BANGLADESH BANK

REGULATIONS FOR E-MONEY IN BANGLADESH

PAYMENT SYSTEMS DEPARTMENT

PART I: INTRODUCTION AND SCOPE

1 Short Title and Commencement

1.1 These Regulations shall be called the Regulations for E-Money in Bangladesh.

1.2 Existing mobile financial services and payment service providers that have previously been offering mobile financial services, bank-led or not, or e-money services must apply within six (6) months of the coming into effect of these Regulations, for an approval in order to conform to the new framework.

2 Preamble and Objectives

These Regulations are issued by Bangladesh Bank pursuant to its mandate under পরিশোধ ও নিষ্পত্তি ব্যবস্থা আইন, ২০২৪ (২০২৪ সনের ৯নং আইন) to promote, regulate, and supervise safe and efficient payment systems and payment services. These Regulations for e-money is set out by the Bangladesh Bank are aimed at achieving the following objectives:

2.1 Promote financial inclusion and extend financial services beyond traditional channels with due consideration to the safety and soundness of the financial system;

2.2 Create an enabling and competitive regulatory environment for convenient, efficient, and safe retail payment and funds transfer mechanisms;

2.3 Ensure that electronic money is only provided by duly licensed e-money issuers which are engaged solely in the business of e-money and activities related or incidental to the business of e-money and which are regulated and supervised by the Bangladesh Bank;

2.4 Ensure the safety and reliability of e-money issued and preserve customer and merchant confidence;

2.5 Specify necessary safeguards and controls to mitigate risks associated with e-money business, including AML/CFT risks;

2.6 Ensure consumer protection, adequate transparency, fair treatment, and effective recourse for customers.

3 Scope of Application

These Regulations apply to all entities authorized or licensed by Bangladesh Bank to issue e-money in Bangladesh. This includes, but is not limited to:

3.1 Payment Service Providers (PSPs) licensed by Bangladesh Bank that issue e-money.

3.2 Mobile Financial Service (MFS) Providers licensed by the Bangladesh Bank in Bangladesh.

3.3 Other categories of institutions permitted by Bangladesh Bank to issue e-money.

4 Exclusions

These Regulations may not apply to payment instruments usable only within the issuer's premises or a strictly limited network/range of goods ("closed loop" systems), unless otherwise specified.

PART II: DEFINITIONS AND INTERPRETATIONS

5 Key Terms

In these Regulations, unless the context otherwise requires, the words and expressions used herein shall have the same meanings assigned to them in the Payment and Settlement Systems Act, 2024, and,

5.1 "agent" means a person appointed by an e-money issuer to perform agency services on its behalf;

5.2 "agency services" means the registration of new e-money account holders on behalf of an e-money issuer and shall include services incidental to the performance of these services;

5.3 "AML/CFT" means Anti-Money Laundering and Combating the Financing of Terrorism;

5.4 "Authorized EMI" means a regulated financial institution that has been authorized to carry-out e-money business under **Paragraph** 8 of these Regulations;

5.5 "cash-in" means accepting banknotes or coins and performing the necessary steps to initiate the crediting of that monetary value to the customer's e-money account;

5.6 "cash-out" means giving out banknotes or coins and performing the necessary steps to initiate the debiting of that monetary value from the customer's e-money account;

5.7 "complete application" means the submission of all required documents needed to process an application/authorization;

5.8 "customer due diligence" (CDD) means the process of obtaining customer information and verifying/assessing the value of the information from independent and reliable sources to identify the customer upfront, as well as to detect, monitor and report suspicious activity;

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

5.10 "Dedicated EMI" or "DEMI" means a legal person that has been licensed under **Paragraph 9** of these Regulations;

5.11 "electronic money" or "e-money" means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds, redeemable against cash and accepted by a natural or legal person other than the e-money issuer;

5.12 "e-money account" means the account held by an e-money holder with an e-money issuer for conducting e-money transactions and/or for cash-in/cash-out transactions;

5.13 "e-money business" means the issuance, transfer, payment and redemption of electronic money, and any other activity permitted under these Regulations and by the Bangladesh Bank.

5.14 "e-money float" or "float" means the total outstanding e-money liabilities of the e-money issuer to its customers at any point in time;

5.15 "e-money holder" means a person who has a claim on an e-money issuer for e-money issued by e-money issuer;

5.16 "e-money issuer" or "EMI" means an entity issuing e-money and could be either a Dedicated EMI licensed under these regulations or a financial institution regulated under the Bank Company Act, 1991, and authorized under these Regulations;

5.17 "e-money user" means a person who uses e-money for making financial transactions either with or without opening an e-money account;

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

5.19 "KYC" means Know Your Customer;

5.20 "merchant" means a commercial establishment where customers are able to pay for goods and services using e-money;

5.21 "mobile financial services (MFS)" refers to an e-money issuer under these Regulations and shall be known henceforth as an Authorized EMI or a Dedicated EMI, depending on its corporate structure, and are permitted to perform all permissible activities under **Paragraph** 44;

5.22 "MSISDN" means Mobile Station International Subscriber Directory Number;

5.23 "over-the-counter transaction" or "OTC transaction" refers to a transaction conducted by a customer with an EMI or its agents in cash without making use of an e-money account held in their own name. The sub-set of OTC transactions for which this applies to both sender and recipient shall be called "Cash-to-cash" or "C2C" transactions;

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

5.25 "outsourcing arrangement" refers to an arrangement in which a service provider performs an activity on behalf of EMI on a continuing basis (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), where the activity would otherwise be undertaken by the EMI but does not include activities set out in Appendix 2;

5.26 "outstanding e-money liabilities" refers to:

5.26.1 the unutilized amount of e-money which has been issued; and

5.26.2 the utilized amount of e-money which is pending payment to merchants;

5.27 "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;

5.28 "payment service provider" means an e-money issuer licensed under these Regulations and permitted to carry out the activities specified in **Paragraph**s 44 except 44.2.4 & 44.2.5.

5.29 "real-time" means the electronic processing of transactional data instantaneously;

5.30 "regulated financial institution" or "RFI" means a financial institution regulated under the Bank Company Act, 1991;

5.31 "significant shareholding" means a direct or indirect holding which

5.31.1 represents ten per cent or more of the capital or of the voting right; or

5.31.2 makes it possible to exercise a significant influence over the management of the entity in which a holding exists.

5.32 "significant owners" are such owners that have significant shareholding in an entity;

5.33 "scheduled bank" means a bank licensed by the Bangladesh Bank under the Bank Company Act, 1991, to carry out the business of banking;

5.34 "trust and settlement account" means a special account required for EMIs issuing e-money in Bangladesh to hold customer funds awaiting transfer or collection;

5.35 "trust fund" means any fund held by an EMI that creates a liability of the service providing entity to its customers/participants;

5.36 "wallet limit" means the maximum monetary value that can be stored in an e-money account.

6 Repeals and Savings

These Regulations do not, in general, supersede or revoke any of the existing laws, rules and regulations.

PART III: LICENSING AND AUTHORIZATION

7 Areas and Limitations of Regulations

7.1 No person other than a regulated financial institution authorized under these Regulations or a Dedicated EMI shall conduct the business of an e-money issuer unless that person is authorized to do so under these Regulations.

7.2 These Regulations apply to all issuers of e-money licensed or authorized under these Regulations or existing e-money issuers duly licensed or authorized by Bangladesh Bank.

7.3 These Regulations do not apply to payment instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a strictly limited network of service providers or for a strictly limited range of goods or services (usually referred to as "closed loop" systems).

7.4 These Regulations apply to prepaid cards, to the extent that the value stored on such cards falls under the definition of electronic money as per **Paragraph** 5.11 and are not explicitly exempt as per **Paragraph** 7.3 above.

7.5 The issuance of e-money does not constitute the business of banking pursuant to the Bank Company Act, 1991, and hence on its own does not lead to a licensing requirement under the Bank Company Act, 1991.

8 Authorization of E-Money Issuers

8.1 Any financial institution regulated under the Bank Company Act, 1991, wishing to issue e-money shall make an application to the Bangladesh Bank for authorization in the form prescribed below.

8.2 An application under this clause shall set out the nature and functionality of the proposed e-money operations that will be made available to e-money holders and shall contain sufficient information to enable the Bangladesh Bank to evaluate the requirements.

8.3 Without limiting the generality of the foregoing, the application shall contain:

8.3.1 Proposed e-money services to be offered;

8.3.2 A business plan for its proposed e-money operations covering at a minimum, the subsequent three years and indicating the intended initial geographical coverage of the service, including agent coverage, as well as its expansion over time;

8.4 Bangladesh Bank undertakes to respond with authorization or refusal within one-eighty (180) calendar days from receipt of the complete application.

8.5 Any applicant for such authorization whose application has been refused under **Paragraph** 8.4 above may, within thirty (30) calendar days from the date on which the refusal is communicated, appeal against the decision to the Governor of Bangladesh Bank.

8.6 A regulated financial institution (RFI) which carries on the business of e-money issuance without authorization from the Bangladesh Bank commits an offence and shall be liable to a fine of not less than Taka 50 lakhs payable to Bangladesh Bank.

8.7 A person who contravenes **Paragraph** 8.6 above shall immediately cease the issuance of e-money and seek the authorization of the Bangladesh Bank.

9 Licensing of Dedicated EMIs

9.1 In order to conduct business as Dedicated EMIs, entities shall make an application to the Bangladesh Bank for licensing, along with a "no objection certificate", if relevant, from the regulating body they are affiliated to. The application shall be accompanied by a nonrefundable application fee as may be prescribed by Bangladesh Bank from time to time. The approval process typically involves two phases.

9.1.1 Phase 1 (Letter of Intent): Issuance of letter of intent to set up the infrastructure, based on evaluation of submitted documents and proposals.

9.1.2 Phase 2 (License): Issuing a license to commence operations after the infrastructure is ready and satisfactory on-site inspection is conducted.

9.1.3 If a company licensed under paragraph 9.1.2 as a Payment Service Provider and the said PSP wants to convert to a dedicated e-money issuer to provide all the services specified in paragraph 44, it must first meet the capital requirements and fulfill the Phase 2 conditions before getting the DEMI license.

9.2 An application under this clause shall set out the nature and functionality of the proposed e-money operations that will be made available to e-money holders and shall contain sufficient information to enable the Bangladesh Bank to evaluate the requirements.

9.3 Without limiting the generality of the foregoing, the application shall contain:

9.3.1 Identifying information about the applicant and his/her business organization;

9.3.2 Identifying information for any and all bank accounts to be used in the conduct of e-money operations;

9.3.3 Company documents such as Memorandum and Articles of Association, Certificate of Incorporation, Trade License, e-TIN, BIN, Corporate Profile, etc.

9.3.4 A list of the current or proposed significant owners of the applicant, profile of significant owners and details of their kinship, and the percentages of shares owned or to be owned by each;

9.3.5 Governance and management details such as organizational structure, identity/suitability of directors and key management, evidence of their good repute and experience, CIB clearance, etc.;

9.3.6 A business plan with detailed description of services, business case analysis, market analysis, execution plan, initial and future geographical/agent coverage covering at a minimum period of the subsequent three years as well as its expansion over time;

9.3.7 Details of capital structure and financial soundness including information on paid-up capital, source of funds, budget forecasts, etc.;

9.3.8 Operational and risk management plans including the policies and procedures for risk management, AML/CFT, KYC, internal controls, business continuity management, disaster recovery plan, IT risk management, security measures, dispute management, policies for agent services, etc.;

9.3.9 Safeguarding arrangements such as description of measures to safeguard funds, including Trust and Settlement Account details;

9.3.10 Details of technology infrastructure such as description of technology, process flow, hardware/software details, network plan, proposed data center/disaster recovery, user capacity,

9.4 The Bangladesh Bank shall not authorize a person[1] as a Dedicated EMI unless the person complies with the following requirements:

9.4.1 The person is established and incorporated as a limited liability company under the Companies Act, 1994, in Bangladesh;

9.4.2 The person shall include in their Articles of Association language to the effect that e-money owed to their customers are purely held in trust and will not be encumbered in the case of insolvency or liquidation of the EMI.

9.4.3 The significant owners and ownership structure are suitable;

9.4.4 The board of directors adequately reflects the balance of interests represented by the Dedicated EMI, in particular that the company will hold funds in trust on behalf of e-money holders;

9.4.5 The person engages only in the business of e-money and other activities related or incidental to the business of e-money, such as money transfer/remittance;

9.4.6 The person is financially sound;

9.4.7 The individuals proposed to manage or control the Dedicated EMI are fit and proper and have the necessary experience and qualifications to perform their functions;

[1] The use of "person" here and in 4a) 4b) 4e) and 4f) refers to a legal person

9.4.8 The following minimum systems and controls are in place:

9.4.8.1 Sound and prudent management, administrative and accounting procedures and adequate internal control systems;

9.4.8.2 Appropriate and tested technology systems;

9.4.8.3 Appropriate security policies and measures intended to safeguard the integrity, authenticity and confidentiality of date and operating processes;

9.4.8.4 Adequate business continuity and disaster recovery plan; and

9.4.8.5 An effective audit function to provide periodic review of the security control environment and critical systems.

9.4.9 Any other requirement that the Bangladesh Bank may prescribe.

9.5 Without limiting the generality of the foregoing, the Bangladesh Bank may reject the application for a license on any of the following grounds:

9.5.1 The applicant or any of its significant owners has been convicted of a crime involving a financial transaction in any jurisdiction within the past ten (10) years or is a convicted felon;

9.5.2 The application contains false information;

9.5.3 The applicant fails to respond to a request from the Bangladesh Bank for additional information within ten (10) days of a second request for the same information;

9.5.4 The documents submitted are incomplete, deceptive or misleading.

9.6 Bangladesh Bank undertakes to respond with licensing or refusal within one hundred eighty (180) calendar days from receipt of the complete application.

