payments for purchases of goods and services to merchants who accept e-money as a mode of payment. E-money users may also send or receive funds to or from another user's e-money or bank account, respectively, through person-to-person (P2P) fund transfer service if the EMI enables such service.

1.2 Over the past decade, e-money has evolved and grown significantly due to the proliferation of mobile technology such as Quick Response (QR) codes and mobile applications (apps), digitalization of financial services and shift in consumer behaviour. For example, the use of e-money for payments has steadily recorded a double-digit growth for the past five years and the form of e-money has progressed from the traditional stored value cards to network-based solutions such as online accounts or e-wallets.

1.3 E-money represents 33% of total electronic payments (e-payments) in Malaysia, with 131% increase in e-wallet[1] transactions to RM0.6 billion in 2020 as compared to RM0.3 billion in 2019. For the past five years, e-money liabilities have also grown significantly from RM0.5 billion to RM1.6 billion. Therefore, given the growing prominence of e-money in the e-payments landscape, enhancements to the e-money regulatory framework are needed to ensure e-money continues to be a safe and reliable payment instrument amidst the increase in functionalities and evolvement in the enabling technology. It is important to ensure the safety of the e-money funds/float[2] and the soundness of the EMIs in order to mitigate potential risk of loss to customers, as well as, to foster public confidence in the use of e-money.

1.4 This policy document outlines requirements aimed to–
(a) ensure the safety and reliability of e-money issued by EMIs; and
(b) preserve customers' and merchants' confidence in using or accepting e-money for the payment of goods and services.

2 Applicability

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

[1] Network-based e-money.
[2] Referring to the funds collected by an EMI from their customers, which is also known as outstanding e-money liabilities.

2.2 This policy document is not applicable to issuer of limited purpose e-money as defined in paragraph 5.2 and subject to the said issuer fulfilling the conditions specified in Appendix 2.

2.3 The following requirements are only applicable to eligible EMIs as defined in paragraph 5.2–

(a) paragraph 9.12, 9.17, 9.18 to 9.21, 10.2 and 10.7 on governance arrangement; and

(b) paragraph 15.1(b) on minimum capital funds.

3 Legal provisions

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

(a) sections 47(1), 123(1) and 143 of the FSA; and

(b) sections 29(2), 57(1), 135(1) and 155 of the 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, IFSA or Development Financial Institutions Act 2002 (DFIA), as the case may be, unless otherwise defined in this policy document.

5.2 For the purpose of this policy document–

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

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

"**active politician**" refers to an individual who is a member of any national or state legislative body, or who is an office bearer of, or holds any similar office or position in a political party;

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

"Bank" refers to Bank Negara Malaysia;

"**banking institution**" refers to a licensed bank as defined under the FSA, a licensed Islamic bank as defined under the IFSA, and a development financial institution prescribed under the DFIA;

"**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 an EMI'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;

"credit transfer" refers to a payment service which allows a payer to instruct the institution with which the payer's bank account or e-money account is held to transfer funds to a beneficiary in another bank account or e-money account, irrespective of any underlying obligation between the payer and the beneficiary. For the avoidance of doubt, any reference to "credit transfer" in this policy document shall include a reference to both a fund transfer transaction and a purchase transaction regardless of the technology used to facilitate the transaction including Quick Response (QR) code;

"critical system" refers to any application system that supports the provision of EMI services, where failure of the system has the potential to significantly impair the EMI's provision of financial services to customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements;

"cross-selling" refers to an act of an EMI offering to its customers either complementary or related financial products or services. This may include an EMI acting as an agent to provide the financial products or services;

"customer or user" refers to any person to whom the e-money has been issued or any person who uses the e-money to make payments or any other transactions allowed by the EMI;

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

"customer information" refers to any information relating to the affairs or, in particular, the account, of any particular customer of the EMI in whatever form including in the form of a record, book, register, correspondence, other document or material;

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

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

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

"electronic money (e-money)" refers to any payment instrument, whether tangible or intangible, that–

(a) stores funds electronically in exchange of funds paid to the issuer; and
(b) is able to be used as a means of making payment to any person other than the issuer;

"eligible EMI" refers to an approved EMI with substantial market presence based on the criteria set out in accordance with Appendix 1 or such other criteria as may be specified by the Bank from time to time;

"executive director" refers to a director of an approved EMI who has management responsibilities in the EMI;

"Financial Ombudsman Scheme (FOS)" refers to a scheme that functions as an alternative dispute resolution channel to resolve disputes between financial institutions and consumers. The Ombudsman for Financial Services (OFS) is the operator of the FOS approved by the Bank pursuant to section 126(2) and section 138(2) of the FSA and IFSA, respectively;

"internal control framework" refers to the set of rules and controls governing an EMI's organisational and operational structure, including reporting processes and control functions;

"issuer of e-money (EMI)" refers to a person approved under section 11 of the FSA or IFSA to issue e-money;

"issuer of limited purpose e-money (limited purpose EMI)" refers to an EMI that satisfies the definition and conditions of limited purpose e-money set out under Appendix 2 and qualifies to be exempted from requiring approval from the Bank under section 11 of the FSA or IFSA and the relevant legal provisions and standards applicable to EMIs that are approved under the FSA or IFSA;

"licensed bank" refers to any person licensed under section 10 of the FSA to carry on banking business;

"licensed Islamic bank" refers to a person licensed under section 10 of the IFSA to carry on Islamic banking business and includes a licensed international Islamic bank;

"material outsourcing arrangement[3]" refers to an outsourcing arrangement which–

(a) in the event of a service failure or security breach, has the potential to significantly impact the EMI's provision of financial services to customers, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements; or

(b) involves customer information and in the event of unauthorised access, disclosure or modification, or loss or theft of the information, has a material impact on the customer or the EMI;

"merchant" refers to a person or an entity that accepts e-money for the sale of goods or services;

"non-bank EMI" refers to an approved EMI who is not a licensed person under the FSA or IFSA, or a prescribed institution under the DFIA;

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

"outsourcing arrangement" refers to an arrangement in which a service provider performs an activity on behalf of the EMI on a continuing basis[4], where the activity would otherwise be undertaken by the EMI and does not include activities set out in Appendix 5;

[3] For the avoidance of doubt, any arrangement involving internal control functions (i.e. risk management, internal audit and compliance) and customer funds management would generally be considered as a material outsourcing arrangement.

[4] 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.

"outstanding e-money liabilities" refers to the amount of e-money yet to be utilised by customers and the utilised amount of e-money which is pending payment to merchants;

"payment instrument" refers to any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services or to make any payment;

"production data centre" refers to any facility which hosts active critical production application systems irrespective of location;

"purchase transaction" refers to any transaction between a customer and a merchant for the purchase of goods and services;

"registered merchant acquirer" refers to any person who has been registered by the Bank pursuant to sections 17(1) and 18(1) of the FSA to provide merchant acquiring services;

"senior management" refers to the CEO and senior officers;

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

"service provider" refers to an entity, including an affiliate, providing services to an EMI under an outsourcing arrangement;

"shareholder" refers to a person that holds an aggregate interest of 5% or more in the shares of an EMI[5];

"Shariah compliant e-money" refers to a designated Islamic payment instrument that is structured based on appropriate Shariah contracts, whether tangible or intangible, that–

(a) stores funds electronically in exchange of funds paid to the issuer; and
(b) is able to be used as a means of making payment to any person other than the issuer;

"standard EMI" refers to an EMI that does not satisfy the criteria set out for eligible EMIs in Appendix 1;

[5] Interest in shares shall be construed as set out in subsection 2(1) and Schedule 3 of the FSA or IFSA.

"sub-contractor" refers to any entity, including an affiliate, which performs the whole or a part of the outsourced activity for the primary service provider;

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

"wallet limit" refers to the maximum monetary value that can be stored in an e-money at any one time; and

"white labelling" refers to an arrangement between an EMI and a partner or other entity to allow such partner or entity to offer e-money to their customers under their own brand, while the ultimate responsibility remains with the EMI in managing the e-money funds and operations.

Question 1:
Under this exposure draft, an EMI will be categorised into two new categories, i.e. standard and eligible EMI. With the new categorisation, there will be additional requirements imposed on eligible EMIs, which commensurate with their market share, size and complexity. Please provide your views on the new categories, the category criteria in Appendix 1 and the impact of such categorisation to your institution, if any.

6 Related legal instruments and policy documents

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

(a) Anti-Money Laundering, Counter Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) dated 31 December 2019;
(b) Complaints Handling dated 17 December 2009;
(c) Fair Treatment of Financial Consumers dated 6 November 2019;
(d) Fit and Proper Criteria for Approved Person dated 24 December 2018;
(e) Product Transparency and Disclosure dated 31 May 2013;

(f) Management of Customer Information and Permitted Disclosures dated 17 October 2017;
(g) Interoperable Credit Transfer Framework dated 23 December 2019;
(h) Merchant Acquiring Exposure Draft dated 17 July 2020;
(i) Risk-Based Authentication for Online Payment Card Transaction dated 4 November 2020;
(j) Payment Card Reform Framework dated 23 December 2014;
(k) Risk Management in Technology (RMiT) dated 19 June 2020
(l) Electronic Know-Your-Customer (e-KYC) dated 30 June 2020;
(m) Operational Risk Integrated Online Network (ORION) dated 25 February 2021;
(n) Wakalah dated 24 June 2016;
(o) Wadi'ah dated 3 August 2016;
(p) Qard dated 26 February 2018; and
(q) Shariah Advisory Council of Bank Negara Malaysia (SAC) Ruling on E-Money as a Shariah Compliant Payment Instrument

7 Policy documents superseded

7.1 This policy document supersedes the following–

(a) Guideline on Electronic Money (E-money) issued on 31 July 2008; and
(b) Paragraphs 11.2 (for non-bank EMIs only) and 12 of the policy document on Interoperable Credit Transfer Framework issued on 23 December 2019.

PART B GOVERNANCE

8 Governance arrangement

S 8.1 An EMI shall establish adequate governance arrangements, which are effective and transparent, to ensure the continued integrity of its e-money scheme, which include, among others, the following–

(a) a board of directors (the board) and senior management that consists of people with calibre, credibility and integrity.

(b) clearly defined and documented organisational arrangements, such as ownership and management structure.

(c) segregation of duties and internal control arrangements to reduce the chances of mismanagement and fraud.

9 Board of directors

G 9.1 The board responsibilities outlined in this policy document should be read together with section 56 of the FSA and section 65 of the IFSA.

S 9.2 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.

S 9.3 The board has the overall responsibility for promoting the sustainable growth and financial soundness of an EMI, and for ensuring reasonable standards of fair dealing, without undue influence from any party. This includes a consideration of the long-term implications of the board's decisions on the EMI and its customers, officers and the general public. In fulfilling this role, the board must–

(a) approve the risk appetite, business plans and other initiatives which would, singularly or cumulatively, have a material impact on the EMI's risk profile[6];

(b) oversee the selection, performance, remuneration and succession plans of the CEO, control function heads and other members of senior management, such that the board is satisfied with the collective competence of senior management to effectively lead the operations of the EMI;

(c) oversee the implementation of the EMI's governance framework and internal control policies, and periodically review whether these remain

[6] This would include initiatives, which affect the financial soundness, reputation or key operational controls of the EMI.

appropriate in light of material changes to the size, nature and complexity of the EMI operations;

(d) promote, together with senior management, a sound corporate culture within the EMI, which reinforces ethical, prudent and professional conduct and behaviour;

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

(f) promote timely and effective communication between the EMI and the Bank on matters affecting or that may affect the safety and soundness of the EMI.

S 9.4 The chairman, in leading the board, is responsible for the effective overall functioning of the board. In fulfilling this role, the chairman must–

(a) ensure that appropriate procedures are in place to govern the board's operations;

(b) ensure that decisions are taken on a sound and well-informed basis, including by ensuring that all strategic and critical issues are considered by the board, and that directors receive the relevant information in a timely manner;

(c) encourage healthy discussion and ensure that dissenting views can be freely expressed and discussed; and

(d) lead efforts to address the board's developmental needs.

S 9.5 For the board of an EMI that issues Shariah compliant e-money, the overall responsibility outlined in paragraph 9.3 includes the responsibility to promote Shariah compliance in accordance with requirements set out under paragraph 12 and ensure its integration with the EMI business and risk strategies.

Board appointments

S 9.6 A director must fulfil the minimum requirements set out in paragraphs 9.7 to 9.8 at the time of his appointment and on a continuing basis.

S 9.7 A director must not be disqualified under section 59(1) of the FSA or section 68(1) of the IFSA, and must have been assessed by the EMI to have complied with the fit and proper requirements.

S 9.8 A director of an EMI must not be an active politician.

Composition of the board

S 9.9 The board and its committees (if any) must be of a size that promotes effective deliberation and encourages the active participation of all directors.

S 9.10 The chairman of the board must not be an executive director.

S 9.11 An EMI shall ensure no less than two third of the board members are non-executive directors and are not involved in the day-to-day management of the e-money business.

S 9.12 For an eligible EMI, no less than one third of the board members shall be independent directors, who shall be independent in character and judgement and are not a major shareholder or representing major shareholder of the EMI.

Question 2:
Please provide your views and potential challenges in complying with the minimum independent director requirement for eligible EMIs and the impact to your institution, if any.