9.7 Any applicant for a license as a Dedicated EMI whose application has been refused under **Paragraph** 9.5 may, within thirty (30) calendar days from the date on which the refusal is communicated, appeal against the decision to the Governor of Bangladesh Bank.

9.8 A person who carries on the business of e-money without a license from the Bangladesh Bank commits an offence and is liable on summary conviction:

9.8.1 In the case of a corporate body or other body of persons, to a fine of not less than Taka 50 lakhs;

9.8.2 In the case of an individual, to a fine of not less than Taka 50 lakhs.

9.8.3 Bangladesh Bank preserves the discretion in the issuance of a license or approval.

PART IV: GOVERNANCE, INTERNAL CONTROLS, AND RISK MANAGEMENT

10 Governance Arrangements

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

10.1 a board of directors (the board) and senior management that consists of people with caliber, credibility and integrity;

10.2 clearly defined and documented organizational arrangements, such as ownership and management structure; and

10.3 segregation of duties and control function to reduce potential mismanagement, conflict of interest, and fraud.

11 Board of Directors

11.1 The board must have a board charter that sets out the mandate, responsibilities and procedures of the board and its committees, including the matters reserved for the board's decision. The board shall be responsible for strategic decisions, effective oversight, compliance and internal control functions.

11.2 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 consideration of the long-term implications of the board's decisions on the EMI and its customers, employees, officers and the general public. In fulfilling this role, the board must—

11.2.1 approve the risk appetite, business plans and other initiatives which would, individually or collectively, have a material impact on the EMI's risk profile;

11.2.2 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;

11.2.3 oversee the implementation of the EMI's governance framework and internal control framework, and periodically review whether these remain appropriate in light of material changes to the size, nature and complexity of the EMI operations;

11.2.4 promote, together with senior management, a sound corporate culture within the EMI, which reinforces ethical, prudent and professional conduct and behavior;

11.2.5 oversee and approve business continuity plans, as well as exit plan, and ensure such plans are periodically reviewed and 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

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

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

11.3.1 ensure that appropriate procedures are in place to govern the board's operations;

11.3.2 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;

11.3.3 encourage healthy discussion and ensure that dissenting views can be freely expressed and discussed; and

11.3.4 lead efforts to address the board's developmental needs.

11.4 A director must fulfil the minimum requirements set out in **Paragraph**s 11.5 to 11.6 at the time of his appointment and on a continuing basis throughout the appointment period.

11.5 An EMI shall only appoint as its director, a person who has been assessed by the EMI to have complied with the fit and proper requirements specified by the Bangladesh Bank.

11.6 A Dedicated EMI shall establish a board of directors with a minimum of five (5) members, at least forty percent of the members shall be resident in Bangladesh.

11.7 For a Dedicated EMI, no less than one-fourth of the Board members shall be independent directors.

11.8 The board must determine whether an individual to be appointed as an independent director is independent in character and judgment, and free from associations or circumstances that may impair the exercise of his independent judgment. An individual must not be considered to be an independent director if that individual—

11.8.1 is or had been an executive director in the EMI or any of its affiliates in the last two (2) years;

11.8.2 is a substantial shareholder, or acting on behalf of the substantial shareholder, of the EMI or any of its affiliates in the last two (2) years; or

11.8.3 had a significant business or other contractual relationship with the EMI or any of its affiliates in the last two (2) years.

11.9 For the purpose of **Paragraph** 11.8, the board must clearly define what constitutes a "significant business or other contractual relationship", taking into account the nature, size and complexity of the EMI's operations.

11.10 At a minimum, a Dedicated EMI shall establish the following board committees:

11.10.1 board audit committee; and

11.10.2 board risk management committee.

11.11 A Dedicated EMI may combine its board audit committee and board risk management committee; The board committee shall-

11.11.1 not be chaired by the chairman of the board;

11.11.2 have at least three (3) directors of the EMI as members of the board committee;

11.11.3 have at least one-forth of independent directors of the EMI as members of the board committee; and

11.11.4 may be chaired by an independent director.

11.12 Each board committee shall have its Terms of Reference and shall assume the specific responsibilities enumerated for it in **Appendix 1**.

11.13 In the case of an Authorized EMI, the construct of the Board of Directors and its committees will be executed following the prevailing rules and regulations as may be specified in the Bank Company Act, 1991, and other guidelines, regulations, and circulars issued by the Bangladesh Bank.

12 Senior Management

12.1 An EMI shall only appoint as its senior management, a person who has been assessed by the EMI to have complied with the fit and proper requirements specified by the Bangladesh Bank.

12.2 An EMI shall not appoint its substantial shareholder as its senior management. 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.

12.3 A CEO must devote the whole of his professional time to the service of the EMI and shall have his principal or only place of residence within Bangladesh unless the Bangladesh Bank approves otherwise.

12.4 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.

12.5 The senior management of an EMI is responsible for ensuring the following:

12.5.1 effective policies and procedures are established and implemented for, among others, the following areas–

12.5.1.1 risk management and appropriate controls to manage and monitor risks;

12.5.1.2 due diligence and oversight to manage arrangements with service providers supporting the e-money operations;

12.5.1.3 sufficient and timely reporting or escalation of issues to the board;

12.5.2 overseeing the formulation and effective implementation of any business or strategic plan, including the strategic technology plan and associated technology policies and procedures;

12.5.3 robust decision-making processes with adequate consideration on customers' interests; and

12.5.4 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.

12.6 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.

12.7 For the purpose of **Paragraph** 12.6, an EMI shall ensure that a designated staff who does not engage in day-to-day technology operations shall be responsible for the identification, assessment and mitigation of technology risks.

13 Control Function

13.1 The board and senior management are encouraged to create an environment, which—

13.1.1 ensures that the EMI and its officers comply with legal and regulatory requirements;

13.1.2 adopts relevant risk management practices; and

13.1.3 encourages ethical conduct that underlies the legal and regulatory requirements.

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

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

13.2.2 ensure that the control functions are established and sufficiently resourced, with the officers[2] accorded with appropriate stature, authority and independence;

13.2.3 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;

13.2.4 provide the relevant officers with direct and unimpeded access to the board; and

13.2.5 where the risk management officer and compliance officer are the same person or performs the responsibilities of other control functions except for internal audit, be satisfied that a sound overall control

[2] Compliance, risk management and internal audit officer.

environment will not be compromised by the combination of responsibilities performed by the officer.

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

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

13.3.2 establish a control function commensurate with the size, nature of operations and complexity of the EMI, having regard to the requirements in **Paragraph**s 13.4 to 13.7;

13.3.3 provide sufficient resources for the control function, including officers with the appropriate competencies and experience;

13.3.4 ensure that the person performing the control function is kept informed of any organizational developments to facilitate the timely identification of compliance risk;

13.3.5 report to the board regularly on compliance or risk issues, and promptly on any material incidents of non-compliance; and

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

13.4 An EMI shall organize 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.

13.5 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.

13.6 Where two or more control function responsibilities (excluding internal audit) are performed by one officer, senior management must ensure that officer has the capacity and expertise to deliver his broader mandates while providing adequate focus to his control function responsibilities.

13.7 Where two or more control function responsibilities (excluding internal audit) are performed by one officer, 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.

14 Compliance Requirements

14.1 An e-money issuer shall put in place systems that have built-in control mechanisms for a complete audit trail. These control mechanisms include, but are not limited to:

14.1.1 Complete records of e-money accounts opened including the balances;

14.1.2 Identifying e-money users including OTC users;

14.1.3 Tracking and monitoring of all e-money transactions undertaken by e-money users and the individual and aggregate balances held by e-money holders;

14.1.4 Internal policies, procedures and accountability structures pertaining to Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT);

14.1.5 Automatic alerts and flags on suspicious transactions;

14.1.6 Detection of patterns of transactions.

14.2 An e-money issuer shall keep records of every e-money transaction processed by it for a period of not less than twelve (12) years.

14.3 E-money issuers shall ensure that they have systems that provide adequate data protection and data integrity.

14.4 The compliance officer shall identify and assess the compliance risk associated with an EMI's activities. This requires the compliance officer 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.

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

14.5.1 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;

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

14.5.3 an assessment of the impact (both financial and non-financial) of such incidents of non-compliance and deficiencies on the EMI (for example, fines, administrative enforcement or disciplinary actions taken by any regulatory authority against the EMI or its officers);

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

14.5.5 a record of corrective measures already taken and an assessment of the adequacy and effectiveness of such measures.

14.6 The compliance officer shall ensure that the reports referred to in **Paragraph** 14.5 are readily available to the internal audit function of the EMI, the Bangladesh Bank and other relevant regulatory or law enforcement authorities upon request.

14.7 Failure to comply with the provisions under this **Paragraph** shall impose a fine of Taka 10 (Ten) lac.

15 Risk Management

15.1 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 (MIS) that facilitates timely and reliable reporting of risks.

15.2 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.

15.3 The risk management officer must report to the board and senior management on a regular basis on the assessment of 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 Bangladesh Bank and other regulatory authorities upon request.

16 Internal Audit

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

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

16.3 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 assess whether the said functions are working effectively.

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

17 Business Continuity Management

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

17.2 An EMI must undertake a structured risk assessment process to—

17.2.1 identify potential threats that could cause material business disruptions, resulting in inability to fulfil business obligations; and

17.2.2 assess the likelihood of the identified threats occurring and determine the impact on the EMI.

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).

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.

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

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

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 Arrangements

18.1 Subject to the compliance of the Section 9 of Payment and Settlement System Act, 2024 (Act No. 9 of 2024), an e-money issuer may contract a third-party service provider to perform activities relating to the e-money business, including:

18.1.1 Technology platform;

18.1.2 Internal Audit and Risk Management functions

18.1.3 Recruitment and registration of customers;

18.1.4 Selection and/or training of agents;

18.1.5 Management of agents, e.g. monitoring, branding or liquidity management;

18.1.6 Sales and marketing;

18.1.7 Provision and/or maintenance of equipment.

18.2 Such outsourcing shall comply in full with these Regulations as well as with any other Regulations that the Bangladesh Bank may issue hereafter.

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

18.4 An EMI shall obtain the Bangladesh Bank's prior written approval before—

18.4.1 entering into a new material outsourcing arrangement; or

18.4.2 making material changes to an existing material outsourcing

arrangement.

18.5 For the purpose of **Paragraph** 18.4, in assessing whether an outsourcing arrangement is material, an EMI shall take into consideration the following factors:

18.5.1 significance of the outsourcing activity in facilitating the EMI to achieve its strategic and business objectives;

18.5.2 impact on the EMI's continuing ability to meet its obligations to its customers and counterparties in the event the service provider fails to provide the service or encounters a breach of data confidentiality or security;

18.5.3 aggregate exposure to a particular service provider in cases where the EMI, including any affiliates, outsources multiple activities to the same service provider; or

18.5.4 complexity of the outsourcing arrangement and number of parties involved, in particular where the service is sub-contracted or where more than one service provider collaborates to deliver an end-to-end outsourcing solution.

18.6 The board shall review and approve any new material outsourcing arrangement considered by the EMI or any material changes to an existing material outsourcing arrangement, before the proposal is submitted to the Bangladesh Bank for approval.

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

18.7.1 availability of sufficient expertise within the EMI to oversee and manage the outsourcing relationship; and

18.7.2 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—

18.7.2.1 the outsourcing of such processes does not take away the critical decision-making function of the EMI;

18.7.2.2 the outsourcing of such processes does not threaten strategic flexibility and internal control framework of the EMI;

18.7.2.3 the outsourcing of such processes would not impair the reputation, integrity and credibility of the EMI; and

18.7.2.4 processes are in place for the EMI to retain the continuous ability to comply with the regulatory and supervisory requirements on the outsourced functions.

18.8 An EMI shall have a contingency plan or arrangements to secure business continuity in the event the outsourcing arrangement is suddenly terminated. This is to mitigate any major business disruption that may occur as a result of the termination of the outsourcing arrangement. 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 outsourcing arrangement.

18.9 An EMI shall require the service provider to report to the EMI and the EMI shall monitor the service provider to ensure that the integrity and quality of work conducted by the service provider is maintained.

18.10 An EMI shall ensure that periodic independent reviews are conducted on the outsourced arrangement to monitor the performance of service providers. The reviews shall be done either by the EMI's internal and/or external auditors, or independent reports shall be made available by the service providers, with the same scope of review as if the said operations are conducted in-house.