Board meetings

S 9.13 The board must meet sufficiently whereby the number and frequency of board meetings must commensurate with the size and complexity of the EMI's operations, to review the EMI performance, including the status of its compliance with regulatory requirements and to deal with any issues pertaining to the operations of the EMI.

S 9.14 A director must devote sufficient time to prepare for and attend board meetings, and maintain a sound understanding of the business of the EMI as well as relevant market and regulatory developments.

S 9.15 In respect of the quorum for board meetings, an EMI must require at least half of the board members to be present.

S 9.16 The board must ensure that clear and accurate minutes of board meetings are maintained to record the decisions of the board, including the key deliberations, rationale for each decision made, and any significant concerns or dissenting views. The minutes must indicate whether any director abstained from voting or excused himself from deliberating on a particular matter.

S 9.17 For eligible EMIs, a director must attend at least 75% of the board meetings held in each financial year.

Board committees (for eligible EMIs only)

S 9.18 At a minimum, an eligible EMI shall establish the following board committees–
(a) board audit committee; and
(b) board risk management committee.

G 9.19 An eligible EMI may combine its board audit committee and board risk management committee.

S 9.20 Each board committee shall–
(a) not be chaired by the chairman of the board;
(b) have at least three (3) directors;
(c) have at least one third independent directors;
(d) be chaired by an independent director; and
(e) comprise directors who have the skills, knowledge and experience relevant to the responsibilities of the board committee.

S 9.21 Each board committee shall have in place the relevant Terms of Reference and shall assume the specific responsibilities enumerated for it in Appendix 3.

10 Senior management

S 10.1 A member of senior management must not be disqualified under section 59(1) of the FSA or section 68(1) of the IFSA, and must have been assessed to comply with the fit and proper requirements.

S 10.2 For eligible EMIs, substantial shareholders must not hold a senior management position. This serves to preserve an appropriate separation between ownership and management of an EMI in line with the broader responsibilities of EMIs towards its customers and merchants.

S 10.3 A CEO must devote the whole of his professional time to the service of the EMI and resides in Malaysia unless the Bank approves otherwise in writing[7].

S 10.4 An EMI that is involved in other business or activity, other than issuing e-money, shall appoint a dedicated senior officer with relevant expertise and experience to assume the role of the Head of e-money business.

S 10.5 The senior management of an EMI is responsible for ensuring the following–

(a) effective policies and procedures are established and implemented for, among others, the following areas–
   (i) risk management and appropriate controls to manage and monitor risks;
   (ii) due diligence and oversight to manage outsourcing arrangements and other third party arrangements supporting the e-money operations;
   (iii) sufficient and timely reporting or escalation of issues to the board;
(b) overseeing the formulation and effective implementation of any business or strategic plan, including the strategic technology plan and associated technology policies and procedures;
(c) decision making processes give adequate consideration to customers' interests; and
(d) a robust assessment is conducted to approve any deviation from policies and procedures, including technology-related policies. Material deviations must be reported to the board.

S 10.6 The senior management shall consist of individuals with the appropriate skill set and experience to support and manage the e-money business. This includes individuals with technology background to provide guidance on the EMI's technology plans and operations.

S 10.7 For the purpose of paragraph 10.6, an eligible EMI shall ensure that a designated staff who does not engage in day-to-day technology operations should be responsible for the identification, assessment and mitigation of technology risks.

11 Control function

G 11.1 The board and senior management should create an environment, which not only ensures that the EMI and its officers comply with legal and regulatory requirements, and adopt relevant risk management practices, but also encourages the ethical conduct that underlies such requirements.

[7] Pursuant to section 55(3) of the FSA and section 64(3) of the IFSA.

S 11.2 The board is responsible for overseeing the management of an EMI's control function. The board shall–

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

(b) ensure the establishment of the control functions and the position of the relevant officers[8], and ensure that the said functions and officers are provided with appropriate standing, authority and independence;

(c) ensure the appointment of officers who have adequate working knowledge in e-money business and the legal and regulatory framework, and can effectively support the EMI's internal control framework;

(d) provide the relevant officers with direct and unimpeded access to the board; and

(e) where the risk or compliance officer also carries out responsibilities in respect of other control functions[9], be satisfied that a sound overall control environment will not be compromised by the combination of responsibilities performed by the compliance officer.

S 11.3 The senior management is collectively responsible for the effective management of an EMI's internal control framework. In discharging this responsibility, senior management shall–

(a) establish a written policy for the control function and ensure that it is kept up to date;

(b) establish a control function commensurate with the size, nature of operations and complexity of the EMI, having regard to the requirements in paragraphs 11.4 until 11.17;

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

(d) ensure that the control function is kept informed of any organisational developments to facilitate the timely identification of compliance risk;

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

(f) report to the board at least annually on the effectiveness of the EMI's overall management of compliance and risk management.

S 11.4 An EMI 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 EMI's business.

[8] Compliance, risk and internal audit officer

[9] Compliance and risk management function responsibilities cannot be shared with, nor can the compliance or risk officer assume responsibilities for internal audit as such practices would render the independent review process described in paragraph 11.15 ineffective.

S 11.5 The control function must be independent of business lines in order to carry out its role effectively. As such, an EMI must ensure that the control function is not placed in a position where there are real or potential conflicts in respect of its scope of responsibilities, reporting lines or remuneration.

S 11.6 Where control function responsibilities are shared with another control function, senior management must ensure that officers which also assume responsibilities for other control functions have the capacity and expertise to deliver their broader mandates while providing adequate focus to their control function responsibilities.

S 11.7 Where an officer of a control function also assumes responsibilities for another control function, the said officer must ensure that his independence, ability to provide sufficient time, focus and commitment to his responsibilities in respect of the control function are not impaired.

Compliance

S 11.8 The compliance function shall identify and assess the compliance risk associated with an EMI's activities. This requires the compliance function to have adequate knowledge and exposure to key business processes of the EMI and keep up to date with material changes in the EMI's business.

S 11.9 The compliance officer must report to senior management on a regular basis the findings and analyses of compliance risk. The report shall include at minimum–

(a) the results of the compliance risk assessment undertaken during the assessment period, highlighting key changes in the compliance risk profile of an EMI as well as areas where greater attention by senior management would be needed;

(b) a summary of incidents of non-compliance and deficiencies in the management of compliance risk in various parts of the EMI;

(c) an assessment of the impact (both financial and non-financial) of such incidents on the EMI (for example, fines, administrative or otherwise, or other disciplinary actions taken by any regulatory authority in respect of any officers of the EMI);

(d) recommendations of corrective measures to address incidents of non-compliance and deficiencies in the management of compliance risk; and

(e) a record of corrective measures already taken and an assessment of the adequacy and effectiveness of such measures.

S 11.10 The compliance officer shall ensure that the reports referred to in paragraph 11.9 are readily available to the internal audit function of the EMI, the Bank and other relevant regulatory authorities upon request.

Risk management

S 11.11 An EMI shall establish a risk management framework that enables the identification, measurement, and continuous monitoring of all relevant and material risks. The framework shall be supported by a robust management information system that facilitates the timely and reliable reporting of risks.

S 11.12 An EMI shall establish risk monitoring and reporting requirements, which include the development and use of key risk indicators to provide early warnings on adverse risk developments to ensure the EMI is able to manage and mitigate its risks in a timely manner.

S 11.13 The risk officer must report to the board and senior management on a regular basis on the assessment of the material risks affecting the EMI and ensure the material risks are mitigated and periodically monitored. The report must be readily available to the internal audit function of the EMI, the Bank and other regulatory authorities upon request.

Internal Audit

S 11.14 An EMI shall ensure that there is clear separation of the internal audit function and other control functions, i.e. compliance and risk management function.

S 11.15 Compliance and risk management function and the framework for such functions shall be included in the risk assessment methodology of the internal audit function, and an audit programme that covers the adequacy and effectiveness of the compliance and risk management functions' responsibilities shall be established, including testing of controls commensurate with the perceived level of risk.

S 11.16 The internal audit function shall report regularly to the board and senior management on the effectiveness and adequacy of the risk management and compliance functions and whether the said functions are working effectively.

S 11.17 The internal audit function shall inform senior management, including the compliance or risk officer, of any incidents of non-compliance or material risks that it discovers.

12 Shariah governance

S 12.1 An EMI that offers Shariah compliant e-money shall ensure the operationalisation of Shariah compliant e-money complies with the rulings of the Shariah Advisory Council of Bank Negara Malaysia and relevant Shariah standards issued by the Bank.

S 12.2 The board shall be responsible to ensure overall compliance of the EMI's Shariah compliant e-money with Shariah.

S 12.3 Senior management shall ensure the operationalisation of Shariah compliant e-money complies with Shariah at all times.

S 12.4 An EMI shall appoint a qualified Shariah advisor, who is responsible to provide objective and sound advice to ensure that the Shariah compliant e-money complies with Shariah.

S 12.5 In relation to paragraph 12.4, the Shariah advisor shall be an individual, a company or an existing Shariah committee within its group affiliate, that holds qualification in Shariah[10] and possesses reasonable knowledge and experience in Islamic finance. An EMI shall notify the Bank on the appointment of the Shariah advisor no later than fourteen (14) days of such appointment.

S 12.6 An EMI must ensure the robustness of its internal control functions for effective management of Shariah non-compliance risk. This shall include, but is not limited to, the EMI conducting an annual assessment on the compliance of its Shariah compliant e-money with the relevant Shariah requirements.

13 Fit and proper

S 13.1 An EMI shall ensure its directors and CEO consist of people with calibre, credibility, 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.

[10] At minimum, the individual or representative(s) of a company appointed as Shariah advisor is expected to hold a bachelor's degree in Shariah, which includes study in Usul Fiqh (principles of Islamic jurisprudence) or Fiqh Muamalat (Islamic transaction/commercial law).

PART C OPERATIONAL AND RISK MANAGEMENT REQUIREMENTS

14 Local incorporation

S 14.1 An EMI shall be a company incorporated under the Companies Act 2016.

15 Minimum capital funds for non-bank EMI

S 15.1 A non-bank EMI shall maintain, at all times, the following minimum capital funds–

(a) **Standard EMI**: RM1 million or 8% of outstanding e-money liabilities[11], whichever higher; or

(b) **Eligible EMI**: RM5 million or 8% of outstanding e-money liabilities, whichever higher.

S 15.2 A non-bank EMI shall ensure that it has sufficient liquidity for its daily operations. At a minimum, an EMI shall maintain a liquidity ratio[12] of one (1).

S 15.3 A non-bank EMI shall maintain the required minimum capital funds in accordance with the computation specified in Appendix 4.

Question 3:
Please provide feedback on the following–

1) What is the expected timeline for your institution to be able to meet the above requirement?
2) What are the potential challenges in meeting the revised minimum capital funds?

16 Safeguarding of funds

S 16.1 An EMI shall ensure that any funds collected in exchange of the e-money issued are maintained separately (i.e. in a separate account), from the EMI's own working capital funds or any funds collected under the EMI's other business or activity.

[11] Monthly average of outstanding e-money liabilities in the preceding six months.
[12] Liquidity ratio refers to current ratio of the company (current asset / current liabilities).

S 16.2 An EMI shall deposit the funds specified in paragraph 16.1 in a trust account with a banking institution after a customer places funds/tops-up the e-money, which shall be governed as follows–

(a) the trust account shall be established in accordance with the Trustee Act 1949;

(b) the funds can only be used for the following–

(i) refund to customers;

(ii) payment to merchants; or

(iii) payment to another e-money account or bank account arising from a credit transfer transaction.

(c) the funds may only be invested in high quality liquid ringgit assets, which are limited to–

(i) deposits placed with banking institutions;

(ii) debt securities issued or guaranteed by the Federal Government or the Bank;

(iii) Cagamas debt securities; and

(iv) other instruments as may be specified by the Bank;

(d) any revenue earned from the investment of the funds in the trust account may only be used for activities specified under paragraph 16.2(b) unless the funds are in excess of the total outstanding e-money liabilities; and

(e) payment for any costs, charges and expenses incurred in connection with the administration of the trust account can be made from the trust account only if the balance in the trust account after deduction of the cost, charges and expenses is sufficient to cover all outstanding e-money liabilities.

S 16.3 An EMI shall ensure it has sufficient funds in the trust account to cover the total outstanding e-money liabilities, in the event its outstanding e-money liabilities are greater than the funds in the trust account.

G 16.4 In respect of the requirement under paragraph 16.3, an EMI should top-up the trust account within one (1) working day or as soon as reasonably practicable.

S 16.5 An EMI who is unable to restrict their business or activity to e-money business only shall deposit and maintain an additional 2% of their outstanding e-money liabilities in the trust account at all times.

G 16.6 Notwithstanding paragraph 16.2, an EMI with total outstanding e-money liabilities less than RM1 million may safeguard the funds collected in exchange of e-money issued using–

(a) bank guarantee; or

(b) other methods subject to the following conditions:

(i) effectiveness must be at par with a bank guarantee or trust account; and

(ii) subject to the Bank's prior written approval.

G 16.7 An EMI should diversify the placement of the funds received in exchange of the e-money issued, in bank accounts maintained at several banking institutions to mitigate exposure to any single banking institution.