18.11 An EMI shall ensure that any weaknesses highlighted during the review under **Paragraph** 18.10 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.

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

18.12.1 capacity, capability, financial strength and business reputation. This includes an assessment whether the service provider is a going concern and has strong governance structures to manage the outsourced activity throughout the duration of the arrangement;

18.12.2 risk management and internal control capabilities, including physical and IT security controls, and BCM. This includes the ability of the service provider to respond to service disruptions or problems resulting from natural disasters and physical or cyber-attacks, within an appropriate timeframe;

18.12.3 the location of the outsourced activity (e.g. city and country), including primary and back-up sites;

18.12.4 access rights of the EMI and the Bangladesh Bank to the service provider;

18.12.5 measures and procedures to ensure data protection and confidentiality;

18.12.6 reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chain of the outsourcing arrangement;

18.12.7 undue risks[3] resulting from similar business arrangements, if any, between the service provider and the EMI;

[3] 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.

18.12.8 the extent of concentration risk to which the EMI is exposed with respect to a single service provider and 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

18.12.9 ability of the service provider to comply with relevant laws, regulations and requirements in this document.

18.13 In performing due diligence on an affiliate, an EMI shall make an objective assessment of the affiliate's ability to perform the outsourced activity guided by the considerations listed in **Paragraph** 18.12.

18.14 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.

18.15 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 3.

18.16 The outsourcing agreement must also contain provisions which–

18.16.1 enable the Bangladesh Bank to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity;

18.16.2 enable the Bangladesh Bank to conduct on-site supervision of the service provider where the Bangladesh Bank deems necessary;

18.16.3 enable the Bangladesh 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 Bangladesh Bank deems necessary; and

18.16.4 allow the EMI the right to modify or terminate the arrangement when the Bangladesh Bank issues a direction to the EMI to that effect.

18.17 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—

18.17.1 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;

18.17.2 all locations (e.g. city and country) where information is processed or stored by the service provider, including back-up locations, are made known to the EMI;

18.17.3 where the service provider is located, or performs the outsourced activity outside Bangladesh, the service provider is subject to data protection standards that are at a minimum comparable to Bangladesh;

18.17.4 where the service provider provides services to multiple clients, the EMI's information must be segregated, either logically or physically, from the information of other clients of the service provider;

18.17.5 the service provider maintains compliance with applicable security requirements and established relevant security standards, local or international, at all times; and

18.17.6 the service provider undertakes measures to safeguard customer information of the EMI at all times and reports any customer information breach to the EMI within an agreed timeframe.

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

18.19 An EMI shall ensure that the outsourcing arrangements undertaken outside Bangladesh are conducted in a manner which does not affect—

18.19.1 the EMI's ability to effectively monitor the service provider and execute its BCM;

18.19.2 the EMI's ability to promptly recover data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; and

18.19.3 the Bangladesh Bank's ability to exercise its supervisory powers, in particular the Bangladesh Bank's timely and unrestricted access to systems, information or documents relating to the outsourced activity.

18.20 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, but such certifications or reports shall not substitute the EMI's right to conduct on-site inspections where necessary. This is provided that such reliance must be supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access by the EMI to the said third party and cloud service provider to clarify matters relating to the audit.

18.21 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.

19 Fraud Risk Management

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

19.2 An EMI shall establish effective procedures on fraud detection, analysis, investigation and reporting, which include—

19.2.1 fraud detection and transaction monitoring that can facilitate timely identification and mitigation of suspicious transactions;

19.2.2 regular analysis to understand fraud trends and modus operandi. This includes but not limited to 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

19.2.3 reporting of fraud incidents to senior management and the board on a regular basis and take appropriate and corrective measures to prevent the recurrence of these type of incidences.

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

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.

19.5 An EMI shall implement relevant safeguards to prevent unauthorized reloading and usage of an e-money account, in particular if auto reloading and peer-to- peer transfer services are allowed.

20 Risk-based Authentication for Online Payment Transactions

20.1 An EMI shall authenticate its customer for online payment transactions using strong authentication methods, such as multi-factor authentication (MFA)[4], to mitigate the risk of fraudulent online payment transactions.

20.2 Notwithstanding **Paragraph** 20.1, an EMI may adopt risk-based authentication for low-risk online payment transactions.

20.3 For the purpose of **Paragraph** 20.2, low risk online payment transactions shall consist of the following—

20.3.1 online payment transactions below Taka 1500 per transaction; or

20.3.2 recurring or card-on-file[5] transactions below Taka 10,000[6] per transaction, where an EMI has authenticated its customer using strong authentication for first time use.

20.4 In applying risk-based authentication for low-risk online payment transactions under **Paragraph** 20.2, an EMI shall—

---

[4] 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.

[5] Refers to a transaction where the cardholder has authorized the merchant to store the cardholder's card payment information securely for future purchases.

[6] For open third-party fund transfer and open payment transactions with a value of Taka 10,000 and above, an EMI shall deploy multi-factor authentication solutions with stronger security controls.

20.4.1 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

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

20.5 An EMI is encouraged to identify a tolerable aggregate amount of low-risk online payment transactions eligible for risk-based authentication to mitigate against high fraud losses.

20.6 An EMI shall notify the Bangladesh Bank at least fourteen (14) days prior to first-time implementation of risk-based authentication for low-risk online payment transactions under **Paragraph** 20.2.

20.7 Where an EMI adopts risk-based authentication that enables customers to make unauthenticated online payment transactions, the EMI shall—

20.7.1 provide customers with an option to opt-out or disable the function that allows unauthenticated online payment transactions, and the option shall be made available through convenient means;

20.7.2 set a maximum daily cumulative limit for both the amount and number of unauthenticated online payment transactions for a customer;

20.7.3 ensure that customer uses a strong authentication method once the online payment transactions exceed the maximum daily cumulative limit; and

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

20.8 An EMI shall provide convenient means to customers to reduce the limits applied under **Paragraph**s 20.3 or the maximum daily cumulative limit as set under **Paragraph** 20.7.2.

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

20.9.1 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; and

20.9.2 communication methods that can facilitate easy understanding by customers such as by being multi-lingual, publishing frequently-asked- questions and providing clarity in explanation by call-centers.

20.10 An EMI shall immediately provide transaction alerts to customers after every successful online payment transaction that is not authenticated as per **Paragraph** 20.1.

21 Contactless Verification Requirement

21.1 **Paragraph**s 21.2 to 21.5 shall only apply to an EMI that issues international scheme prepaid cards.

21.2 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.

21.3 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—

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

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

21.3.3 raise awareness among customers about the facilities set out in **Paragraph**s 21.3.1 and 21.3.2, at a minimum via the EMI's websites and product disclosure sheet.

21.4 An EMI must by default disable customers from making—

21.4.1 any card-not-present transaction that is not authenticated via a strong authentication method such as a dynamic password; and

21.4.2 any overseas transaction using a prepaid card,

and inform the customers on the risks of such transactions.

21.5 An EMI shall only allow customers to make the transactions listed in **Paragraph** 21.4 where the customers have expressly opted-in to conduct such transactions. Where customers have opted-in to conduct such transactions, the EMI shall provide the customers with the option to disable such transactions.

21.6 Notwithstanding **Paragraph** 21.1, an EMI that facilitates cross-border payment via its network-based e-money is also encouraged to observe the requirements in **Paragraph**s 21.4.2 and 21.5, where relevant.

22 Technology Risk Management

22.1 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.

22.2 An EMI is encouraged to include the following in the TRMF—

22.2.1 clear definition of technology risk;

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

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

22.2.4 risk classification of all information assets/systems based on its criticality;

22.2.5 risk measurement and assessment approaches and methodologies;

22.2.6 risk controls and mitigations; and

22.2.7 continuous monitoring to timely detect and address any material risks.

22.3 An EMI is encouraged to establish an independent enterprise-wide technology risk management function which is responsible for—

22.3.1 implementing the TRMF and Cyber Resilience Framework (CRF) as provided under **Paragraph** 34;

22.3.2 advising on material technology projects and ensuring critical issues that may have an impact on the EMI's risk tolerance are adequately deliberated by or escalated to senior management in a timely manner; and

22.3.3 providing independent views to the board and senior management on third party assessments[7], where necessary.

22.4 An EMI is encouraged to designate a Chief Information Security Officer (CISO), or by whatever name called, to be responsible for the technology risk management function of the EMI. The EMI is encouraged to ensure that the CISO has sufficient authority, independence and resources. It is recommended that the CISO—

22.4.1 be independent from day-to-day technology operations;

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

22.5 An EMI is encouraged to make the CISO responsible for ensuring the EMI's information assets and technologies are adequately protected, which includes—

22.5.1 formulating appropriate policies for the effective implementation of TRMF and CRF;

22.5.2 enforcing compliance with policies in **Paragraph** 22.5.1 above, frameworks and other technology-related regulatory requirements; and

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

22.5.3 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.

23 Technology Operations Management

23.1 An EMI shall establish appropriate governance requirements commensurate with the risk and complexity 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.

23.2 It is recommended that the risk assessment 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. It is recommended that due regard be given to the following areas–

23.2.1 the adequacy and competency of resources including those of the service provider to effectively implement the project. This should also take into consideration the number, size and duration of material technology projects undertaken concurrently by the EMI;

23.2.2 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 service provider-proprietary technologies, large-scale data migration or cleansing efforts and extensive system customization;

23.2.3 the adequacy and configuration of security controls throughout the project life cycle to mitigate cyber security breaches or potential leaks of confidential data;

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

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

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

23.2.7 the adequacy of disaster recovery operational readiness following the implementation of new or enhanced systems.

23.3 The board and senior management are encouraged to receive and review timely reports on the management of key risks arising from the implementation of material technology projects on an ongoing basis throughout the implementation of material technology projects.

24 System Development and Acquisition

24.1 An EMI is encouraged to 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.

24.2 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. 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.

24.3 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 authorization procedures and adequate measures to prevent their unauthorized disclosure are in place. It is encouraged that the scope of system testing includes unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, and exception and negative testing, where applicable.

24.4 An EMI shall ensure any changes to the source code of critical systems are subject to adequate source code reviews to ensure the code is secure and developed in line with recognized coding practices prior to introducing any system changes.

24.5 Where critical systems are developed and maintained by a service provider, an EMI shall ensure the source code continues to be readily accessible and secured from unauthorized access.

24.6 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.

24.7 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 the unsuccessful implementation of material system changes to minimize any business disruption.

24.8 Where an EMI's IT systems are managed by technology service providers, the EMI shall ensure, including through contractual obligations, that the technology service providers provide sufficient

notice to the EMI before any changes are undertaken that may impact the IT systems.

24.9 When decommissioning critical systems, an EMI is encouraged to ensure minimal adverse impact on customers and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

25 Cryptography Operations Management

25.1 An EMI is encouraged to adopt strong cryptographic controls for protection of important data and information which include—

25.1.1 adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;

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

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

25.1.4 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 minimize the impact of a compromise.

25.2 An EMI is encouraged to conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorization and non-repudiation of information. Where an EMI does not generate its own encryption keys, the EMI is encouraged to undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves reliance on third party assessment, the EMI is encouraged to consider whether such reliance is consistent with the EMI's risk appetite and tolerance. An EMI is encouraged to 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.

25.3 An EMI is encouraged to ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. It is recommended that the protocols 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. It is recommended that the selection of such protocols be based on recognized international standards and tested accordingly.

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

25.4 An EMI is encouraged to 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 recognized certificate authorities. The EMI is encouraged to 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.

26 Data Center Infrastructure Management

26.1 An EMI shall ensure proper management of data centers and specify the resilience and availability objectives of its data centers which are aligned with its business needs.

26.2 An EMI shall ensure its network infrastructure is designed to be resilient, secure and scalable proportionate to the EMI's business risk and model. Potential data center failures or disruptions shall not significantly degrade the delivery of its financial services or impede its internal operations.

26.3 An EMI is encouraged to ensure production data centers are concurrently maintainable. This includes ensuring that production data centers have redundant capacity components and distribution paths serving the computer equipment

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

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

26.6 An EMI is encouraged to appoint a technically competent external technology service provider to carry out a production data center 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 center and should be conducted periodically or whenever there is a material change in the data center infrastructure. The assessment should, at a minimum, include a consideration of whether **Paragraph**s 26.3 to 26.5 have been adhered to. In appointing a technology service provider to manage the data center, 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

27 Date Center Operations

27.1 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.

27.2 An EMI shall establish appropriate monitoring mechanisms to track capacity utilization and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.

27.3 An EMI shall segregate incompatible activities[8] in the data center operations environment to prevent any unauthorized activity[9]. Where service providers' or programmers' access to the production environment is necessary, these activities shall be properly authorized and monitored.

27.4 An EMI shall establish adequate control procedures for its data center 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.

27.5 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.

27.6 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.

[8] This includes security administration covering management of user access rights, security operations and network security.

[9] This includes segregating system development activities from data center operations.

27.7 Where there is a reasonable expectation for immediate delivery of service, an EMI is encouraged to ensure the relevant systems are designed for high availability.

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

27.8.1 Deploying the industry-tested and accepted encryption techniques;

27.8.2 Implementing authorized access control to sensitive data (e.g. password protection, user access matrix);

27.8.3 Prohibiting unauthorized copying and reading from the media;

27.8.4 Should there be a need to transport the removable media to a different physical location, EMIs should—

27.8.4.1 strengthen the chain of custody process for media management which includes—

27.8.4.1.1 the media should not be under single custody at any point of time;

27.8.4.1.2 the media should always be within sight of the designated custodians; and

27.8.4.1.3 the media should be delivered to its target destination without unscheduled stops or detours;

27.8.4.2 use secure and official vehicle for transportation; and

27.8.4.3 use strong and tamper-proof containers for storing the media with high security lock (e.g. dual key and combination lock);

27.8.5 Ensuring technology service providers comply with the requirements in **Paragraph**s 27.8.1 to 27.8.4, in the event outsourced services are required in undertaking the storage management or transportation process of sensitive data in removable media.

28 Network Resilience

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

28.2 An EMI is encouraged to 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.

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

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

28.5 An EMI is encouraged to 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.

28.6 An EMI shall ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least 12 years.

28.7 An EMI shall implement appropriate safeguards to minimize 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.

28.8 An EMI is encouraged to appoint a technically competent external technology service provider to carry out regular network risk assessments 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.

29 Technology Service Provider Management

29.1 In addition to the requirements in **Paragraph** 18 on outsourcing arrangements, an EMI and its board and senior management shall comply with the requirements under **Paragraph**s 29.2 to 29.8 for IT-related technology service providers.

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

29.3 28.45 An EMI shall conduct proper due diligence on the technology service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made on the technology service provider's capabilities in managing the following specific risks—

29.3.1 data leakage such as unauthorized disclosure of customer information and counterparty information;

29.3.2 service disruption including capacity performance;

29.3.3 processing errors;

29.3.4 physical security breaches;

29.3.5 cyber threats;

29.3.6 over-reliance on key personnel;

29.3.7 mishandling of confidential information pertaining to the EMI or its customers in the course of transmission, processing or storage of such information; and

29.3.8 concentration risk.

29.4 At a minimum, the agreement between the EMI and its technology service providers shall contain arrangements for disaster recovery and backup capability, where applicable, and critical system availability.

29.5 An EMI shall ensure its ability to regularly review any agreements with its technology service providers taking into account the latest security and technological developments in relation to the services provided.

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

29.7 An EMI shall ensure the storage of its data is at least logically segregated from the other clients of the technology service provider. There shall be proper controls implemented including periodic review of the access provided to authorized users.

29.8 An EMI shall ensure critical systems hosted by technology 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 technology service provider.

30 Cloud Services Operations

30.1 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—

30.1.1 sophistication of the deployment model;

30.1.2 migration of existing systems to cloud infrastructure;

30.1.3 location of cloud infrastructure;

30.1.4 multi-tenancy or data co-mingling;

30.1.5 service provider lock-in and application portability or interoperability;

30.1.6 ability to customize security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;

30.1.7 exposure to cyber-attacks via cloud service providers;

30.1.8 termination of a cloud service provider including the ability to secure the EMI's data following the termination;

30.1.9 demarcation of responsibilities, limitations and liability of the cloud service provider; and

30.1.10 ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

30.2 The risk assessment required under **Paragraph** 30.1 shall be documented and made available for the Bangladesh Bank's review as and when requested by the Bangladesh Bank.

30.3 An EMI shall demonstrate that specific risks associated with the use of cloud services for critical systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in **Paragraph** 30.1, as well as, the following areas—

30.3.1 the adequacy of the over-arching cloud adoption strategy of the EMI including—

30.3.1.1 board oversight over cloud strategy and cloud operational management;

30.3.1.2 senior management roles and responsibilities on cloud management;

30.3.1.3 conduct of day-to-day operational management functions;

30.3.1.4 management and oversight by the EMI of cloud service providers;

30.3.1.5 quality of risk management and internal control functions; and

30.3.1.6 strength of in-house competency and experience;

30.3.2 the availability of independent, internationally recognized certifications of the cloud service providers, at a minimum, in the following areas–

30.3.2.1 information security management framework, including cryptographic modules such as those used for encryption and decryption of user data; and

30.3.2.2 cloud-specific security controls for protection of customer information and counterparty information or proprietary information including payment transaction data in use, in storage and in transit;

30.3.3 the degree to which the selected cloud configuration adequately addresses the following attributes—

30.3.3.1 geographical redundancy;

30.3.3.2 high availability;

30.3.3.3 scalability;

30.3.3.4 portability;

30.3.3.5 interoperability; and

30.3.3.6 strong recovery and resumption capability including appropriate alternate internet paths to protect against potential internet faults.

30.4 An EMI is encouraged to consider the need for a third-party pre-implementation review on cloud implementation that also covers the areas set out in **Paragraph** 30.3.

30.5 An EMI must implement appropriate safeguards on customer information and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer information and counterparty

information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.

31 Access Control Management

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

31.2 In observing **Paragraph** 31.1, an EMI is encouraged to consider the following in its access control policy—

31.2.1 adopt a "deny all" access control policy for users by default unless explicitly authorized;

31.2.2 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;

31.2.3 employ time-bound access rights which restrict access for a specific period including access rights granted to technology service providers;

31.2.4 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–

31.2.4.1 system development and technology operations;

31.2.4.2 security administration and system administration; and

31.2.4.3 network operation and network security;

31.2.5 employ dual control functions which require two or more persons to execute an activity;

31.2.6 adopt stronger authentication for critical activities including for remote access;

31.2.7 limit and control the use of the same user ID for multiple concurrent sessions;

31.2.8 limit and control the sharing of user ID and passwords across multiple users; and

31.2.9 control the use of generic user ID naming conventions in favor of more personally identifiable IDs.

31.3 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).

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

31.5 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.

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

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

31.8 An EMI shall ensure the following—

31.8.1 access controls to enterprise-wide systems are effectively managed and monitored; and

31.8.2 user activities in critical 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.

32 Patch and End-of-Life System Management

32.1 An EMI shall ensure that critical 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—

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

32.1.2 identify critical technology systems that are approaching EOL for further remedial action.

32.2 An EMI is encouraged to establish a patch and EOL management framework which addresses among others the following requirements—

32.2.1 identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;

32.2.2 conduct of compatibility testing for critical patches;

32.2.3 specification of turnaround time for deploying patches according to the severity of the patches; and

32.2.4 adherence to the workflow for end-to-end patch deployment processes including approval, monitoring and tracking of activities.

33 Security of Digital Services

33.1 An EMI shall implement robust technology security controls in providing digital services which assure the following—

33.1.1 confidentiality and integrity of customer information and counterparty information and transactions;

33.1.2 reliability of services delivered via channels and devices with minimum disruption to services;

33.1.3 proper authentication of users or devices and authorization of transactions;

33.1.4 sufficient audit trail and monitoring of anomalous transactions;

33.1.5 ability to identify and revert to the recovery point prior to incident or service disruption; and

33.1.6 strong physical control and logical control measures.

33.2 An EMI is encouraged to 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.

33.3 An EMI must implement additional controls to authenticate devices and users, authorize transactions and support non-repudiation and accountability for high-risk transactions or transactions above Taka 15,000. These measures must include, at a minimum, the following—

33.3.1 ensure transactions are performed over secured channels such as the latest version of Transport Layer Security (TLS);

33.3.2 both client and host application systems must encrypt all confidential information prior to transmission over the network;

33.3.3 adopt MFA for transactions;

33.3.4 if OTP is used as a second factor, it must be dynamic and time-bound;

33.3.5 request users to verify details of the transaction prior to execution;

33.3.6 ensure secure user and session handling management;

33.3.7 be able to capture the location of origin and destination of each transaction;

33.3.8 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

33.3.9 provide timely notification to customers that is sufficiently descriptive of the nature of the transaction.

33.4 An EMI must ensure the MFA solution used to authenticate financial transactions are adequately secure, which includes the following–

33.4.1 binding of the MFA solution to the customer's account;

33.4.2 activation of MFA must be subject to verification by the EMI; and

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

33.5 An EMI is encouraged to deploy MFA technology and channels that are more secured than unencrypted short messaging service (SMS).

33.6 An EMI shall deploy MFA solutions with stronger security controls for open third-party fund transfer and open payment transactions with a value of Taka 15,000 and above.

33.7 Such stronger MFA solutions shall adhere to the following requirements—

33.7.1 payor/sender must be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction;

33.7.2 authentication code must be initiated and generated locally by the payor/sender using MFA;

33.7.3 authentication code generated by payor/sender must be specific to the confirmed identified beneficiary and amount;

33.7.4 secure underlying technology must be established to ensure the authentication code accepted by the EMI corresponds to the confirmed transaction details; and

33.7.5 notification must be provided to the payor/sender of the transaction.

33.8 Where an EMI deploys OTP as part of its stronger MFA solutions, the following features must be implemented–

33.8.1 binding of the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction);

33.8.2 generation of the OTP from the customer's device and not from the EMI's server; and

33.8.3 requiring the customer to physically enter the generated OTP into the application.

33.9 For financial transactions below Taka 15,000, 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.

33.10 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—

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

33.10.2 provide convenient means for customers to reduce the limits described in **Paragraph** 33.10.1 or to opt for MFA;

33.10.3 provide convenient means for its customers to temporarily suspend their account in the event of suspected fraud; and

33.10.4 provide its customers with adequate notice of the safeguards set out in **Paragraph**s 33.10.1 to 33.10.3.

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

33.12 An EMI shall ensure that critical online payments services, e.g. web or mobile applications, or transactions have high availability with reasonable response time to customer actions.

33.13 An EMI is encouraged to ensure the use of more advanced technology to authenticate and deliver digital services such as biometrics, tokenization and contactless communication[10] comply with internationally recognized standards where available. The technology should be resilient against cyber threats[11] including malware, phishing or data leakage.

33.14 An EMI is encouraged to 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 the reliance of reports is consistent with the EMI's risk appetite and tolerance as well as the nature of digital services provided by the EMI which leverage on the technologies and algorithms.

33.15 An EMI is encouraged to 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.

33.16 An EMI is encouraged to 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. It is recommended that an EMI implements sufficient logical and physical safeguards for the following channels/ devices—

33.16.1 QR code;

33.16.2 internet application; and

33.16.3 mobile application and devices.

In view of the evolving threat landscape, these safeguards should be

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

[11] 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

continuously reviewed and updated to protect against fraud and to secure the confidentiality and integrity of customer information and counterparty information and transactions.

33.17 An EMI should ensure the adequacy of security controls implemented for internet applications, which include to—

33.17.1 ensure the internet application only runs on secured versions of web browsers that have continued developer support for security patches to fix any vulnerabilities; and

33.17.2 put in place additional authentication protocols to enable customers to identify the EMI's genuine websites.

33.18 An EMI should ensure digital payment services involving sensitive customer information and counterparty information offered via mobile devices and applications are adequately secured. This includes the following—

33.18.1 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);

33.18.2 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 information 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 centralized at the host;

33.18.3 undertake proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;

33.18.4 ensure proper controls are in place to access, maintain and upload the mobile application on application distribution platforms;

33.18.5 activation of the mobile application must be subject to authentication by the EMIs;

33.18.6 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

33.18.7 monitor the application distribution platforms to identify and address the distribution of fake applications in a timely manner.

33.19 In addition to **Paragraph** 33.18, 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 information and counterparty information—

33.19.1 mobile device to be adequately hardened and secured;

33.19.2 ensure the capability to automatically wipe data stored in the mobile devices in the event the device is reported stolen or missing; and

33.19.3 establish safeguards that ensure the security of customer information 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[12].

33.20 An EMI is encouraged to adopt adequate controls to ensure that QR code authenticity which among others include—

33.20.1 QR codes are securely generated by the host server, unique for each merchant/ customer/ transaction, where dynamic QR codes should have a reasonable expiry time;

33.20.2 block QR code applications from operating on unsecured (e.g. rooted or jailbroken) devices;

33.20.3 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

33.20.4 bind the QR code to the respective customer or merchant ID and transaction amount.

33.21 An EMI shall ensure that QR codes do not contain any confidential data and are not stored in endpoint devices.

33.22 An EMI shall ensure that all relevant risks associated with the use of static QR codes at participating merchants are mitigated, including but not limited to the following—

33.22.1 all information from the scanned QR codes shall be transmitted to the payment instrument's host server for authentication;

33.22.2 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

33.22.3 enforce masking of sensitive customer information and counterparty information when displayed on mobile devices.

34 Cyber Risk Management

34.1 An EMI is encouraged to 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.

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

34.2 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 include ensuring operational resilience against extreme but plausible cyberattacks.

34.3 It is encouraged that the CRF be able to support effective identification, protection, detection, response, and recovery (IPDRR) of systems and data hosted on-premise or by technology service providers from internal and external cyber-attacks. It is recommended that the CRF consists of, at a minimum, the following elements—

34.3.1 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;

34.3.2 identification, classification and prioritization 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;

34.3.3 identification of cybersecurity threats and countermeasures including measures to contain reputational damage that can undermine confidence in the EMI;

34.3.4 layered (defense-in-depth) security controls to protect its data, infrastructure and assets against evolving threats;

34.3.5 timely detection of cybersecurity incidents through continuous surveillance and monitoring;

34.3.6 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

34.3.7 policies and procedures for timely and secure information sharing and collaboration with other EMIs and participants in financial market infrastructure to strengthen cyber resilience.