Question 4:

1) For the purpose of paragraph 16.2, please identify the potential challenges and expected timeline in meeting the requirement on safeguarding of funds, particularly for smaller EMI such as those with outstanding e-money liabilities of less than RM1 million.

2) For the purpose of paragraph 16.5, please provide your view on the said requirement, including challenges faced by your institution (if any) to fulfil this requirement.

3) For the purpose of paragraph 16.6(b), what other methods can be considered of which the effectiveness to safeguard the funds is at par with a bank guarantee or trust account?

17 Business continuity management

S 17.1 The board and senior management are responsible for ensuring the identification and implementation of an effective business continuity management (BCM) framework within the EMI.

S 17.2 An EMI must undertake a structured risk assessment process to–

(a) identify potential threats that could cause material business disruptions, resulting in the inability to fulfil business obligations; and

(b) assess the likelihood of the identified threats occurring and determine the impact on the EMI.

G 17.3 For purposes of paragraph 17.2, the EMI is encouraged to carry out a business impact analysis (BIA) on an annual basis and whenever there are material changes to the EMI's business activity, as this forms the foundation of developing the business continuity plan (BCP).

S 17.4 An EMI shall determine the maximum tolerable downtime (MTD) and recovery time objectives (RTO) for each critical business function. The goal is to develop a BCP that details the procedures and the minimum level of resources required to recover the critical business functions within the recovery timeframe and maintain services at an acceptable level.

S 17.5 An EMI shall develop an effective BCP and disaster recovery plan (DRP) for at least all critical business functions.

S 17.6 To ensure comprehensiveness of its BCM, an EMI shall ensure its outsourced service provider has an effective BCP and DRP, and implements relevant safeguards to ensure the continuity of the material outsourced activities, with the objective to minimise the EMI's business disruptions.

S 17.7 The BCP and DRP of an EMI and its service provider must be tested regularly to ensure the functionality and effectiveness of the recovery strategies and procedures, preparedness of staff and other recovery resources.

18 Outsourcing risk management

S 18.1 An EMI shall remain responsible and accountable for any services outsourced to a service provider under an outsourcing arrangement.

S 18.2 An EMI shall obtain the Bank's prior written approval before–

(a) entering into a new material outsourcing arrangement; or
(b) making material changes to an existing material outsourcing arrangement.

S 18.3 The board shall review and approve any material outsourcing arrangement considered by the EMI, before the proposed material outsourcing arrangement is submitted to the Bank for approval.

S 18.4 Prior to entering into any outsourcing arrangement, an EMI shall, at minimum, ensure the following–

(a) availability of sufficient expertise within the EMI to oversee and manage the outsourcing relationship; and
(b) the scope and nature of services and operations to be outsourced would not compromise the controls and risk management of the EMI services. An EMI shall ensure the following–
    (i) the outsourcing of such processes does not take away the critical decision making function of the EMI;
    (ii) the outsourcing of such processes does not threaten strategic flexibility and control of the EMI;
    (iii) the outsourcing of such processes would not impair the reputation, integrity and credibility of the EMI; and
    (iv) processes are in place for the EMI to retain the continuous ability to comply with the regulatory and supervisory requirements on the outsourced functions.

S 18.5 An EMI shall have a contingency plan or arrangements to secure business continuity in the event the arrangement with the service provider is suddenly terminated. This is to mitigate any significant discontinuity in the work that is supposed to be conducted by the service provider. The contingency plan shall

be reviewed from time to time to ensure that the plan is current and ready for implementation in the event of sudden termination of the service provider.

S 18.6 Reporting by the service provider to the EMI and monitoring mechanisms on the service provider shall be put in place by the EMI to ensure that the integrity and quality of work conducted by the service provider is maintained.

S 18.7 Regular reviews shall be conducted by the EMI to monitor the performance of service providers.

S 18.8 Periodic independent reviews either via internal and/ or external audits, shall be conducted by the EMI on the outsourced operations, with the same scope of review if the said operations are conducted in-house.

S 18.9 An EMI shall ensure that any weaknesses highlighted during the audit under paragraph 18.8 are well documented and promptly rectified by the service provider, especially where such weaknesses may affect the integrity of the internal controls of the EMI.

Assessment of service provider

S 18.10 An EMI shall conduct appropriate due diligence of a service provider at the point of considering new outsourcing arrangements, and renewing or renegotiating existing arrangements. The due diligence must cover, at minimum–

(a) capacity, capability, financial strength and business reputation[13];
(b) risk management and internal control capabilities, including physical and IT security controls, and business continuity management[14];
(c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites;
(d) access rights of the EMI and the Bank to the service provider;
(e) measures and procedures to ensure data protection and confidentiality;
(f) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chain of the outsourcing arrangement;
(g) undue risks[15] resulting from similar business arrangements, if any, between the service provider and the EMI;

[13] This includes an assessment that the service provider is a going concern and has strong governance structures to manage the outsourced activity throughout the duration of the arrangement.
[14] Including the ability of the service provider to respond to service disruptions or problems resulting from natural disasters, or physical or cyber-attacks, within an appropriate timeframe.
[15] For instance, concentration risk to a systemic service provider in the industry or where the service provider's fee structure or relationship with the EMI may create potential conflict of interest issues.

(h) the extent of concentration risk to which the EMI is exposed with respect to a single service provider and the mitigation measures to address this concentration. This does not apply to a service provider that is an affiliate and is supervised by a financial regulatory authority; and
(i) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document.

S 18.11 An EMI shall ensure that the outcomes of the due diligence process are well-documented and included in the outsourcing arrangement proposal to the board, for approval.

Outsourcing agreement

S 18.12 An EMI shall ensure that the outsourcing arrangement is governed by a written agreement that is legally enforceable, and shall include the minimum requirements specified in Appendix 6.

S 18.13 The outsourcing agreement must also contain provisions which–
(a) enable the Bank to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity;
(b) enable the Bank to conduct on-site supervision of the service provider where the Bank deems necessary;
(c) enable the Bank to appoint an independent party to perform a review of the relevant systems, information or documents of the service provider relating to the outsourced activity, where the Bank deems necessary; and
(d) allow the EMI the right to modify or terminate the arrangement when the Bank issues a direction to the EMI to that effect under the FSA or IFSA, as the case may be.

Protection of data confidentiality

S 18.14 An EMI shall ensure that appropriate controls are in place and are effective in safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, an EMI shall ensure that–
(a) information disclosed to the service provider is limited to the extent necessary to provide the contracted service, and only on a need-to-know basis;
(b) all locations (e.g. city and country) where information is processed or stored, including back-up locations, are made known to the EMI;

(c) where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are at a minimum comparable to Malaysia;
(d) where the service provider provides services to multiple clients, the EMI's information must be segregated[16] from the information of other clients of the service provider;
(e) the service provider maintains compliance with applicable security requirements and established security standards[17] at all times; and
(f) the service provider undertakes to safeguard customer information of the EMI at all times and reports any customer information breach to the EMI within an agreed timeframe.

Outsourcing outside Malaysia

S 18.15 In conducting the due diligence process in respect of outsourcing arrangements where the service provider is located or performs the outsourced activity outside Malaysia, an EMI shall ensure that such assessment addresses the added dimensions of risks associated with outsourcing outside Malaysia, and the ability of the EMI or service provider to implement appropriate responses to emerging risk events in a timely manner.

S 18.16 An EMI shall ensure that the outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect–
(a) the EMI's ability to effectively monitor the service provider and execute its BCP;
(b) the EMI's prompt recovery of data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; 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 activity.

Outsourcing involving cloud services

S 18.17 In relation to the EMI's ability to conduct audits and inspections on the cloud service provider and sub-contractors, an EMI may rely on third party certification and reports made available by the cloud service provider for the audit[18], 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 access to the third party and service provider to clarify matters relating to the audit.

[16] Either logically or physically.
[17] Any relevant local or international standards commonly applied by the relevant industry.
[18] For the avoidance of doubt, such certifications or reports should not substitute the EMI's right to conduct on-site inspections where necessary.

S 18.18 In relation to the testing of a cloud service provider's BCP, an EMI must be able to access information on the state of robustness of the controls instituted by such cloud service providers arising from the BCP testing.

Question 5:

Please provide feedback on the following–

1) Please provide your feedback on the interpretation of "material outsourcing arrangement" specified under paragraph 5.2?
2) What are the potential challenges and expected timeline to comply with the enhanced outsourcing requirements specified under paragraph 18?

19 Fraud risk management

S 19.1 An EMI shall ensure risk management processes, procedures, systems and controls are in place to enable fraud risk mitigation and management.

S 19.2 An EMI shall establish effective procedures on fraud detection, analysis, investigation and reporting, which includes–

(a) fraud detection and transaction monitoring that can facilitate timely identification and mitigation of suspicious transactions;
(b) regular analysis to understand fraud trends and modus operandi. This includes the ability to be vigilant of evolving trends and taking into account material changes in the business strategy, which may increase exposure to potential fraud risk; and
(c) reporting of fraud incidents to senior management and the board on a regular basis.

S 19.3 An EMI shall conduct periodic review on the adequacy of its fraud risk mitigation measures.

S 19.4 In the event of fraud occurrences, the EMI shall take appropriate and immediate corrective measures to address gaps and vulnerabilities in order to strengthen the security features of its e-money scheme.

S 19.5 An EMI shall implement relevant safeguards to prevent unauthorized reloading of an e-money account, in particular if reloading using payment cards is allowed.

Risk-based authentication for online payment transactions

S 19.6 An EMI shall authenticate its customer for online payment transactions using strong authentication methods, such as multi-factor authentication (MFA)[19], to mitigate the risk of fraudulent online transactions.

G 19.7 Notwithstanding paragraph 19.6, an EMI may authenticate its customer using risk-based authentication for low risk online payment transactions.

S 19.8 For the purpose of paragraph 19.7, low risk transactions shall consist of the following–

(a) online payment transactions below RM250; or

(b) recurring or card-on-file transactions below RM10,000[20], where an EMI has authenticated its customer using strong authentication for first time use.

S 19.9 In applying risk-based authentication for low risk online payment transactions under paragraph 19.8, an EMI shall–

(a) ensure the use of effective risk analysis tools and establish a set of criteria or factors that appropriately reflect the nature, size and characteristics of the online payment transactions. Such criteria or factors must be consistent with the EMI's risk appetite and tolerance level; and

(b) periodically review the risk assessment criteria or factors to ensure its continued relevance, having regard to the latest development in cybersecurity risks and authentication technologies, as well as, fraud trends and incidents.

G 19.10 An EMI may wish to identify a backstop limit, i.e. tolerable amount of fraud losses, in implementing risk-based authentication to mitigate against high fraud losses.

S 19.11 An EMI shall notify the Bank at least one (1) month prior to first-time implementation of risk-based authentication for low risk online payment transactions under paragraph 19.8.

S 19.12 An EMI shall provide customers with an option to opt-out or disable the function that allows unauthenticated online payment transactions, which shall be done through convenient means.

---

[19] Based on three (3) basic authentication factors, namely, something the user knows (e.g. PIN, personal information), something the user possesses (e.g. identity card, registered mobile number) and something the user is (e.g. biometric characteristics) which are mutually exclusive.

[20] For open third party fund transfer and open payment transactions with a value of RM10,000 and above, an EMI shall deploy multi-factor authentication solutions with stronger security controls as per paragraph 28.71-28.73 of this policy document.

S 19.13 An EMI shall set a maximum daily cumulative limit for both the amount and number of unauthenticated online payment transactions for a customer.

S 19.14 An EMI shall ensure that customer verification with strong authentication method is conducted once the online payment transactions exceed the maximum daily cumulative limit.

S 19.15 An issuer shall provide convenient means to customers to reduce the limits applied under paragraphs 19.8 or the maximum daily cumulative limit as set under paragraph 19.13.

S 19.16 An EMI shall raise awareness among customers on an on-going basis to ensure customers understand the functionalities of risk-based authentication transactions, potential risks of unauthenticated transactions as well as measures that may be taken by customers and options available in limiting such risks (e.g. opt-out). Such awareness shall be made using–

(a) mediums or channels which enable communications to be displayed prominently and easily accessible to customers, such as in mobile phone applications, e-mails and application notifications; or

(b) communication methods that can be easily understood by customers such as multi-lingual, frequently-asked-questions and clarity in explanation by call-centres.

S 19.17 An EMI shall immediately provide transaction alerts to customers, including customers with foreign-registered mobile numbers after every successful unauthenticated online payment transaction.

S 19.18 An EMI shall not hold a customer liable for fraud losses arising from unauthenticated online payment transactions in situations where the EMI has decided not to apply strong authentication methods, unless the EMI can prove with sufficient evidence that the customer has acted fraudulently.

Contactless verification requirement

S 19.19 For the purpose of paragraphs 19.20 and 19.21, the requirements shall be applicable to an EMI that issues international scheme prepaid cards only.

S 19.20 An EMI shall set a maximum amount for each contactless transaction as well as an appropriate cumulative limit for contactless transactions, which do not entail any customer verification.

S 19.21 To promote confidence in the use of contactless prepaid cards, an EMI shall provide customers with the ability to manage the cumulative transaction limit by undertaking the following–

(a) provide customers with convenient means to set a lower cumulative transaction limit for contactless transactions;

(b) provide customers with convenient means to turn off the contactless functionality in contactless prepaid cards; and

(c) raise awareness among customers about the facilities set out in paragraphs (a) and (b) minimally via the EMI's websites and product disclosure sheet.

Question 6:

1) Please provide feedback on the following–
   (a) What is your view on the online payment transaction limits proposed under paragraph 19.8?
   (b) What are the potential challenges and expected timeline to comply with the risk-based authentication requirements specified under paragraph 19.9 -19.18?

2) Debit cardholders are, by default, blocked from making any overseas transactions. Overseas transaction can be conducted only if the cardholder has expressly opted-in to conduct such transaction. As we are considering to impose this requirement on overseas transactions using e-money, given the higher risk on funds stored, what are the challenges that may be faced in operationalising this requirement?

20 Account management

S 20.1 An EMI shall ensure that all e-money transactions in Malaysia are in ringgit.

S 20.2 An EMI shall ensure that e-money transactions comply with the prevailing foreign exchange rules, including but not limited to investment in foreign currency asset by residents and payment in foreign currency between residents, through the implementation of robust internal controls and procedures.

S 20.3 An EMI shall ensure that any physical cash withdrawal outside Malaysia using e-money, shall be undertaken in foreign currency only.

S 20.4 An EMI that facilitates withdrawal of e-money balances into bank account shall ensure that any withdrawal of funds from the e-money account is paid into the customer's own bank account with a banking institution only.

S 20.5 An EMI shall ensure proper recording, management and monitoring of the accounts of all its customers, at all times.

Wallet limit

S 20.6 An EMI shall ensure that the wallet limit adopted for its e-money commensurate with the purpose and size of transactions.

S 20.7 An EMI shall ensure that adequate security and operational safeguards are in place to mitigate any risks associated with the use of e-money within the specified wallet limit.

S 20.8 An EMI shall obtain the Bank's prior written approval if the increase in wallet limit will result in the following–

(a) the wallet limit to be RM5,000 or more; or

(b) changes in the functionality and product features of the e-money account.

S 20.9 An EMI shall notify the Bank at least thirty (30) days prior to any increase in wallet limit below the RM5,000 threshold and does not involve any changes in functionality and product features of the e-money.

Refund of e-money balances

S 20.10 An EMI shall provide refunds of e-money balances in its customers' accounts should they decide to close their account, no longer wish to use the e-money, was wrongly charged due to technical discrepancies or due to disputed transactions.

S 20.11 The sum refunded shall be made without any additional costs, and shall be done in not more than 14 days from the date the claim is made.

S 20.12 For complex refund cases that cannot be completed within 14 days, the EMI shall communicate the reason for such delays to customers.

S 20.13 An EMI shall allow options for methods of refund and shall not limit it to only refund through crediting of funds back into the customer's e-money account.

Unclaimed e-money balances

S 20.14 An EMI shall ensure it manages any unclaimed e-money balances in accordance with the Unclaimed Moneys Act 1965.

21 White labelling

S 21.1 An EMI shall obtain the Bank's prior written approval before–

(a) entering into a white labelling arrangement for the first time; or

(b) making material changes to existing white labelling arrangement(s).

S 21.2 For the purpose of paragraph 21.1(a), an EMI shall notify the Bank on any subsequent white labelling arrangement, at least 14 days prior to entering into the said arrangement.

S 21.3 Prior to obtaining the Bank's approval, the board shall review and approve the EMI's plan to offer the white labelling arrangement and ensure that the EMI has sufficient resources and capacity to offer such solution. This includes, but is not limited to, having in place a framework, policy and operational procedures, manpower and system infrastructure to support the white labelling solution(s) offered to the partner(s) or other entity(s).

S 21.4 Senior management shall ensure adequate oversight on the implementation of the EMI's white labelling arrangement(s).

S 21.5 By providing white labelling solutions to the partner or another entity, it does not absolve the EMI's responsibility to ensure that the said solution complies with the requirements under this policy document and other applicable standards including those specified in paragraph 6.1.

S 21.6 An EMI must not engage with partner(s) or entity(s) with dubious or illegal activities.

S 21.7 At a minimum, an EMI that provides white labelling of its e-money shall ensure the following are met–

(a) proper due diligence is conducted on the partner(s) or entity(s) that it plans to offer the white labelling solution to, which includes assessments on their credibility and capability;

(b) an agreement with the partner(s) or entity(s) involved in the white-labelling arrangement is in place and clearly indicates the following–

(i) the rights and responsibilities of each party;

(ii) responsibilities of the partner(s) or entity(s) on controls and measures to ensure information security;

(iii) dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant;

(iv) ability of the EMI and its external auditor[21] to conduct audits and on-site inspections on the partner(s) or entity(s) in relation to the white labelling arrangement;

(c) partner(s) or other entity(s) involved in the white-labelling arrangement provide adequate system safeguards for the installation and use of the white labelling solution; and

(d) partner(s) or other entity(s) involved in the white-labelling arrangement have appropriate policies and procedures for customer and merchant on-boarding process.

S 21.8 The EMI shall provide clear and prominent disclosure to customers on the roles and responsibilities of the partner(s) or entity(s) as well as the EMI for the e-money issued, including in managing any disputes or issues faced by the customers.

S 21.9 The EMI shall disclose the name and brand of the partner(s) and other entity(s) that is using its white labelling solution on the EMI's website and any other relevant platform.

S 21.10 The EMI shall maintain proper records with appropriate level of granularity of funds tagged to each partner(s) or entity(s) and their individual customers, including but not limited to, records of funds collected from customers, the e-money transactions, complaints and resolutions, as well as, refunds made to its customers or payment to its merchants. The EMI shall ensure that the appointed trustee also has clarity on the funds tagged to the customer and merchants of each partner to ensure proper distribution of funds.

22 Other business or activity

Promoting or cross-selling financial products or services

S 22.1 A non-bank EMI shall not use its e-money platform or system to promote or cross-sell any financial products or services[22] except with the Bank's prior written approval.

S 22.2 The board shall review and approve any arrangement to promote or cross-sell any financial products or services, before the proposal is submitted to the Bank for approval.

[21] Including an agent appointed by the EMI.

[22] For the avoidance of doubt, this shall include financial products or services that is not offered by institutions regulated by the Bank under the FSA, IFSA, DFIA, Money Services Business Act 2011 and any other written law administered by the Bank.

S 22.3 Notwithstanding paragraph 22.1, a non-bank EMI shall only notify the Bank where the arrangement to promote or cross-sell involves non-financial products or services.

S 22.4 Prior to entering into any arrangement specified in paragraph 22.1, a non-bank EMI shall, at minimum, ensure the following–

(a) the scope and nature of such arrangement would not significantly increase the risk exposure to the non-bank EMI and would not impair the reputation, integrity and credibility of the non-bank EMI; and

(b) the necessary controls and risk management are in place to manage any risks from such arrangement.

S 22.5 A non-bank EMI shall ensure that the agreement to promote or cross-sell any financial products or services specified in paragraph 22.1 clearly sets out the accountabilities of each party in the arrangement.

S 22.6 A non-bank EMI shall provide clear communication to its customers on the demarcation of roles between the non-bank EMI for the e-money and the provider of the products or services under the arrangement specified in paragraph 22.1.

S 22.7 A non-bank EMI shall inform customers on who is responsible to manage complaints or disputes pertaining to the products or services under the arrangement specified in paragraph 22.1, including appropriate avenues for customers to seek redress.

Other business of EMI

S 22.8 A non-bank EMI that carries on other business or activity within the same entity, which is not in connection with or for the purpose of its e-money business, shall ensure the following–

(a) a clear segmentation between the e-money business and other business or activity is established, which shall include but is not limited to, establishing and maintaining segmented financial reports[23] on e-money business;

(b) a clear segregation of policies and procedures between e-money activities and other business or activity is established;

(c) clear roles, responsibilities and accountability of the board, senior management and staff for each business or activity are established;

(d) no comingling of e-money funds with other working capital or funds of other business or activity; and

[23] May be segmented in the management accounts.

(e) a strong financial position is demonstrated if the non-bank EMI is involved in other business or activity that may pose higher risk to the sustainability of the non-bank EMI.

S 22.9 A non-bank EMI shall notify the Bank in a timely manner on the following–

(a) prior to operationalising other business or activities that may potentially be of high risk, in terms of financial viability or reputation of the entity; and

(b) if there is potential risk or issues arising from other business or activity, which may significantly impact the financial viability or reputation of the non-bank EMI.

23 Specific requirement for registered merchant acquirers

S 23.1 An EMI that acquires merchants for the purpose of accepting payment instruments including its own e-money shall be registered pursuant to subsection 17(1) and 18(1) of the FSA.

S 23.2 For the purpose of paragraph 23.1, the EMI shall refer to the requirements specified in the Merchant Acquiring Exposure Draft issued on 17 July 2020.

24 Exit plan

S 24.1 A non-bank EMI shall be prepared to exit the e-money business in the event its business proves to be unsustainable or can no longer support its operations in a reliable manner.

S 24.2 A non-bank EMI shall maintain an exit plan, which will enable the non-bank EMI to unwind its business operations voluntarily without any regulatory intervention and in an orderly manner without causing disruption to its customers, merchants and the payment ecosystem where it operates.

S 24.3 For purposes of paragraph 24.2, a non-bank EMI shall establish an exit plan valid for a three-year period, which can be operationalised, if needed. At minimum, the exit plan must include the following–

(a) plausible internal triggers[24] for exiting the business, which demonstrate unsustainable business, inability to fulfil the value proposition for its e-money business or materialisation of risks beyond the non-bank EMI's own risk appetite;

[24] Refer to paragraph 24.4 (b).

(b) likely options and related measures to be taken for exiting that minimises disruption to its customers, merchants and the payment ecosystem[25] where it operates;
(c) potential impediments to the execution of identified exit options and measures to mitigate the impact of such impediments; and
(d) sources of funding and liquidity for exit (in addition to safeguarded customer funds) and the estimated timeframe to exit the business.

S 24.4 In relation to paragraph 24.3, the exit plan shall contain the following–

Table 1: Content of an exit plan

	Requirement	**Details**
(a)	Governance to support informed decision making in the activation of exit plan	• Well-defined roles and responsibilities of the board, senior management and business unit(s). • Policies, procedures and management information systems (MIS) to inform and support decision-making and smooth coordination of exit plan execution.
(b)	Exit triggers	• Identification of exit triggers, i.e. factors and indicators/thresholds that will prompt activation/execution of the exit plan. • Processes for continuous monitoring of factors and indicators/thresholds. • The exit triggers shall include, <u>but are not limited to</u>– (i) Compliance-related indicators, in particular incidences on non-compliance with minimum capital funds, liquidity ratio and safeguarding of customer funds; (ii) Financial-related indicators, in particular return on equity, cost-to-income ratio or any other going concern indicators; (iii) Operational-related indicators, in particular frequent unscheduled downtime of e-money system, cyber-attack incidences, breaches of

[25] For example, if the e-money is used for transportation purposes, whether its exit will cause the transportation community to be significantly disrupted.

		customer information, critical staff turnover rate.
(c)	Execution of measures that enable an orderly exit from the business without causing disruption to third-parties, in particular customers and counterparties	• Identification of possible actions that can be undertaken under different scenarios. • Identification of possible and credible funding sources to implement the exit plan. • Description of operational dependencies on external parties and its associated costs throughout the exit phase to ensure smooth operational continuity throughout the exit phase.
(d)	Communication and engagement strategy (including to the Bank) to mitigate unintended consequences	• Identification of key stakeholders, including customers, merchants, relevant regulators and authorities, counterparties, service providers, etc. • Information needs of respective stakeholders. • Medium, timing and frequency of communication. • Person(s) responsible for ensuring the effective coordination and execution of the communication and engagement strategy.

S 24.5 A non-bank EMI shall provide an undertaking that it will commit to its exit plan if its internal triggers are met within the three-year period.

S 24.6 The initial exit plan by an existing non-bank EMI shall be submitted to the Bank within one (1) year from the effective date of the final policy document. For applicant applying for approval to issue e-money, an exit plan shall be submitted upon submission of application to issue e-money. Subsequent exit plan(s) and undertaking(s) shall be endorsed by the board and submitted to the Bank within one (1) month after it being endorsed.

S 24.7 The exit plan and undertaking shall be reviewed every three (3) years or as and when there are material changes to the non-bank EMI's structure or operations.

S 24.8 The full implementation of the exit plan shall result in the cessation of the e-money business by the non-bank EMI.

S 24.9 For purposes of paragraph 24.2, within the exit plan, the non-bank EMI shall demonstrate the following–

(a) the necessary capabilities required to extract and aggregate real time data on customers and/or merchants, upon request, including up-to-date contact information and refund/payment mechanism; and
(b) the necessary capabilities and resources required to ensure continuity of services throughout the implementation of the exit plan, with specific focus on continuity of services under outsourcing arrangements.

25 Winding down or cessation of e-money business

S 25.1 An EMI shall wind-down its existing e-money operations upon the date of revocation of its e-money approval or cessation of business or operations. The winding down procedures shall commensurate with the nature, size and complexity of the EMI's e-money business and be made in accordance with relevant regulatory requirements.