35 Cybersecurity Operations

35.1 An EMI is encouraged to establish clear responsibilities for cybersecurity operations which include implementing appropriate mitigating measures in the EMI's conduct of business that correspond to the following phases of the cyberattack lifecycle—

35.1.1 reconnaissance;

35.1.2 weaponization;

35.1.3 delivery;

35.1.4 exploitation;

35.1.5 installation;

35.1.6 command and control; and

35.1.7 exfiltration.

35.2 Where relevant, an EMI is encouraged to adopt the control measures on cybersecurity to enhance its resilience to cyberattacks as specified in the following—

35.2.1 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.

35.2.2 Update checklists on the latest security hardening of operating systems.

35.2.3 Update security standards and protocols for web services encryption regularly. Disable support of weak ciphers and protocols in web-facing applications.

35.2.4 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 firewalls and Intrusion Prevention Systems (IPS).

35.2.5 Ensure security controls for server-to-server external network connections include the following—

35.2.5.1 server-to-server authentication such as Public Key Infrastructure (PKI) certificate or user ID and password;

35.2.5.2 use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and

35.2.5.3 deploying staging servers with adequate perimeter defenses and protection such as firewall, IPS and antivirus.

35.2.6 Ensure security controls for remote access to server include the following—

35.2.6.1 restrict access to only hardened and locked down end-point devices;

35.2.6.2 use secure tunnels such as TLS and VPN IPSec;

35.2.6.3 deploy "gateway" server with adequate perimeter defenses and protection such as firewall, IPS and antivirus; and

35.2.6.4 close relevant ports immediately upon expiry of remote access.

35.2.7 Ensure overall network security controls are implemented including the following—

35.2.7.1 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;

35.2.7.2 IPS at all critical network segments with the capability to inspect and monitor encrypted network traffic;

35.2.7.3 web and email filtering systems such as web-proxy, spam filter and anti-spoofing controls;

35.2.7.4 end-point protection solution to detect and remove security threats including viruses and malicious software;

35.2.7.5 solution to mitigate advanced persistent threats including zero-day and signatureless malware; and

35.2.7.6 capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.

35.2.8 Synchronize and protect the Network Time Protocol (NTP) server against tampering.

35.3 An EMI is encouraged to deploy effective tools to support 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.

35.4 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.

35.5 An EMI shall conduct annual penetration tests on its internal and external network infrastructure, as well as, critical 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 technology service providers to perform this function.

35.6 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.

35.7 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.

36 Distributed Denial of Service (DDoS)

36.1 An EMI is encouraged to ensure its technology systems and infrastructure, including critical systems outsourced to or hosted by technology service providers, are adequately protected against all types of DDoS attacks (including volumetric, protocol and application layer attacks) through the following measures—

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

36.1.2 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

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

37 Data Loss Prevention (DLP)

37.1 An EMI is encouraged to establish a clear DLP strategy and processes in order to ensure that proprietary and customer information and counterparty information is identified, classified and secured. It is recommended for an EMI to—

37.1.1 ensure that data owners are accountable and held responsible for identifying and appropriately classifying data;

37.1.2 undertake a data discovery process prior to the development of a data classification scheme and data inventory; and

37.1.3 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.

37.2 An EMI is encouraged to 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—

37.2.1 data in-use – data being processed by IT resources;

37.2.2 data in-motion – data being transmitted on the network; and

37.2.3 data at-rest – data stored in storage mediums such as servers, backup media and databases.

37.3 An EMI is encouraged to implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorized access to data.

38 Security Operations Center (SOC) Management

38.1 An EMI shall have in place an SOC – whose functions can either be performed in-house or by technology service providers – with 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 review of its cybersecurity posture and strategy.

38.2 The SOC is encouraged to be able to perform the following functions—

38.2.1 log collection and the implementation of an event correlation engine with parameter-driven use cases such as Security Information and Event Management (SIEM);

38.2.2 incident coordination and response;

38.2.3 vulnerability management;

38.2.4 threat hunting;

38.2.5 remediation functions including the ability to perform forensic artifact handling, malware and implant analysis; and

38.2.6 provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). This includes advanced behavioral analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers.

38.3 An EMI is encouraged to ensure that the SOC provides a regular threat assessment report, which should include, at a minimum, the following—

38.3.1 trends and statistics of cyber events and incidents categorized by type of attacks, target and source IP addresses, location of data centers and criticality of applications; and

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

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

38.5 An EMI shall ensure the following—

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

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

39 Cyber Response and Recovery Operations

39.1 An EMI shall establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organization'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.

39.2 An EMI is encouraged to establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP should address the following—

39.2.1 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;

39.2.2 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;

39.2.3 Containment, eradication and recovery: Identify and implement remedial actions to prevent or minimize damage to the EMI, remove the known threats and resume business activities; and

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

39.3 An EMI is encouraged to 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 technology service providers. The test scenarios should include scenarios designed to test—

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

39.3.2 the readiness and effectiveness of CERT and relevant technology service providers in supporting the recovery process.

39.4 An EMI shall immediately notify the Bangladesh Bank of any cyber-incidents (Examples include (but not limited to) phishing, ransomware, malware, DDoS and brute force attack, network intrusion, advance persistent threats, insider threats, data exfiltration and compromised credentials) affecting the EMI. Upon completion of the investigation, the EMI is also required to submit a report on the incident to the Bangladesh Bank through the relevant Operational Risk Reporting (ORR) system or any other channel as specified by the Bangladesh Bank.

39.5 An EMI shall collaborate and cooperate closely with relevant stakeholders and authorities in combating cyber threats and sharing threat intelligence and mitigation measures.

40 Technology Audit

40.1 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.

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

40.3 An EMI is encouraged to ensure its technology audit staff are adequately conversant with the developing sophistication of the EMI's technology systems and delivery channels.

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

40.5 The internal audit function under **Paragraph** 40.2 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.

41 Internal Awareness and Training

41.1 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 programs. This cybersecurity awareness education shall be conducted at least annually by the EMI and shall reflect the current cyber threat landscape.

41.2 An EMI is encouraged to 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.

41.3 An EMI is encouraged to provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

42 Transaction Security Requirements

42.1 In order to minimize risk to customer funds, all agent-based transactions must be undertaken electronically and settled in real-time against a pre-funded account held by the agent,

42.2 All transactions against customer accounts must be duly authorized by the account holder. For all amounts, a two-factor authentication using a PIN code, biometric signature or similar as well as a physical token in the form of a card, SIM card or similar must be used to authenticate the account holder.

42.3 Customers shall be notified of all transactions on their accounts via electronic notification or a physical receipt providing at least the following information:

42.3.1 Transaction amount;

42.3.2 Transaction type;

42.3.3 Any fees charged;

42.3.4 Unique transaction reference;

42.3.5 Date and time of transaction;

42.3.6 Identifying details of the recipient of an outbound transaction or of the sender of an inbound transaction

PART VI: ISSUANCE AND OPERATION OF E-MONEY

43 Issuance, Redemption and Account Management

43.1 E-money accounts and transactions within Bangladesh shall be denominated only in Bangladeshi Taka.

43.2 E-money issuers shall issue e-money at par value on the receipt of funds in advance.

43.3 An EMI shall ensure e-money transactions comply with the prevailing foreign exchange rules, including but not limited to those related to investments in foreign currency assets by residents and payment in foreign currency between residents, through the implementation of robust internal controls and procedures.

43.4 An EMI shall ensure any physical cash withdrawal outside Bangladesh using e-money, is undertaken in foreign currency only. An EMI that facilitates withdrawal of e-money balances into a bank account shall ensure any withdrawal of funds from the e-money account is paid into the customer's own bank account with a banking institution only, unless the EMI participates in a suitable real-time payment system and offers credit transactions where withdrawal of e-money balances, subject to the compliance of AML/CFT requirements, may be made to other bank or e-money accounts.

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

43.6 E-money issuers shall, upon request by the e-money holder, redeem, at any moment and at par value, the monetary value of e-money held.

43.7 Notwithstanding **Paragraph** 43.6, redemption may be subject to a fee if clearly stated in the contract between the e-money issuer and e-money holder.

43.8 E-money issuers must utilize at least 80% of the earned interest (after deducting regular account fees) by spending it directly on activities that benefit (for example- reducing operational costs & transactional costs etc.) the e-money holders. These fees must be the usual, standard charges for that type of account. If any special or unusual fees are added, or if a new type of account is created just to reduce the interest income, it will be considered fraud. This could lead to strict penalties for both the scheduled bank and any partners involved. Also, the total fees charged cannot be more than the interest earned, and the account balance must always be equal to or more than the total amount of e-money it is supposed to hold.

43.9 Any amount in excess of the minimum of 80% interest (i.e. 20% or lower) may be retained by the EMI. Furthermore, interest generated on

over-the-counter transactions which are not associated with a given customer account may be retained in by the EMI.

43.10 For purposes of transparency and accountability, interest shall be paid into a separate account (interest account) held in the name of the pooled account. Withdrawals from this account shall be only to distribute interest.

43.11 An EMI shall submit a proposal to Bangladesh Bank for approval on how it intends to distribute the interest.

43.12 The provisions in **Paragraph**s 43.8 and 43.9 above may be reviewed by the Bangladesh Bank as it deems fit.

43.13 An EMI shall provide refunds of e-money balances in its customers' accounts in the event a customer decides to close their account, was wrongly charged or due to disputed transactions.

43.14 The refund shall be made without any additional costs and shall be done within seven (7) days from the date the claim is made by the customer except for complex refund cases.

43.15 For complex refund cases that cannot be completed within seven (7) days, the EMI shall communicate the reason for such delays to customers in a timely manner and complete the cases within thirty (30) days.

43.16 An EMI shall provide customers with options for the method of refund and shall not limit refunds only via the crediting of funds back into the customer's e-money account.

43.17 Any e-money issuer which fails to comply with the requirement under **Paragraph** 43.8 above shall pay to the Bangladesh Bank a fine not exceeding Taka 30 (Thirty) Lakhs.

44 Permissible Activities

44.1 In addition to issuing e-money, Dedicated EMIs shall be entitled to engage in any of the following activities:

44.1.1 The operation of payment systems, where the conditions of applicable rules are met, notably including those of the Payment and Settlement Systems Act, 2024;

44.1.2 The provision of operational services and closely related ancillary services in respect of the issuing of e-money or to the operation of payment systems referred to in **Paragraph** 44.1.1 above.

44.1.3 Any other activity permitted by the Bangladesh Bank.

44.2 E-money systems may be used for the following:

44.2.1 Domestic payments;

44.2.2 Domestic money transfers, including to and from bank accounts;

44.2.3 Bulk transactions, including payments of salaries, benefits, pensions etc.;

44.2.4 Cash-in and cash-out transactions;

44.2.5 Over-the-counter transactions;

44.2.6 Inward international remittances;

44.2.7 Savings products in partnership with banks and other deposit-taking institutions;

44.2.8 Credit products under-written by a duly licensed RFI;

44.2.9 Insurance products under-written by a duly licensed insurer;

44.2.10 Any other transactions the Bangladesh Bank may prescribe. The Bangladesh Bank may, by notification, restrict the permissible transactions of EMIs or remove the restrictions so imposed as it considers appropriate.

45 Prohibited Activities

45.1 An EMI shall not—

45.1.1 issue e-money at a premium or discount, i.e. issue e-money that has a monetary value different than the funds received;

45.1.2 use the funds collected in exchange of e-money issued to extend loans or financing to any person;

45.1.3 extend credit to the customer or any other person, or pay interest, profit or any other form of returns on the e-money balances, that would add to the monetary value of the e-money;

45.1.4 comingle customer funds with their own working capital or funds from other businesses; and

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

45.2 Airtime shall not count as e-money and as such cannot be used for permissible transactions under these Regulations.

45.3 Any other activity prohibited by the Bangladesh Bank.

45.4 Failure to comply with the provisions under this **Paragraph** shall impose a fine of up to Take 10 Lac.

46 Transaction Limits

46.1 Customer e-money accounts have been categorized in three levels as part of a risk-based approach to KYC. Minimum KYC accounts, intended as a first step towards financial inclusion for the unbanked, are subject to very low transaction limits and correspondingly low documentation requirements, while Medium KYC accounts have intermediate transaction limits and documentation requirements and Enhanced KYC accounts give access to high limits but come with bank grade account opening requirements. Furthermore, over-the-counter transactions have been categorized separately.

46.1.1 Every Minimum KYC account issued shall be subject to a maximum balance limit of Taka 20,000, a single transaction limit of Taka 1,000, an aggregate daily transaction limit of Taka 5,000 and an aggregate monthly transaction limit of Taka 20,000.

46.1.2 Every Medium KYC account issued shall be subject to a maximum balance limit of 50,000, a single transaction limit of Taka 5,000, an

aggregate daily transaction limit of 15,000 and an aggregate monthly transaction limit of 50,000.