S 25.2 In line with sections 23(2)(b) and 20(2)(b) of the FSA and IFSA respectively, where the approval to issue e-money is either revoked by the Bank or the EMI has ceased its business or operations, such EMI shall continue to discharge its obligations which includes but is not limited to the following–

(a) reimburse the funds collected from customers and settle the outstanding amount with the merchants and relevant beneficiaries of its e-money scheme at a reasonably practicable time;
(b) contact and provide adequate reminders, on a periodic basis to the relevant stakeholders, which includes but is not limited to customers and merchants, for a request of any unclaimed balances of e-money from the EMI;
(c) provide adequate notice to the relevant stakeholders on its winding down or cessation of e-money business and that it no longer has the approval under the FSA or IFSA to issue e-money;
(d) ensure customer information continues to be safeguarded and/or disposed appropriately in accordance with statutory records retention requirements.

S 25.3 An EMI shall keep relevant records and accounts to identify the beneficiaries of the e-money funds at all times to enable the EMI to clearly identify and distinguish the safeguarded funds from other working capital funds of the EMI. These records and information shall be made available to trustees to facilitate proper distribution of funds upon winding down or cessation of business.

S 25.4 An EMI shall lodge the outstanding e-money balances that remain unclaimed within the period stipulated under the Unclaimed Moneys Act 1965 with the Registrar.

26 Prohibitions

S 26.1 An EMI shall not–

(a) issue the e-money at a discount, i.e. issue e-money that has a monetary value greater than the sum received;

(b) use the money collected in exchange of e-money issued to extend loans or financing to any other persons;

(c) extend credit to the customer or any other person, or pay interest or profit on the e-money balances, or anything else that would add to the monetary value of the e-money; and

(d) associate, link or use the e-money scheme or platform to conduct dubious or illegal activities.

PART D IT REQUIREMENTS[26]

27 Technology risk management

S 27.1 An EMI shall establish the Technology Risk Management Framework (TRMF), which is a framework to safeguard the EMI's information infrastructure, systems and data as an integral part of the EMI's risk management framework.

G 27.2 The TRMF should include the following–

(a) clear definition of technology risk;

(b) clear responsibilities assigned for the management of technology risk at different levels and across functions, with appropriate governance and reporting arrangements;

(c) the identification of technology risks to which the EMI is exposed, including risks from the adoption of new or emerging technology;

(d) risk classification of all information assets/systems based on its criticality;

(e) risk measurement and assessment approaches and methodologies;

(f) risk controls and mitigations; and

(g) continuous monitoring to timely detect and address any material risks.

G 27.3 An EMI should establish an independent enterprise-wide technology risk management function which is responsible for–

(a) implementing the TRMF and Cyber Resilience Framework (CRF) as provided under paragraph 29;

(b) advising on critical technology projects and ensuring critical issues that may have an impact on the EMI's risk tolerance are adequately deliberated or escalated in a timely manner; and

(c) providing independent views to the board and senior management on third party assessments[27], where necessary.

G 27.4 An EMI should designate a Chief Information Security Officer (CISO), by whatever name called, to be responsible for the technology risk management function of the EMI. The EMI should ensure that the CISO has sufficient authority, independence and resources[28]. The CISO should–

(a) be independent from day-to-day technology operations;

[26] For the avoidance of doubt, eligible EMIs as defined in the policy document on Interoperable Credit Transfer Framework and EMIs that are banking institution shall comply with the IT requirements that are more stringent under the policy document on Risk Management in Technology.

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

[28] An EMI's CISO may take guidance from the expertise of a group-level CISO, in or outside of Malaysia, and may also hold other roles and responsibilities. Such designated CISO shall be accountable for and serve as the point of contact with the Bank on the EMI's technology-related matters, including managing entity-specific risks, supporting prompt incident response and reporting to the EMI's board.

(b) keep apprised of current and emerging technology risks which could potentially affect the EMI's risk profile; and
(c) be appropriately certified.

G 27.5 The CISO should be responsible for ensuring the EMI's information assets and technologies are adequately protected, which includes–
(a) formulating appropriate policies for the effective implementation of TRMF and CRF;
(b) enforcing compliance with these policies, frameworks and other technology-related regulatory requirements; and
(c) advising senior management on technology risk and security matters, including developments in the EMI's technology security risk profile in relation to its business and operations.

28 Technology operations management

Technology Project Management

S 28.1 An EMI shall establish appropriate governance requirements commensurate with the risk and complexity[29] of technology projects undertaken. This shall include establishing project oversight roles and responsibilities, authority and reporting structures, and risk assessment throughout the project life cycle.

G 28.2 The risk assessment should identify and address the key risks arising from the implementation of technology projects. These include the risks that could threaten successful project implementation and the risks that a project failure will lead to a broader impact on the EMI's operational capabilities. At a minimum, due regard should be given to the following areas–
(a) the adequacy and competency of resources including those of the vendor to effectively implement the project. This should also take into consideration the number, size and duration of significant technology projects undertaken concurrently by the EMI;
(b) the complexity of systems to be implemented such as the use of unproven or unfamiliar technology and the corresponding risks of integrating the new technology into existing systems, managing multiple vendor-proprietary technologies, large-scale data migration or cleansing efforts and extensive system customisation;

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

(c) the adequacy and configuration of security controls throughout the project life cycle to mitigate cybersecurity breaches or exposure of confidential data;
(d) the comprehensiveness of the user requirement specifications to mitigate risks from extensive changes in project scope or deficiencies in meeting business needs;
(e) the robustness of system and user testing strategies to reduce risks of undiscovered system faults and functionality errors;
(f) the appropriateness of system deployment and fallback strategies to mitigate risks from prolonged system stability issues; and
(g) the adequacy of disaster recovery operational readiness following the implementation of new or enhanced systems.

G 28.3 The board and senior management should receive and review timely reports on the management of these risks on an ongoing basis throughout the implementation of significant projects.

System Development and Acquisition

G 28.4 An EMI should establish an Enterprise Architecture Framework (EAF) that provides a holistic view of technology throughout the EMI. The EAF is an overall technical design and high-level plan that describes the EMI's technology infrastructure, systems' inter-connectivity and security controls. The EAF facilitates the conceptual design and maintenance of the network infrastructure, related technology controls and policies and serves as a foundation on which the EMI's plan and structure system development and acquisition strategies to meet business goals.

S 28.5 An EMI shall establish clear risk management policies and practices for the key phases of the system development life cycle (SDLC) encompassing system design, development, testing, deployment, change management, maintenance and decommissioning. Such policies and practices shall also embed security and relevant enterprise architecture considerations into the SDLC to ensure confidentiality, integrity and availability of data[30]. The policies and practices shall be reviewed at least once every three (3) years to ensure that they remain relevant to the EMI's environment.

G 28.6 An EMI is encouraged to deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to support more secure systems development.

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

G 28.7 An EMI should consider the need for diversity[31] in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

S 28.8 An EMI shall establish a sound methodology for rigorous system testing prior to deployment. The testing shall ensure that the system meets user requirements and performs robustly. Where sensitive test data is used, the EMI shall ensure proper authorisation procedures and adequate measures to prevent their unauthorised disclosure are in place.

G 28.9 The scope of system testing referred to in paragraph 28.8 should include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, and exception and negative testing, where applicable.

S 28.10 An EMI shall ensure any changes to the source code of IT systems are subject to adequate source code reviews to ensure the code is secure and was developed in line with recognised coding practices prior to introducing any system changes.

S 28.11 In relation to IT systems that are developed and maintained by vendors, an EMI shall ensure the source code continues to be readily accessible and secured from unauthorised access.

S 28.12 An EMI shall physically segregate the production environment from the development and testing environment for critical systems. Where an EMI is relying on a cloud environment, it shall ensure that these environments are not running on the same virtual host.

S 28.13 An EMI shall establish appropriate procedures to independently review and approve system changes. An EMI shall also establish and test contingency plans in the event of unsuccessful implementation of material changes to minimise any business disruption.

S 28.14 Where an EMI's IT systems are managed by third party service providers, the EMI shall ensure, including through contractual obligations, that the third party service providers provide sufficient notice to the EMI before any changes are undertaken that may impact the IT systems.

[31] Diversity in technology may include the use of different technology architecture designs and applications, technology platforms and network infrastructure.

G 28.15 When decommissioning systems, an EMI should ensure minimal adverse impact on customers and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

Cryptography

G 28.16 An EMI should promote the adoption of strong cryptographic controls for protection of important data and information which include–

(a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;

(b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;

(c) the periodic review, at least every three (3) years, of existing cryptographic standards and algorithms in IT systems, external linked or customer-facing applications to prevent exploitation of weakened algorithms or protocols; and

(d) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This should set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

G 28.17 An EMI should conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Where an EMI do not generate its own encryption keys, the EMI should undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessment[32], the EMI should consider whether such reliance is consistent with the EMI's risk appetite and tolerance. An EMI should also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.

G 28.18 An EMI should ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols should include secret and public cryptographic key protocols, both of which should reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols should be based on recognised international standards and tested accordingly. Commensurate with the level of risk, secret

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

cryptographic key and private-cryptographic key storage and encryption/ decryption computation should be undertaken in a protected environment, supported by a hardware security module (HSM) or trusted execution environment (TEE).

G 28.19 An EMI should store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers should be issued by recognised certificate authorities. The EMI should ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates should be consistent with industry best practices and applicable legal/ regulatory specifications.

Data Centre Infrastructure

S 28.20 An EMI shall ensure proper management of data centres and specify the resilience and availability objectives[33] of its data centres which are aligned with its business needs.

G 28.21 The network infrastructure should be designed to be resilient, secure and scalable. Potential data centre failures or disruptions should not significantly degrade the delivery of its financial services or impede its internal operations.

G 28.22 An EMI should ensure production data centres are concurrently maintainable. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment.

G 28.23 An EMI should host IT systems in a dedicated space intended for production data centre usage. The dedicated space should be physically secured from unauthorised access and is not located in a disaster-prone area. An EMI should also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure.

S 28.24 An EMI shall establish proportionate controls, ensure adequate maintenance, and holistic and continuous monitoring of the critical components of the production data centres aligned with the EMI's risk appetite.

[33] Availability objectives refer to the level of availability of the data centre, which is expected to be specified as an internal policy.

G 28.25 An EMI is encouraged to appoint a technically competent external third party service provider to carry out a production data centre risk assessment and set proportionate controls aligned with the EMI's risk appetite. The assessment should consider all major risks associated with the production data centre and should be conducted periodically or whenever there is a material change in the data centre infrastructure. The assessment should, at a minimum, include a consideration of whether paragraphs 28.22 to 28.24 have been adhered to. For data centres managed by third party service providers, an EMI may rely on independent third party assurance reports provided such reliance is consistent with the EMI's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the assessment. The designated board-level committee should deliberate the outcome of the assessment.

Data Centre Operations

S 28.26 An EMI shall ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth.

G 28.27 An EMI should involve both the technology stakeholders and the relevant business stakeholders within the EMI in its development and implementation of capacity management plans.

S 28.28 An EMI shall establish appropriate monitoring mechanisms to track capacity utilisation and performance of key processes and services[34]. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.

S 28.29 An EMI shall segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity[35]. In the case where vendors' or programmers' access to the production environment is necessary, these activities shall be properly authorised and monitored.

S 28.30 An EMI shall establish adequate control procedures for its data centre operations. These control procedures shall include procedures for batch processing management to ensure timely and accurate batch processes, implementing changes in the production system, error handling, as well as, management of other exceptional conditions.

[34] For example, batch runs and backup processes for the EMI's application systems and infrastructure.
[35] For example, system development activities must be segregated from data centre operations.

G 28.31 An EMI is encouraged to undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times.

S 28.32 An EMI shall maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes. Backup media shall be stored in an environmentally secure and access-controlled backup site.

G 28.33 In regard to paragraph 28.32, an EMI should also adopt the controls as specified in Appendix 7 or their equivalent to secure the storage and transportation of sensitive data in removable media.

G 28.34 Where there is a reasonable expectation for immediate delivery of service, an EMI should ensure that the relevant systems are designed for high availability.

Network Resilience

G 28.35 An EMI should design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.

G 28.36 An EMI should ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.

G 28.37 An EMI should establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.

S 28.38 An EMI shall ensure network services supporting IT systems are designed and implemented to ensure the confidentiality, integrity and availability of data.

G 28.39 An EMI should establish and maintain a network design blueprint identifying all of its internal and external network interfaces and connectivity. The blueprint should highlight both physical and logical connectivity between network components and network segmentations.

S 28.40 An EMI shall ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three (3) years.

S 28.41 An EMI shall implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the EMI from other entities within the group.

G 28.42 An EMI is encouraged to appoint a technically competent external third party service provider to carry out regular network risk assessment and set proportionate controls aligned with its risk appetite. The assessment should be conducted periodically or whenever there is a material change in the network design. The assessment should consider all major risks and determine the current level of resilience.

Third Party Service Provider Management

S 28.43 In addition to the requirements in paragraph 18 on outsourcing arrangements, the EMI shall fulfil the requirements under paragraphs 28.44 to 28.50 specifically for IT related third party service providers.

S 28.44 The board and senior management of the EMI shall exercise effective oversight and address associated risks when engaging third party service providers for critical technology functions and systems. Engagement of third party service providers, including engagements for independent assessment, does not in any way reduce or eliminate the principal accountabilities and responsibilities of an EMI for the security and reliability of technology functions and systems.