46.1.3 Accounts opened for transactions or balances exceeding the permissible limits of a Medium KYC account must comply with Enhanced KYC requirements before issuance.

46.2 Over-the-counter transactions that do not involve the use of a customer e-money account shall be permitted and subject to the following transaction limits:

46.2.1 Where the customer presents acceptable ID as per **Paragraph 49.1** below, over-the counter transactions shall be subject to the limits set by the Bangladesh Bank through relevant circulars issued from time to time.

46.2.2 Where the customer does not present an acceptable ID, he/she shall be required to be introduced by someone with an acceptable ID. E-Money Issuers will in all instances of such transactions be required to capture under separate fields in their system at least the following information on the customer: name, date of birth, address, telephone number; and the details of the ID of the one doing the introduction. Such transactions shall be subject to the limits set by the Bangladesh Bank through relevant circulars issued from time to time.

46.3 All transactions except cash-out, payments for government services, utility bills, satellite TV, school fees, post-paid telephone/broadband internet bills, or such transactions as shall be determined by Bangladesh Bank from time to time, shall count towards the above limits. Thus, the limits will be restricting the aggregated value of: cash-in to own or someone else's account; physical or online merchant payments; person to person transfers (account-based and over-the-counter); airtime purchases; and any other type of transaction not explicitly exempted by this **Paragraph**.

46.4 Agent e-money accounts are a separate category intended for agents' to provide e-money services to end-customers.
Such accounts shall be restricted as follows:

46.4.1 No limits on account balance or transactions directly serving customers, which are inherently limited by the restrictions articulated in preceding sub-**Paragraph**s of this section.

46.4.2 Transactions against the accounts of the EMI or those of RFIs involved in liquidity management for the EMI shall not count towards these limits.

46.4.3 Agent accounts belonging to RFIs shall not be subject to any limits.

46.4.4 Master-agents shall not be subject to any limits.

46.4.5 EMIs may apply to the Bangladesh Bank on case-by-case basis for approval for higher agent limits, justifying the need, proposing a

revised set of limits and providing the necessary business information supporting the proposal.

46.5 Merchant e-money accounts are a separate category intended for companies that need to receive customer payments, make purchases from suppliers and/or pay salaries to employees in volumes higher than an Enhanced KYC account would permit. Such accounts shall be restricted as follows:

46.5.1 No limits on account balance, inward receipt of electronic payments, outward bulk transactions or transfers to and from a pre-registered bank account belonging to the merchant.

46.5.2 For very large companies where even these limits would be overly restrictive, an approval to supersede these limits may be granted by Bangladesh Bank on a case-by-case basis upon receipt of application from the EMI justifying the need, proposing a revised set of limits and providing business information supporting the proposal. If approved, EMIs are strictly obliged to ensure that the revised limits for each merchant are continuously adhered to. If Bangladesh Bank perceives that this privilege is being abused, it shall prescribe rectifying action for the EMI and may ultimately revoke the privilege.

46.5.3 For individual payment instances where the limits would be overly restrictive, EMIs shall be permitted to supersede prescribed limits on a one-off basis. This shall be subject to the EMI reporting and justifying each such instance to Bangladesh Bank within thirty (30) calendar days. If Bangladesh Bank perceives that this privilege is being abused, it shall prescribe rectifying action for the EMI and may ultimately revoke the privilege.

46.5.4 Merchant accounts belonging to RFIs shall not be subject to any limits.

46.5.5 Only merchant accounts are permitted to perform outward bulk transactions (salaries and benefits).

46.5.6 Any EMI failing to comply with the prescribed transaction limits is liable to a fine not exceeding Taka 5,00,000 per day or equal to the amount transacted, whichever is higher.

47 Dormant Accounts

47.1 An e-money account that has registered no transaction for a consecutive period of twelve (12) months shall be considered dormant. In order to limit the possibility for third party misuse of such an account, the EMI shall adhere to the following:

47.1.1 The relevant customer shall be notified no less than one month before the twelve (12) month mark is reached that the account will be suspended unless there is some form of activity. The customer would then be advised to perform a transaction to keep the account active or to close the account and should be provided with instructions as to how to do so.

47.1.2 If no activity has still taken place when the twelve (12) month mark is reached, the EMI shall not permit further transactions until reactivated by the customer, supported by the original ID used to open the account. The EMI shall notify the customer that the account is **dormant** and provide instructions on how to reactivate it.

47.1.3 An account that has been so dormant for **Six (06)** months without reactivation by or communication from the relevant customer shall be blocked by the EMI.

47.1.4 All outstanding balances in the blocked account shall be transferred, along with identifying information on the customer, into a separate account held by the EMI with a specific scheduled bank designated for this purpose for a period of no less than **six (06)** years;

47.1.5 Scheduled banks holding these accounts are permitted to intermediate the funds and retain the proceeds.

47.1.6 The relevant customer shall be notified, at least three (03) months prior to the completion of the six (06) year period, informing them of the conditions applicable to the blocked accounts;

47.1.7 After a period of **six (06)** years, as mentioned in paragraph 47.1.4, has passed without claim from the original customer, the EMI shall transfer all such funds to the Bangladesh Bank and retain all identifying information;

47.1.8 All identifying information relating to the account and its closing balance shall be retained by the EMI and the bank for a period of no less than **12** years.

47.2 In the case of mobile money, all outstanding e-money balances may be dissociated from MSISDNs after one month (30 calendar days) of inactivity. An MSISDN that is linked to an e-money account shall not be reassigned to a new customer without the following actions on the part of the EMI:

47.2.1 The e-money account shall be terminated;

47.2.2 The EMI shall follow steps in **Paragraph**s 47.1.4 to 47.1.7 above.

47.3 The treatment of dormant accounts shall comply in full with these Regulations as well as any other directive that the Bangladesh Bank may issue hereafter;

47.4 Failure to comply with the provisions under this **Paragraph** shall impose a fine of up to Taka 10 Lac.

47.5 If no claim is made on the remaining money or valuables within 2 (two) years after Bangladesh Bank has received them and settled any valid claim made by the customer, and if no party informs Bangladesh Bank during this time, then after the 2-year period, no one will have any right to that money or those valuables. They will be considered the property of the government and will be transferred to the government account accordingly.

48 Closure of E-Money Accounts

48.1 An EMI shall set up systems, processes, and policies that allow e-money account holders to close their accounts with the same ease that was available to e-money account holders at the time of opening e-money accounts.

48.2 The EMI must keep the records of the transaction history and other data of the e-money accounts closed for twelve (12) years from the date of the closure of e-money accounts.

48.3 If any person who has closed their e-money account previously opt to open a new account within the five years from the date of the closure of e-money account previously closed, their stored data must be synchronized to the newly opened account.

49 Customer Due Diligence Requirements

49.1 The following types of identification documents (IDs) are considered acceptable for the purposes of Customer Due Diligence under these Regulations: National ID, Driver's License, and Passport.

49.2 The following minimum CDD requirements shall be adhered to by every EMI in opening the various types of accounts for e-money holders:

49.2.1 For OTC, each transaction must not be more than Taka 5,000, with a daily limit of Taka 15,000 and a maximum monthly limit of Taka 20,000. The user must have a valid mobile number, and the payment, both cash-in and cash-out, must be verified using a dynamic, time-based OTP (One-Time Password). Payments made at agent points for things like government services, utility bills, school or university fees, job application fees, NID or passport services fee, motor vehicle fines, satellite TV, and post-paid phone or internet bills, or any other payments decided by Bangladesh Bank, will be exceptions to the usual OTC transaction rules. DEMIs will have to sensitize the agents' properly about AML/CFT risks inherent in their transactions and also to monitor transaction patterns carefully towards identifying possible unauthorized/suspicious transaction activities.

49.2.2 For Minimum KYC accounts, customers have to provide their name, date of birth, residential address, mobile number (mobile registered with client's national identity information) and any type of Photo ID that can reliably identify the customer and verifiable digitally.

49.2.3 For Medium KYC accounts, customers have to provide the documents as per **Paragraph** 49.2.1 above, and a declaration of the sources and usage of funds.

49.2.4 For Enhanced KYC accounts, customers have to fully comply with the Bangladesh Bank identification requirements for opening bank accounts, meaning they will in addition to acceptable ID as per **Paragraph** 49.1 above also need to provide a declaration of the sources and usage of funds and at least one of the following: registered

Tenancy Agreement, Utility Bill, Income Tax Certificate, Bank Statements, Reference Letter, or Employer's reference letter. EMIs must verify/validate these documents.

49.2.5 For merchant accounts, companies have to provide their Certificate of Incorporation, Business Identification Number, Tax Identification Number and bank account information.

49.2.6 For OTC transactions, customers should be subject to the same KYC requirements as in **Paragraph** 49.2.1 above.

49.3 E-money issuers will, in all instances of opening Minimum KYC accounts, be required to capture under separate fields in their system at least the following information: customer name; address; customer date of birth; ID type and number; image of the photo ID and for all customers that have one, the customer's telephone number.

49.4 E-money issuers will in all instances of opening Medium or Enhanced KYC accounts be required to capture under separate fields in their system at least the following information: customer name; customer date of birth; address, ID type; ID number; image of photo ID; address and for all customers that have one, the customer's telephone number.

49.5 CDD requirements for the higher level of over-the-counter transactions outlined in **Paragraph** 46.3.1 are limited to the presentation of an acceptable ID as per **Paragraph** 49.1 above. EMIs will in all instances of such transactions be required to capture under separate fields in their system at least the following information: ID type and ID number; image of photo ID and for all customers that have one, the customer's telephone number.

49.6 E-money issuers that have already collected and retained customer ID information, e.g. during registration of SIM cards or bank accounts, are allowed to directly use this information to satisfy relevant CDD requirements across the various account tiers outlined in **Paragraph** 49.2 above, without requiring the presentation of the same documentation again. In cases relying on information from SIM registration, EMIs must validate the data against the database of the National Communications Authority within forty-eight (48) hours of account opening. Accounts where discrepancies are identified must be suspended until such time as these discrepancies have been eliminated.

49.7 E-money issuers are in all instances under strict obligation to conduct such verification of customer information as is necessary to appropriately manage material risks of error, fraud and breaches of applicable rules and principles with regard to AML/CFT.

49.8 Failure to comply with the provisions under this **Paragraph** shall impose a fine of Taka 1 Lac. The EMI shall be required to rectify violations and report to Bangladesh Bank within ten (10) working days.

PART VII: ESTABLISHMENT OF TRUST AND MANAGEMENT OF TRUST AND SETTLEMENT ACCOUNTS

50 Trust Board

50.1 An electronic money issuer under these Regulations shall constitute a separate and autonomous Trust Board responsible for overseeing the management of the Trust and Settlement Account and act as trustee of e-money or electronic money holders. The composition of the Trust Board shall consist of trustees. The number and representation of the members of the Trust board shall be determined by the Bangladesh Bank. All the Trust Board members shall be selected by the Bangladesh Bank.

50.2 Subject to **Paragraph** 50.1, an EMI shall, prior to form a Trust Board submit a written application to the Bangladesh Bank including the following information—

50.2.1 list of the proposed trustees from the EMI, their addresses, their nationalities, and whether they are directors or shareholders of the electronic money issuer;

50.2.2 reference letters from two individuals who are not relatives vouching for the good moral character of each of the trustees;

50.2.3 a documented detailed governance plan within the organizational structure reflecting the directives of Bangladesh Bank;

50.2.4 documented internal mechanisms, including sound administrative and accounting procedures that highlight the separation of the trust funds from the business of the electronic money issuer; and

50.2.5 such other information that the Bangladesh Bank may prescribe time to time.

50.3 The Bangladesh Bank shall notify the electronic money issuer about the selected members of the Trust Board or denial of the nomination.

50.4 The electronic money issuer shall resubmit application with new nominations or any other information subject to denial as per **Paragraph** 50.3.

50.5 Subject to **Paragraph** 50.4, the Bangladesh Bank shall not grant/process the application, if the electronic money issuer fails to-

50.5.1 resubmit its application; or

50.5.2 provide information to rectify the deficiency identified by the Bangladesh Bank.

51 Trust and Settlement Account

51.1 An electronic money issuer shall not issue electronic money without opening a trust and settlement account in accordance with these Regulations and পরিশোধ ও নিষ্পত্তি ব্যবস্থা আইন, ২০২৪ (২০২৪ সনের ৯নং আইন)

51.2 Subject to **Paragraph** 51.1 an electronic money issuer shall be required to open and maintain a Trust and Settlement Accounts in one or more scheduled banks.

52 Commencement of E-Money Issuance

An electronic money issuer shall not commence to issue electronic money unless the Trust Board has been approved and formed and opened Trust and Settlement Accounts as mentioned in these Regulations.

53 Interest in Funds Held in Trust and Settlement Accounts

53.1 Interest accrued in the trust and settlement account shall be used for the direct benefit of the electronic money holders as determined by the Bangladesh Bank.

53.2 Subject to **Paragraph** 53.1 the accrued interest and charges shall be separated from the trust and settlement accounts by opening an interest and charges account in respect of the trust and settlement account balances.

53.3 The electronic money issuer shall utilize the interests accrued in the trust and settlement accounts pursuant to regulations in **Paragraph** 43 unless directed by the Bangladesh Bank otherwise.

54 Administration of Trust

54.1 The EMI shall provide necessary support and logistics with access to its information and systems so that the Trust Board is able to perform its duties and responsibilities under পরিশোধ ও নিষ্পত্তি ব্যবস্থা আইন, ২০২৪ (২০২৪ সনের ৯নং আইন) and these Regulations.

PART VIII: AGENT MANAGEMENT

55 Appointment of Agents

55.1 An electronic money issuer may appoint an agent to provide services on its behalf by entering into an agency agreement.

55.2 Subject to **Paragraph** 55.1, the agency agreement shall-

55.2.1 provide for non-exclusive use of an agent;

55.2.2 provide for compliance to anti-money laundering and combating financing of terrorism laws;

55.2.3 consumer protection mechanisms; and

55.2.4 any other requirements that the Bangladesh Bank shall prescribe.

55.3 For purposes of this regulation an agent is an entity that is contracted by payment systems provider to provide services on behalf of the payment system provider under an agency agreement.

56 Liability for agents' act and omission

A electronic money issuer is liable to its customers for the act and omissions of its agents performed within the scope of the agency agreement.

57 Agent Recruitment

57.1 An electronic money issuer shall, prior to appointing agents for the next six months, submit to the Bangladesh Bank documentation on the proposed agents that include—

57.1.1 procedure for appointment of an agent including a due diligence plan;

57.1.2 copy of the proposed agency agreement based on the agent type and nature of business of the agent;

57.1.3 policies for mitigating money laundering and financing of terrorism in compliance to the anti-money laundering laws;

57.1.4 risk mitigation plan associated with the agency business;

57.1.5 description of the proposed technology to be used by the agent;

57.1.6 agent training materials; and

57.1.7 any other information the Bangladesh Bank may require.

57.2 Subject to **Paragraph 57.1** the electronic money issuer shall carry out a due diligence and assessment of the agent's ability to conduct the agency business.

57.3 The Bangladesh Bank shall review the documentation on the proposed appointment of agents for regulatory compliance.

58 Type of Agents

58.1 Subject to **Paragraph**s 55, 56, and 57, an electronic money issuer shall appoint—

58.1.1 a retail agent that has a trade license, tax identification number, tax clearance certificate and other necessary permits for conducting commercial activities;

58.1.2 a wholesale agent that is a registered corporate, with necessary permits for conducting commercial activities; and has capacity, competence and internal controls to perform the agency services that may include—

58.1.2.1 electronic money distribution;

58.1.2.2 retail agent management; and

58.1.2.3 any other services approved by the Bangladesh Bank.

58.2 Subject to **Paragraph** 58.1, an electronic money issuer shall ensure that an agent opens a bank account for the operations of the agency business.

59 Maintenance of Agents' Records

59.1 An electronic money issuer shall maintain records of its appointed agents, publish them on its website, and submit the same to Bangladesh Bank. Such records shall include-

59.1.1 agents' and their outlet's identity, full addresses including business physical address, global position system coordinates; and

59.1.2 a list of suspended or terminated agents with reasons for such suspension or termination.

59.2 The Bangladesh Bank may develop a public registry of agents and their geographical distribution and place it in its website.

60 Electronic Money Issuer Responsibility

60.1 Subject to the provisions of this Part, an electronic money issuer shall be responsible to—

60.1.1 conduct training for the agents and the operations of the agency business including internal controls, accounting, risk management, consumer protection and anti-money laundering and combating financing of terrorism; and

60.1.2 conduct effective oversight of the agents and its outlets and take appropriate action in events of breach of the agency agreement.

60.1.3 strictly comply with the instructions, directives, and guidelines issued by Bangladesh Bank from time to time.

PART IX: CAPITAL AND SAFEGUARDING REQUIREMENTS

61 Capital Requirements

61.1 At the time of licensing and at any point thereafter, an Authorized EMI, a Dedicated EMI shall maintain a minimum paid-up capital as specified in **Appendix 4** or as may be specified by the Bangladesh Bank from time to time, whichever is latest. In addition, the licensed EMI must maintain 1% of the average outstanding electronic money balance calculated over the last three months of the year ending as on 31 December.

61.2 The sponsor shareholders of any Dedicated EMI shall be prohibited from exiting, transferring, or otherwise disposing of their shareholding, in whole or in part, for a period of five (5) years from the date of issuance of the license by Bangladesh Bank.

61.3 Notwithstanding the provisions of 61.2, new shares may be issued to additional investors for the purpose of capital augmentation. Any shareholder, other than the sponsor shareholders, shall be subject to a lock-in period of three (3) years in respect of their shareholding.

61.4 However, publicly listed DEMIs are exempted from the provisions of 61.2 and 61.3.

61.5 Any Dedicated EMI which fails to maintain the required minimum paid-up capital as stipulated under **Paragraph** 61.1 above shall:

61.5.1 Submit a plan to Bangladesh Bank for approval as to how it intends to restore its paid-up capital to the required minimum level; and

61.5.2 Pay to the Bangladesh Bank on each day that the deficiency continues as penalty 0.05 percent of the difference between the capital that the EMI should have maintained and the level of capital actually maintained by the EMI.

61.6 Where the deficiency is not rectified within one hundred and twenty (120) calendar days after it has occurred, the Bangladesh Bank may suspend the license of the EMI or take such other punitive action as it deems fit.

61.7 Each director and chief executive officer of a Dedicated EMI which fails to comply with the minimum capital commits an offence and is liable on summary conviction to a fine not exceeding Taka 10 Lac that the Bangladesh Bank may impose.

62 Safeguarding of Funds

62.1 An EMI must ensure any funds collected in exchange of e-money issued are maintained separately in a separate account from other funds be it the EMI's working capital or any funds maintained for the EMI's other business or activity and are not commingled at any time with the funds

of any natural or legal person other than the e-money holders on whose behalf the funds are held.

62.2 A Dedicated EMI shall deposit the funds collected in exchange of e-money issued in a single or pooled Trust and Settlement Accounts with a scheduled bank after receiving it from a customer in accordance with the following requirements—

62.2.1 the funds can only be used for the following—

62.2.1.1 refund to customers;

62.2.1.2 payment to merchants for settlement of transaction conducted by the customer, including for repayment of any advance settlement by relevant intermediaries (e.g. payment system operator, acquirer) involved in making the payment to merchants; or

62.2.1.3 payment to another e-money account or bank account arising from a credit transfer transaction conducted by the customer.

62.3 A Dedicated EMI shall ensure that funds in the Trust and Settlement Account are at all times sufficient to cover the total outstanding e-money liabilities.

62.4 Where a Dedicated EMI's total outstanding e-money liabilities are greater than the funds in the Trust and Settlement Account, a Dedicated EMI is encouraged to deposit funds into the Trust and Settlement Account within one (1) working day to ensure **Paragraph** 62.3 is complied with.

62.5 In the interest of protecting e-money holders from the risk of bank insolvency, the sum total of e-money accounts held with any one scheduled bank on behalf of a given e-money issuer cannot exceed 15% of the net worth (total assets-total liabilities) of the scheduled bank. Whenever the threshold is exceeded on average for three consecutive months, the EMI must place any excess float in another scheduled bank. The terms and conditions of the account should require the float holding scheduled bank to promptly inform the EMI when the threshold is exceeded.

62.6 A Dedicated EMI shall ensure that it has sufficient liquidity for its daily operations. At a minimum, an EMI shall maintain a liquidity ratio of one (1).

63 Failure to comply with the provisions under this **Paragraph** shall impose a daily fine of Taka 5 (Five) Lac.

64 Investment of Funds

64.1 Dedicated e-money issuers shall keep 100% of the e-money float in liquid assets denominated in Bangladeshi Taka. The liquid assets shall remain unencumbered and may take the form of:

64.1.1 Cash balances held at scheduled banks in Bangladesh and withdrawable on demand, provided that such balances shall be held

separately from balances relating to any other operations of the Dedicated EMI; or

64.1.2 Short-term securities issued or guaranteed by the Government of Bangladesh or the Bangladesh Bank can be used for investment, with a maximum limit of one-third of the outstanding electronic money calculated at the end of the year on 31 December; and

64.1.3 Any other liquid assets or instruments as may be specified by the Bangladesh Bank.

64.2 Scheduled banks regulated under the Bank Company Act, 1991 are not subject to the liquid asset requirement under **Paragraph** 63.1 above, but are required to include e-money balances in the calculation of their statutory reserve requirement and liquidity requirement as prescribed by the Bangladesh Bank.

64.3 Dedicated EMIs shall on a daily basis, no later than 5.00 p.m. Bangladesh time each day, reconcile the liquid assets held by them for the redemption of e-money with the e-money value held by the customers, agents and merchants on their platforms. Any deficiencies in the amount of liquid assets held shall be rectified by 1.00 pm the next day.

64.4 Records pertaining to the above liquid assets as well as reconciliations shall be made available to the Bangladesh Bank for inspection at any time and the confidentiality of bank deposits shall be waived.

64.5 A violation of this requirement by EMIs shall attract a daily fine of not less than Taka 5 Lac as the deficiency persists, payable to the Bangladesh Bank.

65 Settlement of Transactions in Pooled Accounts

If a Dedicated EMI holds the e-money float with more than one bank, all settlement transactions between the respective bank accounts must be settled through one of the inter-bank payment systems operated by the Bangladesh Bank, i.e., NPSP, BEFTN, BACH or RTGS.

PART X: REGULATORY OVERSIGHT AND REPORTING

66 Oversight

The Bangladesh Bank shall in respect of e-money issuers exercise the oversight and supervisory powers and functions conferred on it by the Bangladesh Bank Order, 1972 (President's Order No. 127) and the Payment and Settlement Systems Act, 2024.

67 Regulatory Approval and Notification

67.1 An EMI shall seek the Bangladesh Bank's prior written approval on any proposed changes to its e-money business model that are significant or that changes the risk profile of its business model.

67.2 An EMI shall notify the Bangladesh Bank fourteen (14) days prior to establishing or relocating its offices in Bangladesh.

67.3 An EMI shall notify the Bangladesh Bank fourteen (14) days prior to the appointment of an auditor.

67.4 An EMI shall notify the Bangladesh Bank on the appointment of its chairman, director or CEO, within fourteen (14) days from the date of appointment.

67.5 The Bangladesh Bank may direct the EMI to terminate the appointment of its chairman, director or CEO if it determines that such appointment is not commensurate with the fit and proper criteria laid out in these Regulations or any other document issued from time to time.

68 Submission Requirements

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

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

68.3 An Authorized EMI is deemed to fulfill the requirement under **Paragraph** 68.2 upon submission to the Bangladesh Bank of its audited financial statements in accordance with the requirements of Bangladesh Financial Reporting Standard or as may be specified by the Bangladesh Bank and as amended from time to time.

68.4 A Dedicated EMI shall submit written assurance from its external auditor on the adequacy of controls for its safeguarding methods in accordance with **Paragraph** 62. At a minimum, the written assurance shall include a review of the following—

68.4.1 the separation of funds collected from customers, from other funds be it the working capital funds of the Dedicated EMI or funds for its other business;

68.4.2 ensure the balance of funds maintained by the Dedicated EMI under **Paragraph** 62.2 or 62.5, is greater than or at least equal to the Dedicated EMI's outstanding e-money liabilities;

68.4.3 the effectiveness of the controls put in place by a Dedicated EMI to ensure that the funds maintained by the Dedicated EMI under **Paragraph** 62.2 or 62.5 are topped up in a timely manner if the outstanding e-money liabilities of the Dedicated EMI are greater than the said funds; and

68.4.4 ensure the funds maintained by the Dedicated EMI under **Paragraph** 62.2 or 62.5 are only used for purposes permitted under these regulations.

68.4.5 The written assurance specified in **Paragraph** 67.4 from the external auditor shall include the method of assessment and basis of opinion on the compliance level. A Dedicated 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 Bangladesh Bank on an annual basis no later than three (3) months after its financial year-end.