S 28.45 An EMI shall conduct proper due diligence on the third party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made of the third party service provider's capabilities in managing the following specific risks–

(a) data leakage such as unauthorised disclosure of customer and counterparty information;
(b) service disruption including capacity performance;
(c) processing errors;
(d) physical security breaches;
(e) cyber threats;
(f) over-reliance on key personnel;
(g) mishandling of confidential information pertaining to the EMI or its customers in the course of transmission, processing or storage of such information; and
(h) concentration risk.

S 28.46 At a minimum, the service level agreements with the EMI's service providers shall contain arrangements for disaster recovery and backup capability, where applicable, and IT system availability.

S 28.47 An EMI shall ensure its ability to regularly review the service level agreements with its third party service providers to take into account the latest security and technological developments in relation to the services provided.

S 28.48 An EMI shall ensure data residing in third party service providers are recoverable in a timely manner. The EMI shall ensure clearly defined arrangements with the third party service provider are in place to facilitate the EMI's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.

S 28.49 An EMI shall ensure the storage of its data is at least logically segregated from the other clients of the third party service provider. There shall be proper controls over and periodic review of the access provided to authorised users.

S 28.50 An EMI shall ensure IT system hosted by third party service providers have adequate recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third party service provider.

Cloud Services

S 28.51 An EMI shall fully understand the inherent risk of adopting cloud services. In this regard, an EMI is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment shall specifically address risks associated with the following–

(a) sophistication of the deployment model;
(b) migration of existing systems to cloud infrastructure;
(c) location of cloud infrastructure;
(d) multi-tenancy or data co-mingling;
(e) vendor lock-in and application portability or interoperability;
(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;
(g) exposure to cyber-attacks via cloud service providers;
(h) termination of a cloud service provider including the ability to secure the EMI's data following the termination;

(i) demarcation of responsibilities, limitations and liability of the cloud service provider; and
(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

S 28.52 The risk assessment as outlined in paragraph 28.51 shall be documented and made available for the Bank's review as and when requested by the Bank.

S 28.53 An EMI is expected to demonstrate that specific risks associated with the use of cloud services for IT systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in paragraph 28.51, as well as, the following areas–

(a) the adequacy of the over-arching cloud adoption strategy of the EMI including–
  (i) board oversight over cloud strategy and cloud operational management;
  (ii) senior management roles and responsibilities on cloud management;
  (iii) conduct of day-to-day operational management functions;
  (iv) management and oversight by the EMI of cloud service providers;
  (v) quality of risk management and internal control functions; and
  (vi) strength of in-house competency and experience;
(b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas–
  (i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and
  (ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit;
(c) the degree to which the selected cloud configuration adequately addresses the following attributes–
  (i) geographical redundancy;
  (ii) high availability;
  (iii) scalability;
  (iv) portability;
  (v) interoperability; and
  (vi) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.

G 28.54 An EMI should consider the need for a third party pre-implementation review on cloud implementation that also covers the areas set out in paragraph 28.53.

S 28.55 An EMI must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against

unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.

Access Control

S 28.56 An EMI must implement an appropriate access control policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.

G 28.57 In observing paragraph 28.56, an EMI should consider the following in its access control policy–

(a) adopt a "deny all" access control policy for users by default unless explicitly authorised;

(b) employ "least privilege" access rights or on a "need-to-have" basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;

(c) employ time-bound access rights which restrict access to a specific period including access rights granted to third party service providers;

(d) employ segregation of incompatible functions to ensure that no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as –

(i) system development and technology operations;

(ii) security administration and system administration; and

(iii) network operation and network security;

(e) employ dual control functions which require two or more persons to execute an activity;

(f) adopt stronger authentication for critical activities including for remote access;

(g) limit and control the use of the same user ID for multiple concurrent sessions;

(h) limit and control the sharing of user ID and passwords across multiple users; and

(i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs.

S 28.58 An EMI must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall commensurate with the

criticality of the functions and adopt at least one (1) or more of these three (3) basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).

S 28.59 An EMI shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There shall be appropriate controls in place to check the strength of the passwords created.

G 28.60 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, an EMI is encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) MFA that are more reliable and provide stronger fraud deterrents.

G 28.61 An EMI is encouraged to adopt dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system.

S 28.62 An EMI shall establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.

S 28.63 An EMI shall ensure the following–

(a) access controls to enterprise-wide systems are effectively managed and monitored; and

(b) user activities in IT systems are logged for audit and investigations. Activity logs shall be maintained for at least three (3) years and regularly reviewed in a timely manner.

Patch and End-of-Life System Management

S 28.64 An EMI shall ensure that IT systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, an EMI shall clearly assign responsibilities to identified functions–

(a) to continuously monitor and implement latest patch releases in a timely manner; and

(b) identify critical technology systems that are approaching EOL for further remedial action.

G 28.65 An EMI should establish a patch and EOL management framework which addresses among others the following requirements–

(a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;
(b) conduct of compatibility testing for critical patches;
(c) specification of turnaround time for deploying patches according to the severity of the patches; and
(d) adherence to the workflow for end-to-end patch deployment processes including approval, monitoring and tracking of activities.

Security of Digital Services

S 28.66 An EMI shall implement robust technology security controls in providing digital services which assure the following–

(a) confidentiality and integrity of customer and counterparty information and transactions;
(b) reliability of services delivered via channels and devices with minimum disruption to services;
(c) proper authentication of users or devices and authorisation of transactions;
(d) sufficient audit trail and monitoring of anomalous transactions;
(e) ability to identify and revert to the recovery point prior to incident or service disruption; and
(f) strong physical control and logical control measures.

G 28.67 An EMI should implement controls to authenticate and monitor all financial transactions. These controls, at a minimum, should be effective in mitigating man-in-the-middle attacks, transaction fraud, phishing and compromise of application systems and information.

S 28.68 An EMI must implement additional controls to authenticate devices and users, authorise transactions and support non-repudiation and accountability for high-risk transactions or transactions above RM10,000. These measures must include, at a minimum, the following–

(a) ensure transactions are performed over secured channels such as the latest version of Transport Layer Security (TLS);
(b) both client and host application systems must encrypt all confidential information prior to transmission over the network;
(c) adopt MFA for transactions;
(d) if OTP is used as a second factor, it must be dynamic and time-bound;
(e) request users to verify details of the transaction prior to execution;
(f) ensure secure user and session handling management;
(g) be able to capture the location of origin and destination of each transaction;

(h) implement strong mutual authentication between the users' end-point devices and EMI's servers, such as the use of the latest version of Extended Validation SSL certificate (EV SSL); and
(i) provide timely notification to customers that is sufficiently descriptive of the nature of the transaction.

S 28.69 An EMI must ensure the MFA solution used to authenticate financial transactions are adequately secure, which includes the following–
(a) binding of the MFA solution to the customer's account;
(b) activation of MFA must be subject to verification by the EMI; and
(c) timely notification to customers of any activation of and changes to the MFA solution via the customers' verified communication channel.

G 28.70 An EMI should deploy MFA technology and channels that are more secured than unencrypted short messaging service (SMS).

S 28.71 An EMI shall deploy MFA solutions with stronger security controls for open third party fund transfer and open payment transactions with a value of RM10,000 and above.

S 28.72 Such stronger MFA solutions shall adhere to the following requirements–
(a) payer/sender must be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction;
(b) authentication code must be initiated and generated locally by the payer/sender using MFA;
(c) authentication code generated by payer/sender must be specific to the confirmed identified beneficiary and amount;
(d) secure underlying technology must be established to ensure the authentication code accepted by the EMI corresponds to the confirmed transaction details; and
(e) notification must be provided to the payer/sender of the transaction.

S 28.73 Where an EMI deploys OTP as part of its stronger MFA solutions, the following features must be implemented–
(a) binding of the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction);
(b) generation of the OTP from the customer's device and not from the EMI's server; and
(c) requiring the customer to physically enter the generated OTP into the application.

S 28.74 For financial transactions below RM10,000, an EMI may decide on proportionate controls and authentication methods for transactions assessed by the EMI to be

of low risk. In undertaking the assessment, the EMI must establish a set of criteria or factors that reflect the nature, size and characteristics of a financial transaction. Such criteria or factors must be consistent with the EMI's risk appetite and tolerance. The EMI must periodically review the risk assessment criteria to ensure its continued relevance, having regard to the latest developments in cybersecurity risks and authentication technologies as well as fraud trends and incidents.

S 28.75 Where an EMI decides not to adopt MFA for financial transactions that are assessed to be of low risk, the EMI must nevertheless implement adequate safeguards for such transactions which shall include at a minimum the following measures–

(a) set appropriate limits on a per-transaction basis, and on a cumulative basis;

(b) provide a convenient means for customers to reduce the limits described in paragraph (a) or to opt for MFA;

(c) provide a convenient means for its customers to temporarily suspend their account in the event of suspected fraud; and

(d) provide its customers with adequate notice of the safeguards set out in sub-paragraphs (a) to (c).

S 28.76 An EMI shall ensure sufficient and relevant digital service logs are retained for investigations and forensic purposes for at least three (3) years.

S 28.77 An EMI shall ensure that critical online payments[36] services or transactions have high availability with reasonable response time to customer actions.

G 28.78 An EMI should ensure that the use of more advanced technology to authenticate and deliver digital services such as biometrics, tokenisation and contactless communication[37] comply with internationally recognised standards where available. The technology should be resilient against cyber threats[38] including malware, phishing or data leakage.

G 28.79 An EMI should undertake a comprehensive risk assessment of the advanced technologies and the algorithms deployed in its digital services. Algorithms should be regularly reviewed and validated to ensure they remain appropriate and accurate. Where third party software is used, an EMI may rely on relevant independent reports provided that such reliance is consistent with the EMI's risk

[36] For example, Internet and mobile application.

[37] Such as Quick Response (QR) code, Bar Code, Near Field Communication (NFC), Radio Frequency Identification (RFID).

[38] For example, in respect of QR payments, an EMI shall implement safeguards within its respective mobile applications to detect and mitigate risks relating to QR code that may contain malware or links to phishing websites.

appetite and tolerance, and the nature of digital services provided by the EMI which leverage on the technologies and algorithms.

G 28.80 An EMI should ensure authentication processes using biometric technology are secure, highly resistant to spoofing and have a minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions.

G 28.81 An EMI should perform continuous surveillance to assess the vulnerability of the operating system and the relevant technology platform used for its digital delivery channels to security breaches and implement appropriate corresponding safeguards. At a minimum, an EMI should implement sufficient logical and physical safeguards for the following channels/ devices–

(a) QR code;
(b) internet application; and
(c) mobile application and devices.

In view of the evolving threat landscape, these safeguards should be continuously reviewed and updated to protect against fraud and to secure the confidentiality and integrity of customer and counterparty information and transactions.

G 28.82 With respect to paragraph 28.81, an EMI should adopt the controls specified in the following Appendices for the respective digital delivery channel–

(a) Appendix 8: Control Measures on Internet Application;
(b) Appendix 9: Control Measures on Mobile Application and Devices; and
(c) Appendix 10: Control Measures on QR Code.

29 Cybersecurity management

Cyber Risk Management

G 29.1 An EMI should ensure that there is an enterprise-wide focus on effective cyber risk management to reflect the collective responsibility of business and technology lines for managing cyber risks.

S 29.2 An EMI shall develop a CRF which articulates the EMI's governance for managing cyber risks, its cyber resilience objectives and its risk tolerance, with due regard to the evolving cyber threat environment. Objectives of the CRF includes ensuring operational resilience against extreme but plausible cyber-attacks.

G 29.3 The CRF should be able to support the effective identification, protection, detection, response, and recovery (IPDRR) of systems and data hosted on-premise or by third party service providers from internal and external cyber-attacks. The CRF should consist of, at a minimum, the following elements–

(a) development of an institutional understanding of the overall cyber risk context in relation to the EMI's businesses and operations, its exposure to cyber risks and current cybersecurity posture;
(b) identification, classification and prioritisation of critical systems, information, assets and interconnectivity (with internal and external parties) to obtain a complete and accurate view of the EMI's information assets, critical systems, interdependencies and cyber risk profile;
(c) identification of cybersecurity threats and countermeasures including measures to contain reputational damage that can undermine confidence in the EMI;
(d) layered (defense-in-depth) security controls to protect its data, infrastructure and assets against evolving threats;
(e) timely detection of cybersecurity incidents through continuous surveillance and monitoring;
(f) detailed incident handling policies and procedures and a crisis response management playbook to support the swift recovery from cyber-incidents and contain any damage resulting from a cybersecurity breach; and
(g) policies and procedures for timely and secure information sharing and collaboration with other EMIs and participants in financial market infrastructure to strengthen cyber resilience.

Cybersecurity Operations

G 29.4 An EMI should establish clear responsibilities for cybersecurity operations which should include implementing appropriate mitigating measures in the EMI's conduct of business that correspond to the following phases of the cyber-attack lifecycle–
(a) reconnaissance;
(b) weaponisation;
(c) delivery;
(d) exploitation;
(e) installation;
(f) command and control; and
(g) exfiltration.

G 29.5 Where relevant, an EMI should adopt the control measures on cybersecurity as specified in Appendix 11 to enhance its resilience to cyber-attacks.

G 29.6 An EMI should deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure. The scope of monitoring should cover all critical systems including the supporting infrastructure.

S 29.7 An EMI shall ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture.

S 29.8 An EMI shall conduct annual penetration tests on its internal and external network infrastructure as well as IT systems including web, mobile and all external-facing applications. The penetration testing shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. An EMI shall engage suitably accredited penetration testers and third party service providers to perform this function.

S 29.9 An EMI shall establish standard operating procedures (SOP) for vulnerability assessment and penetration testing (VAPT) activities. The SOP shall outline the relevant control measures including ensuring the external penetration testers are accompanied on-premises at all times, validating the event logs and ensuring data purging.

S 29.10 An EMI shall ensure the outcome of the penetration testing exercise is properly documented and escalated in a timely manner to senior management to identify and monitor the implementation of relevant remedial actions.

Distributed Denial of Service (DDoS)

G 29.11 An EMI should ensure its technology systems and infrastructure, including IT systems outsourced to or hosted by third party service providers, are adequately protected against all types of DDoS attacks (including volumetric, protocol and application layer attacks) through the following measures–

(a) subscribing to DDoS mitigation services, which include automatic "clean pipe" services to filter and divert any potential malicious traffic away from the network bandwidth;

(b) regularly assessing the capability of the service provider to expand network bandwidth on-demand including upstream service provider capability, adequacy of the service provider's incident response plan and its responsiveness to an attack; and

(c) implementing mechanisms to mitigate against Domain Name Server (DNS) based layer attacks.

Data Loss Prevention (DLP)

G 29.12 An EMI should establish a clear DLP strategy and processes in order to ensure that proprietary and customer and counterparty information is identified, classified and secured. At a minimum, an EMI should–

(a) ensure that data owners are accountable and responsible for identifying and appropriately classifying data;
(b) undertake a data discovery process prior to the development of a data classification scheme and data inventory; and
(c) ensure that data accessible by third parties is clearly identified and policies should be implemented to safeguard and control third party access. This includes having in place adequate contractual agreements to protect the interests of the EMI and its customers.

G 29.13 An EMI should design internal control procedures and implement appropriate technology in all applications and access points to enforce DLP policies and trigger any policy violations. The technology deployed should cover the following–
(a) data in-use – data being processed by IT resources;
(b) data in-motion – data being transmitted on the network; and
(c) data at-rest – data stored in storage mediums such as servers, backup media and databases.

G 29.14 An EMI should implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorised access to data.

Security Operations Centre (SOC)

S 29.15 An EMI shall ensure its SOC, whether managed in-house or by third party service providers, has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the EMI to detect anomalous user or network activities, flag potential breaches and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts. The outcome of the SOC activities shall also inform the EMI's reviews of its cybersecurity posture and strategy.

G 29.16 The SOC should be able to perform the following functions–
(a) log collection and the implementation of an event correlation engine with parameter-driven use cases such as Security Information and Event Management (SIEM);
(b) incident coordination and response;
(c) vulnerability management;
(d) threat hunting;
(e) remediation functions including the ability to perform forensic artifact handling, malware and implant analysis; and
(f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify

anomalies that may pose security threats including at endpoints and network layers.

G 29.17 An EMI should ensure that the SOC provides a regular threat assessment report, which should include, at a minimum, the following–

(a) trends and statistics of cyber events and incidents categorised by type of attacks, target and source IP addresses, location of data centres and criticality of applications; and

(b) intelligence on emerging and potential threats including tactics, techniques and procedures (TTP).

G 29.18 An EMI should subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and support the implementation of countermeasures.

S 29.19 An EMI shall ensure the following–

(a) the SOC is located in a physically secure environment with proper access controls; and

(b) the SOC operates on a 24x7 basis with disaster recovery capability to ensure continuous availability.

Cyber Response and Recovery

S 29.20 An EMI shall establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident.

G 29.21 An EMI should establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP should address the following–

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

(b) Detection and analysis: Ensure effective and expedient processes for identifying points of compromise, assessing the extent of damage and preserving sufficient evidence for forensics purposes;

(c) Containment, eradication and recovery: Identify and implement remedial actions to prevent or minimise damage to the EMI, remove the known threats and resume business activities; and

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

G 29.22 An EMI should conduct an annual cyber drill exercise to test the effectiveness of its CIRP, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third party service providers. The test scenarios should include scenarios designed to test–

(a) the effectiveness of escalation, communication and decision-making processes that correspond to different impact levels of a cyber-incident; and

(b) the readiness and effectiveness of CERT and relevant third party service providers in supporting the recovery process.

S 29.23 An EMI shall immediately notify the Bank of any cyber-incidents affecting the EMI. Upon completion of the investigation, the EMI is also required to submit a report on the incident to the Bank.

G 29.24 An EMI is strongly encouraged to collaborate and cooperate closely with relevant stakeholders and competent authorities in combating cyber threats and sharing threat intelligence and mitigation measures.

30 Technology audit

S 30.1 An EMI shall ensure that the scope, frequency and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.

S 30.2 The audit function shall be adequately resourced with relevant technology audit competencies and sound knowledge of the EMI's technology processes and operations.

G 30.3 An EMI should ensure its technology audit staff are adequately conversant with the developing sophistication of the EMI's technology systems and delivery channels.

S 30.4 An EMI shall establish a technology audit plan that provides appropriate coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation reviews of new or material enhancements of technology services.

G 30.5 The audit function (in the case of paragraph 30.2) may be enlisted to provide advice on compliance with and adequacy of control processes during the planning and development phases of new major products, systems or

technology operations. In such cases, the technology auditors participating in this capacity should carefully consider whether such an advisory or consulting role would materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.

31 Internal awareness and training

S 31.1 An EMI shall provide adequate and regular technology and cybersecurity awareness education for all staff in undertaking their respective roles, and measure the effectiveness of its education and awareness programmes. This cybersecurity awareness education shall be conducted at least annually by the EMI and should reflect the current cyber threat landscape.

G 31.2 An EMI should provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent to effectively perform their roles and responsibilities.

G 31.3 An EMI should provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

Question 7:
What are the potential challenges and the expected timeline for your institution to be able to meet the enhanced IT requirements specified under Part D?

PART E REGULATORY PROCESS

32 Notification

S 32.1 An EMI shall notify the Bank in writing, to the Director of Payments Oversight Department, of any proposed changes to its e-money business model that are significant or changes the risk profile of its business model within thirty (30) days prior to the effective date of the proposed changes.

S 32.2 An EMI shall notify the Bank within thirty (30) days prior to establishing or relocating its offices in or outside Malaysia[39].

S 32.3 An EMI shall notify the Bank within thirty (30) days prior to the appointment of an auditor[40].

S 32.4 An EMI shall notify the Bank on the appointment of its chairman, director or CEO, within seven (7) days from the date of appointment.

33 Submission requirements

S 33.1 An EMI shall submit monthly statistics on the operation of its e-money business to the Bank no later than the 15th day of the month following the reporting month using the format provided by the Bank, as well as, via the STATsmart online submission system.

S 33.2 An EMI shall submit independent audit reports of its e-money business, including IT audit, as and when required by the Bank.

S 33.3 An EMI shall submit to the Bank its audited financial statement on an annual basis no later than three (3) months after the financial year-end.

S 33.4 An EMI shall submit a written assurance from its external auditor on the adequacy of controls for its safeguarding methods in accordance with paragraph 16. The written assurance shall include a review of minimally, the following–

(a) the separation of funds collected from customers from the working capital funds of an EMI;

(b) the balance of the funds in the EMI's safeguarded account to ensure that the said balance is greater than or at least equal to the EMI's outstanding e-money liabilities;

[39] Pursuant to section 25(2) of the FSA or section 22(2) of the IFSA.
[40] Pursuant to section 67(3) of the FSA or section 76(3) of the IFSA.

(c) the effectiveness of the controls put in place by an EMI to ensure that the customer funds in the safeguarded account are topped up in a timely manner if the outstanding e-money liabilities of the EMI are greater than the funds in the safeguarded account; and

(d) the usage of the customer funds in the safeguarded account, to ensure the funds are only used for refund to customers, payment to merchants or payment to another e-money account or bank account arising from a credit transfer transaction.

S 33.5 The written assurance specified in paragraph 33.4 from the external auditor shall include the method of assessment and basis of opinion on the compliance level. An EMI shall ensure that the written assurance, together with details of the action plans and timelines to address any gaps identified, are deliberated at its board or board audit committee and submitted to the Bank on an annual basis no later than three (3) months after its financial year-end.

34 Disclosure requirement

S 34.1 An EMI shall publish[41] its audited financial statements, at least on their official website no later than six (6) months after its financial year-end.

35 Membership in the Financial Ombudsman Scheme

S 35.1 An EMI shall be a member of an approved FOS pursuant to regulation 3 of the Financial Services (Financial Ombudsman Scheme) Regulation 2015.

S 35.2 The membership of an EMI in the FOS shall commence on the date it begins its operation. An EMI shall notify the OFS on the commencement of its operations within seven (7) days from the date it begins its operations.

S 35.3 An EMI shall comply at all times with the terms of membership as set out in the terms of reference for the OFS.

S 35.4 For disputes within the OFS' jurisdiction, an EMI shall attach a copy of the OFS pamphlet[42] and include the following statement in the letter conveying the final decision on a dispute so that the customer may pursue the next course of action:

"If you are not satisfied with our decision, please refer your dispute to the Ombudsman for Financial Services (OFS) within six months from the date of our decision. The procedure for lodging a dispute with OFS is provided in the attached pamphlet on "Resolution of Financial Disputes".

[41] Pursuant to section 66(1) of the FSA and 75(1) of the IFSA.
[42] Available in OFS official website.

APPENDICES

Appendix 1 Criteria for eligible EMI

For the purpose of the definition of 'eligible EMI' under paragraph 5.2, an EMI is deemed to have 'substantial market presence' if it fulfils any of the following criteria–

(a) the EMI has at least 500,000 active users (i.e. with at least one financial transaction[43] per month) for a consecutive period of six months;
(b) the EMI has a market share of at least 5% of the total e-money transaction volume or transaction value in Malaysia for a given year beginning 2017; or
(c) the EMI has a market share of at least 5% of the total outstanding e-money liabilities in Malaysia for a given year beginning 2017.

The Bank reserves the right to add, vary, amend or remove the criteria set out above from time to time.

[43] This includes reloading of an e-money account, fund transfer or purchase transaction.

Appendix 2 Limited purpose e-money

A. Definition of limited purpose e-money

Limited purpose e-money refers to–

1. E-money used for payment at a network of merchants, a single premise or closed community

(1) Any e-money that is accepted as a means of making payment for–
  (a) goods or services under a network of merchants that belong to a single business network and operates under single brand;
  (b) goods or services within a physical premise[44]; or
  (c) a limited[45] range of goods or services within a closed community[46]; and

(2) the funds stored in the e-money account–
  (a) is or is intended to be used for payment of goods or services only in Malaysia;
  (a) shall not exceed RM250;
  (b) shall not be used for funds transfer; and
  (c) is not redeemable for cash, unless it is withdrawn to the customer's own bank account with a banking institution in Malaysia; and

(3) the total e-money issued shall have an average daily outstanding e-money liabilities and average monthly payment transaction value not exceeding RM1,000,000[47].

2. E-money used for cash rewards or loyalty points

(1) Any payment instrument, whether tangible or intangible, that–
  (a) stores cash rewards or loyalty points that are money's worth electronically, which is funded by the EMI or any other person who is under an arrangement with the EMI; and
  (b) is able to be used as means of making payment of goods or services to any person other than the EMI; and

(2) the stored cash rewards or loyalty points referred to under paragraph 2(1)(a)–

[44] Consist of the following:
  i) E-money accepted only by a merchant occupying a single premise (e.g. a grocery shop in location A). It cannot be accepted by the same/other merchant in other places; or
  ii) E-money accepted by multiple merchants occupying a single premise (e.g. a shopping complex with several merchants. It cannot be accepted by any other merchant in other places, other than in that particular shopping complex).

[45] Closely or functionally related/needed within a particular community (e.g. e-money accepted for payments at a canteen and bookstore in a school).

[46] Within a singular type of community or area where there are minimal changes in residents of the community or users (e.g. students in schools or colleges, residents in apartments, members in clubhouse).

[47] The amount shall be based on past or projected amount for a calendar year period.

(a) is issued to the customer of the EMI as a reward arising from the purchase of goods or the use of services provided by the EMI or any other person who is under an agreement with the EMI;
(b) is not redeemable for cash; and
(c) is stored in an account separated from the customer's e-money account

3. E-money used for refund purposes

(1) Any payment instrument, whether tangible or intangible, that–
(a) stores funds electronically, of which such funds are intended to be refunded to the user of the payment instrument by the issuer or any other person who is under an agreement with the issuer; and
(b) is able to be used as means of making payment of goods or services to any person other than the issuer; and

(2) the stored funds can be used for payment within the EMI's merchant network only;

(3) the stored funds has no expiry period; and

(4) the total e-money issued referred to paragraph 3(1)(a) shall have an average daily outstanding e-money liabilities not exceeding RM1,000,000[47].

4. Mobile prepaid airtime used for purchase of digital content

(1) Any payment instrument, whether tangible or intangible that–
(a) stores fund electronically in exchange of funds paid to the issuer;
(b) is able to be used as means of making payment for–
(i) telecommunication related services provided by the issuer or any other person who is under an agreement with the issuer; and
(ii) digital goods or services provided by any person other than the issuer, whereby such goods or services are limited to consumer related items with low transaction values such as ringtones, games and online movies.

(2) the payment for digital goods or services is made using any telecommunication, digital or IT device; and

(3) the digital goods or services are delivered to and are to be used through a telecommunication, digital or IT device.

B. Conditions to qualify for exemption of limited purpose e-money

A limited purpose EMI shall ensure that it complies with the following conditions imposed on limited purpose e-money–

1. In order to be qualified for exemption from requiring approval under section 11 of the FSA or IFSA and to operate as a limited purpose EMI, the limited purpose EMI shall satisfy the definition of limited purpose e-money at all times.

2. A limited purpose EMI shall submit a notification to the Bank on an annual basis, which includes–
   (a) a description of the limited purpose e-money, such as functionality and product features;
   (b) a description that demonstrates fulfilment of the definition and conditions of limited purpose e-money; and
   (c) an undertaking that the e-money qualifies for the exemption from section 11 of the FSA or IFSA.

   For limited purpose EMI that has yet to commence business operation, it shall submit the first notification at least one (1) month prior to operationalising the e-money scheme.

   For existing EMI that satisfy the limited purpose EMI, it shall submit the first notification within such period as may be specified by the Bank.

3. A limited purpose EMI shall submit to the Bank statistical information on the limited purpose e-money, which is attested by an external auditor[48] on an annual basis as follows–
   (a) total outstanding e-money liabilities;
   (b) number of registered and active users;
   (c) total transaction volume; and
   (d) total transaction value.

4. A limited purpose EMI shall comply with requirements under the Personal Data Protection Act 2010 and subsidiary legislation issued under the said Act at all times.

5. A limited purpose EMI shall provide clear and prominent disclosures to caution its users or potential users (i.e. the disclaimer must not be in fine notes through channels such as official websites, social media accounts and branches (if any)) that–
   (a) it is a limited purpose EMI exempted from requiring approval pursuant to section 11 of the FSA or IFSA; and
   (b) the operation of the limited purpose e-money scheme is not subjected to the relevant requirements made applicable to approved EMIs under the FSA or IFSA.

6. A limited purpose EMI shall provide users or potential users with clear information on the procedures to be followed in raising complaints or in the event of a dispute.

[48] Registered as an auditor of a public interest entity with the Audit Oversight Board.

7. A limited purpose EMI shall not be exempted from requiring approval under section 11 of the FSA or IFSA if–
   (a) the Bank considers that it is necessary in the public interest or in the interests of the users or potential users of the e-money to do so; or
   (b) the Bank is satisfied that the risks posed by the EMI are material–
      (i) to the users or potential users of the EMI; or
      (ii) on public confidence or integrity of the payment systems of Malaysia.

8. A limited purpose EMI that no longer satisfies the limited purpose e-money definition or has its exemption disqualified by the Bank shall submit to the Bank an application for approval under section 11 of the FSA or IFSA if it plans to continue issuing e-money.

Question 8:
An EMI that satisfies the definition of limited purpose e-money will be allowed to operate without requiring prior approval from the Bank under section 11 of the FSA or IFSA and will not be obligated to comply with the relevant provisions of the FSA or IFSA and standards applicable to EMIs. However, the said exemption is subject to the conditions specified in this Appendix 2. In this regard, please provide your views on the criteria of limited purpose e-money, the exemption conditions and the implications to your institution.

Appendix 3 Responsibilities of board committees

Board risk management committee

1. Support the board in overseeing the implementation of the EMI's risk management framework.

Board audit committee

1. Support the board in ensuring that there is a reliable and transparent financial reporting process within the EMI.
2. Oversee the effectiveness of the internal audit function of the EMI. At a minimum, this must include–
   (a) reviewing and approving the audit plan, scope, procedures and frequency;
   (b) reviewing audit reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with laws, regulatory requirements, policies and other problems identified by the internal audit and other control functions; and
   (c) establishing a mechanism to assess the performance and effectiveness of the internal audit function.
3. Foster quality audits of the EMI by exercising oversight over the external auditor. At a minimum, this must include–
   (a) making recommendations to the board on the appointment, removal and remuneration of the external auditor;
   (b) monitoring and assessing the independence of the external auditor including by approving the provision of non-audit services by the external auditor;
   (c) monitoring and assessing the effectiveness of the external audit, including by meeting with the external auditor without the presence of senior management at least annually;
   (d) maintaining regular, timely, open and honest communication with the external auditor, and requiring the external auditor to report to the board audit committee on significant matters; and
   (e) ensuring that senior management is taking necessary corrective actions in a timely manner to address external audit findings and recommendations.
4. Review and update the board on all related party transactions.
5. Review third-party opinions on the design and effectiveness of the EMI's internal control framework.

Appendix 4 Computation of capital funds

Share capital *which includes*–

- Paid-up ordinary shares/common stock
- Paid-up irredeemable non-cumulative preference shares

plus **Reserves** *which includes*–

- Share premium
- General reserve fund

less **Intangible Assets**[49]

plus **Retained Profit** (or *less* **Accumulated Losses)**

plus **Audited Profit for the period** (or *less* **Unaudited Loss for the period)**

[49] Including goodwill, capitalised development costs, licenses and intellectual properties.

Appendix 5 Examples of arrangements excluded from the scope of outsourcing

1. For the purpose of paragraph 18, arrangements which entail procurement of services[50], leveraging common industry-wide infrastructure driven by regulatory requirements, and involvement of third parties due to legal requirements, are generally not considered as outsourcing arrangements. These include–
   (a) services for the transfer, clearing and settlement of funds or securities provided by an operator of a designated payment system or an operator of an approved payment system under the FSA or IFSA;
   (b) global financial messaging network services provided by an operator that is owned by its member financial institutions and is subject to the oversight of relevant regulators;
   (c) independent consultancy service (e.g. legal opinions, tax planning and valuation);
   (d) independent audit assessment;
   (e) clearing and settlement arrangement between clearing houses and settlement institutions and their members;
   (f) agent banking;
   (g) trustee arrangement;
   (h) credit or market information services;
   (i) repair, support and maintenance of tangible assets;
   (j) purchase or subscription of commercially available software;
   (k) maintenance and support of licensed software;
   (l) marketing and advertising;
   (m) telecommunication, postal and courier service;
   (n) physical security, premise access and guarding services; and
   (o) catering, cleaning and event services.

[50] Where an EMI acquires services, goods or utilities which are not expected to be performed by the EMI.

Appendix 6 Minimum requirements on the outsourcing agreement

1. The outsourcing agreement shall, at a minimum, provide for the following–
   (a) duration of the arrangement with date of commencement and expiry or renewal date;
   (b) responsibilities of the service provider, with well-defined and measurable risk and performance standards in relation to the outsourced activity. Commercial terms tied to the performance of the service provider must not create incentives for the service provider to take on excessive risks that would affect the EMI;
   (c) controls to ensure the security of any information shared with the service provider at all times, covering at a minimum−
      (i) responsibilities of the service provider with respect to information security;
      (ii) scope of information subject to security requirements;
      (iii) provisions to compensate the EMI for any losses and corresponding liability obligations arising from a security breach attributable to the service provider;
      (iv) notification requirements in the event of a security breach; and
      (v) applicable jurisdictional laws;
   (d) continuous and complete access by the EMI to its data held by the service provider in the event of a dispute with the service provider, or termination of the arrangement;
   (e) ability of the EMI and its external auditor[51] to conduct audits and on-site inspections on the service provider and its sub-contractors, and to obtain any report or finding made in relation to the outsourced activity;
   (f) notification to the EMI of adverse developments that could materially affect the service provider's ability to meet its contractual obligations;
   (g) measures that the service provider would take to ensure continuity of the outsourced activity in the event of an operational disruption or failure on the part of the service provider;
   (h) regular testing of the service provider's BCP, including specific testing that may be required to support the EMI's own BCP testing, and a summary of the test results to be provided to the EMI with respect to the outsourced activity;
   (i) the dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant;
   (j) circumstances that may lead to termination of the arrangement, the contractual parties' termination rights and a minimum period to execute the termination provisions, including providing sufficient time for an orderly transfer of the outsourced activity to the EMI or another party;

[51] Including an agent appointed by the EMI.

(k) where relevant, terms governing the ability of the primary service provider to sub-contract to other parties. Sub-contracting should not dilute the ultimate accountability of the primary service provider to the EMI over the outsourcing arrangement, and the EMI must have clear visibility over all sub-contractors[52]. Therefore, the outsourcing agreement between the EMI and primary service provider must stipulate the following–

(i) the accountability of the primary service provider over the performance and conduct of the sub-contractor in relation to the outsourcing arrangement;

(ii) the rights of the EMI to terminate the outsourcing agreement in the event of excessive reliance on sub-contracting (e.g. where the sub-contracting materially increases the risks to the EMI);

(iii) the requirement for the sub-contractor and its staff to be bound by confidentiality provisions even after the arrangement has ceased; and

(iv) use of information shared with the service provider is limited to the extent necessary to perform the obligations under the outsourcing agreement.

[52] In this respect, the primary service provider must provide sufficient notice to the EMI before entering into an agreement with the sub-contractor.

Appendix 7 Storage and transportation of sensitive data in removable media

An EMI should ensure adequate controls and measures are implemented for the storage and transportation of sensitive data in removable media, including–

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

Appendix 8 Control measures on Internet application

1. An EMI should ensure the adequacy of security controls implemented for Internet application, which include to–
   (a) ensure Internet application only runs on secured versions of web browsers that have continued developer support for security patches to fix any vulnerabilities; and
   (b) put in place additional authentication protocols to enable customers to identify the EMI's genuine websites.

Appendix 9 Control measures on mobile application and devices

1. An EMI should ensure digital payment services involving sensitive customer and counterparty information offered via mobile devices are adequately secured. This includes the following–
   (a) ensure mobile applications run only on the supported version of operating systems and enforce the application to only operate on a secure version of operating systems which have not been compromised, jailbroken or rooted (i.e. the security patches are up-to-date);
   (b) design the mobile application to operate in a secure and tamper-proof environment within the mobile devices. The mobile application shall be prohibited from storing customer and counterparty information used for authentication with the application server such as PIN and passwords. Authentication and verification of unique key and PIN shall be centralised at the host;
   (c) undertake proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;
   (d) ensure proper controls are in place to access, maintain and upload the mobile application on application distribution platforms;
   (e) activation of the mobile application must be subject to authentication by the EMIs;
   (f) ensure secure provisioning process of mobile application in the customer's device is in place by binding the mobile application to the customer's profile such as device ID and account number; and
   (g) monitor the application distribution platforms to identify and address the distribution of fake applications in a timely manner.

2. In addition to the guidance in paragraph 1, an EMI should also ensure the following measures are applied specifically for applications running on mobile devices used by the EMIs, appointed parties or intermediaries for the purpose of processing customer and counterparty information–
   (a) mobile device to be adequately hardened and secured;
   (b) ensure the capability to automatically wipe data stored in the mobile devices in the event the device is reported stolen or missing; and
   (c) establish safeguards that ensure the security of customer and counterparty information (e.g. Primary Account Numbers (PAN), Card Verification Value Numbers (CVV), expiry dates and Personal Identification Numbers (PIN) of payment cards), including to mitigate risks of identity theft and fraud[53].

[53] This includes risks associated with malwares that enable keystroke logging, PIN harvesting and other malicious forms of customer and counterparty information downloading.

Appendix 10 Control measures on QR code

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

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

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

Appendix 11 Control measures on cybersecurity

1. Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings.
2. Update checklists on the latest security hardening of operating systems.
3. Update security standards and protocols for web services encryption regularly. Disable support of weak ciphers and protocol in web-facing applications.
4. Ensure technology networks including mobile and wireless networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including firewall and Intrusion Prevention System (IPS).
5. Ensure security controls for server-to-server external network connections include the following–
   (a) server-to-server authentication such as Public Key Infrastructure (PKI) certificate or user ID and password;
   (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and
   (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.
6. Ensure security controls for remote access to server include the following–
   (a) restrict access to only hardened and locked down end-point devices;
   (b) use secure tunnels such as TLS and VPN IPSec;
   (c) deploy “gateway” server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and
   (d) close relevant ports immediately upon expiry of remote access.
7. Ensure overall network security controls are implemented including the following–
   (a) dedicated firewalls at all segments. All external-facing firewalls must be deployed on High Availability (HA) configuration and “fail-close” mode activated. Deploy different brand name/model for two firewalls located in sequence within the same network path;
   (b) IPS at all critical network segments with the capability to inspect and monitor encrypted network traffic;
   (c) web and email filtering systems such as web-proxy, spam filter and anti-spoofing controls;
   (d) end-point protection solution to detect and remove security threats including viruses and malicious software;
   (e) solution to mitigate advanced persistent threats including zero-day and signatureless malware; and
   (f) capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.
8. Synchronise and protect the Network Time Protocol (NTP) server against tampering.