68.5 An EMI shall submit monthly statistics on the operation of its e-money business to the Bangladesh Bank no later than the 15th day of the month following the reporting month using the format provided by the Bangladesh Bank via **EDW online submission** system. Primarily the following information are to be reported—

68.5.1 The names of e-money holders and their corresponding tier levels;

68.5.2 The number of registered and active e-money accounts issued by the EMI respectively broken down by type of account level, with activity counted on a ninety (90) day basis;

68.5.3 The volumes and values of all activity on its e-money platform broken down by type of transaction, including cash-in, cash-out and OTC transactions;

68.5.4 The number and types of registered and active agent locations in its network, including sub-agents not directly under contract with activity counted on a thirty (30) day basis;

68.5.5 The sum total of outstanding e-money balances held by the EMI;

68.5.6 The aggregate value of all float accounts used in the e-money business;

68.5.7 The value of each float account used in the e-money business held with respective banks;

68.5.8 The number and value of all dormant accounts;

68.5.9 Number of incidents of fraud, theft or robbery respectively, including at agent points;

68.5.10 Number of complaints received, broken down by category and agent location;

68.5.11 Number of complaints resolved and number currently outstanding

68.5.12 Number and type of material service interruptions and significant security breaches;

68.5.13 Suspicious transaction reports (STRs) generated;

68.5.14 Number of system outages that result in the inability of the customer to access his/her wallet(s) lasting more than 2 hours;

68.5.15 Such other information as may be required by the Bangladesh Bank from time to time.

68.6 Reports of all surveillance activities carried out by certified bodies should be submitted to the Bangladesh Bank;

68.7 On an ad-hoc basis, the e-money issuer shall report in writing to the Bangladesh Bank on the following, no later than ten (10) calendar days after occurrence—

68.7.1 Material changes of any of the items required to be included in the licensee's application;

68.7.2 Any transfer of shares that involves more than 15% of all shares or results in any shareholder acquiring or disposing of a significant shareholding of the e-money issuer;

68.7.3 Any material changes in the e-money service that changes the scope of the service, such as new service capabilities or a change in technology service providers;

68.7.4 Any indications of suspected or confirmed fraud relating to the e-money service, any security breaches, any material service interruption or other significant issues that may affect the safety and efficiency of the e-money service. This reporting shall also be made by the EMI to the Cyber Security Unit of Bangladesh Bank;

68.7.5 Any indications of loss of confidential data; and

68.7.6 Any other information that may be requested by the Bangladesh Bank or by the Bangladesh Financial Intelligence Unit.

68.8 Every e-money issuer shall get its books of accounts and IT systems audited and shall submit a copy of each to the Bangladesh Bank within three months of the close of the financial year.

68.9 Any substantial change or enhancement in the e-money payment system which an e-money issuer intends to introduce shall be subject to the approval of the Bangladesh Bank and the e-money issuer shall notify the Bangladesh Bank in writing thirty (30) days prior to the proposed implementation of the change or enhancement. A substantial change or enhancement is one that will expand the scope or change the nature of the e-money payment system and may include, among others, the following:

68.9.1 Additional functionality of the e-money payment instrument such as accessing new e-channels;

68.9.2 Change of payment service providers and other major partners in the business.

68.10 The Bangladesh Bank shall be allowed access to review the e-money systems and databases of the e-money issuer. Whenever the circumstances warrant, such access shall extend to the agents, partners, service providers, or outsourced entities of the e-money issuers in view of their participation in the business of issuing e-money.

68.11 The Bangladesh Bank may impose fines not exceeding Taka 1 Lac on an EMI for:

68.11.1 Non-submission;

68.11.2 Incomplete submission;

68.11.3 Delayed submission;

68.11.4 Inaccurate submission;

of the required information, data, statement or returns.

68.12 The Bangladesh Bank shall be allowed access to review the e-money systems, databases, and the operations of agents, partners, and service providers involved in the e-money business.

PART XI: CONSUMER PROTECTION

69 Principles of Consumer Protection

E-money issuers are under strict obligation to fully adhere to any rules issued by the Bangladesh Bank pertaining to consumer protection as well as such basic principles of consumer protection as:

69.1 Equitable, honest and fair treatment of all customers, notably, vulnerable groups such as the illiterate, women and the physically challenged.

69.2 Transparency and the disclosure of clear, sufficient and timely information on the fundamental benefits, risks and terms of any product or service offered in an objective and accessible form;

69.3 Sufficient and accessible information to customers on their rights and responsibilities;

69.4 Protection of customers' privacy as well as tangible and intangible assets related to the service, notably including personal details, financial information and transaction data;

69.5 Responsible business conduct of all staff and authorized agents; and

69.6 Adequate systems and processes for complaints handling and redress.

70 Responsibilities of E-Money Issuers

70.1 Every e-money issuer shall ensure high quality performance of the system. It shall promptly inform the e-money users about any disruption or anticipated disruption in the system. In so doing, it and any parties it directly or indirectly engages in the execution of its business shall comply with relevant sections of the Payment and Settlement Systems Act, 2024.

70.2 E-money issuers shall enter into a written agreement, physical or electronic, with every e-money account holder for whom they open an e-money account. The e-money issuer will provide explanation and product material on the general product elements to prospective clients and ensure that prospective clients have understood the general product elements even if they are not literate. The agreement shall at a minimum:

70.2.1 Clearly identify the e-money account holder;

70.2.2 If the payment system utilizing the e-money account is operated by a person other than the e-money issuer, clearly identify the name of the payment system provider;

70.2.3 Provide clear guidance on the e-money holders' right of redemption, including conditions and fees for redemption, if any;

70.2.4 State in its fine print that the ownership of the e-money holders' funds is not in any way impaired by the use of pooled float accounts established in the name of the EMI;

70.2.5 Include information on available redress procedures for complaints together with the address and contact information of the e-money issuer;

70.3 Any marketing by e-money issuers should follow the general principles of honesty and transparency. The addresses, telephone lines and e-mail address of the provider must be included in all physical marketing material;

70.4 Each e-money issuer shall provide a list with details about name of location of all its customer service points and its agents, and a description of its products and services including the applicable charges on its website;

70.5 All fees and service charges for e-money transactions shall be prominently displayed at its head office, branches as well as the premises of its agents using a standard summary sheet prescribed by Bangladesh Bank;

70.6 Each agent should be allocated a unique ID number that is prominently displayed at its agent location;

70.7 SMS messages or any other effective means of information, shall be sent to customers of agents whose agencies are terminated;

70.8 E-money issuers shall maintain a functional dispute and complaints resolution desk which shall be equipped to receive complaints through phone calls, e-mails, and personal visit by the e-money user;

70.9 Each e-money issuer shall display the address, telephone lines, and e-mail address of the complaint resolution desk prominently at its offices and agent locations.

71 Responsibilities of Trust Board

71.1 The Trust Board of an EMI shall independently notify each e-money account holder of the existence of their account with the EMI and the e-money balance in their respective e-money accounts at the end of each calendar year.

71.2 The Trust Board of an EMI shall independently notify the Bangladesh Bank of any material breach of trust, if any, by the EMI or any other members of the Trust Board as soon as any of the members of the Trust Board become aware of such material breach of trust.

71.3 Members of the Trust Board will individually or collectively be liable for any non-compliance of these regulations and/or non reporting of any material breach.

72 Complaint Procedures

72.1 E-money issuers shall set up effective procedures that allow e-money users to submit complaints. At a minimum, these procedures shall:

72.1.1 Provide easily understood information about the customer care system that should be easily accessible at least during normal business hours;

72.1.2 Allow for complaints to be lodged orally or in writing, but in each case the complaint must be lodged within a period of thirty (30) calendar days from the date of detection of the anomaly;

72.1.3 Be provided free of charge;

72.1.4 Provide for complaints to be resolved within five (5) working days of lodging. An additional ten (10) working days is permitted provided the customer is informed;

72.2 E-money issuers shall acknowledge all complaints filed with them within five days;

72.3 At the time of making a complaint the complainant shall be advised of the expected actions and timing for investigating and resolving the complaint;

72.4 E-money issuers shall put in place processes to provide complainants with sufficient information and the means to inquire on the progress of complaints and such processes may include complaint reference numbers or other identifiers in order to facilitate timely and accurate responses to subsequent inquiries by complainants;

72.5 Complainants shall be advised of the outcome of the investigation of their complaint, and any resulting decision by the e-money issuer;

72.6 The EMI shall establish an identified unit within its Compliance Function, separate from the Complaint Resolution Process, so that when a complainant is not satisfied with a decision reached pursuant to a complaint, the complainant can escalate the issue to that separate Complaint Resolution Process.

PART XII: TRANSFER AND TERMINATION

73 Exit Plan

73.1 An 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.

73.2 An EMI shall maintain an exit plan, which will enable the 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.

73.3 For the purpose of **Paragraph** 72.2, an EMI shall establish an exit plan valid for a three (3)-year period, which can be operationalized, if needed. At a minimum, the exit plan must include the following—

73.3.1 plausible internal triggers for exiting the business, which demonstrate unsustainable business, inability to fulfill the value proposition for its e-money business or materialization of risks beyond the EMI's own risk appetite;

73.3.2 likely options and related measures to be taken for exit that minimizes disruption to its customers, merchants and the payment ecosystem where it operates;

73.3.3 potential impediments to the execution of identified exit options and measures to mitigate the impact of such impediments;

73.3.4 sources of funding and liquidity for exit (in addition to safeguarding customer funds) and the estimated timeframe to exit the business;

73.3.5 the necessary capabilities required to extract and aggregate data on customers and/or merchants in a timely manner, upon request, including up-to-date contact information and refund/payment mechanism; and

73.3.6 the necessary capabilities and resources required to ensure continuity of services throughout the implementation of the exit plan, including the continuity of services under outsourcing arrangements.

73.3.7 In relation to **Paragraph** 72.3, a Dedicated EMI shall provide to the Bangladesh Bank, a comprehensive description of its exit plan as specified in **Appendix 5**.

73.4 An EMI is encouraged to consider the following exit triggers to be included in the exit plan—

73.4.1 Financial-related indicators which include but not limited to–

73.4.1.1 Significantly low return on equity for a continuous time period;

73.4.1.2 Significantly high cost-to-income ratio for a continuous time period; or

73.4.1.3 EMI's paid-up capital is eroded by 60% or more.

73.4.2 Operational-related indicators which include but not limited to–

73.4.2.1 Prolonged and/or frequent unscheduled downtime of e-money system.

73.4.2.2 Multiple successful cyber-attack incidences; or

73.4.2.3 Breaches of customer information with monetary impact to customer.

73.5 A Dedicated EMI shall submit an exit plan, together with an undertaking to the Bangladesh Bank within one (1) year from the effective date of this requirement, or upon submission of application to issue e-money. The subsequent exit plan and undertaking shall be endorsed by the board and submitted to the Bangladesh Bank within one (1) month after it being endorsed. The undertaking shall cover the Dedicated EMI's commitment to its exit plan if its internal triggers are met within the stipulated period.

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

73.7 The full implementation of the exit plan shall result in the cessation of the e-money business by the Dedicated EMI.

74 Transfer and Termination of E-money Services

74.1 Authorization or license to provide e-money services may not be transferred from one entity to another without the written approval of the Bangladesh Bank.

74.2 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 be commensurate with the nature, size and complexity of the EMI's e-money business and be made in accordance with relevant regulatory requirements

74.3 An EMI that has its approval to undertake e-money business is either revoked by the Bangladesh Bank or wishes to terminate its e-money business is obligated to wind down operations in a structured and orderly manner. In particular, such EMI shall continue to discharge its obligation which includes but not limited to the following—

74.3.1 refund, at no charge, 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;

74.3.2 contact and periodically provide reminders, through direct communication as well as public information via the media, to relevant stakeholders, which includes but is not limited to customers and merchants, for them to claim any unclaimed balances of e-money from the EMI, any procedures for retrieving their funds, the locations in which they can do so and the time span during which they can retrieve their funds.

74.3.3 provide adequate notice to the relevant stakeholders on its winding down or cessation of e-money business or operations and that it no longer has the approval under the Payment and Settlement System Act, 2024, to issue e-money; and

74.3.4 ensure customer information continues to be safeguarded and/or disposed appropriately in accordance with statutory records retention requirements.

74.3.5 ensure that the scheduled bank holding the e-money pooled account has updated identifying information of the associated customers and their respective balances. The scheduled bank is:

74.3.5.1 obliged to hold the funds and identifying information for no less than five years;

74.3.5.2 permitted to intermediate the funds and retain the proceeds;

74.3.5.3 after a period of five years has elapsed without claim from the original customer, the scheduled bank shall transfer all such funds to the Bangladesh Bank but retain all identifying information.

74.4 An EMI shall maintain relevant records and accounts to identify the beneficiaries of the e-money funds to enable the EMI to clearly identify and distinguish the funds maintained under **Paragraph**s 62.1 and 62.2 from other working capital funds of the EMI.

74.5 For purposes of **Paragraph** 73.4, a Dedicated EMI shall ensure these records and information are made available to the trustee who manages the Trust and Settlement Account required under **Paragraph** 62.2 to facilitate proper distribution of funds upon winding down or cessation of business or operations.

PART XIII: SANCTIONS AND PENALTIES

75 Penalties and Sanctions

75.1 Notwithstanding anything contained in Payment and Settlement Systems Act, 2024, the Bangladesh Bank shall prescribe penalties and sanctions for negligence or non-compliance with the provisions set forth in these Regulations. In particular as pertains to Customer Due Diligence and AML/CFT, penalties and sanctions shall be severe and may include fines, administrative penalties or revocation of the authorization to conduct e-money business as well as civil or criminal proceedings in a court of law.

75.2 The Bangladesh Bank may by notice in writing to an authorized e-money issuer, revoke or suspend an authorization for such period as it may specify, if the authorized e-money issuer:

75.2.1 Ceases to carry on business in Bangladesh or goes into liquidation, is wound up, or is otherwise dissolved; or

75.2.2 Fails to adequately comply with the provisions of these Regulations.

75.3 Before revoking or suspending an authorization under **Paragraph** 8 or a license under **Paragraph** 9 of these Regulations, the Bangladesh Bank shall give an e-money issuer not less than fourteen days' notice in writing and shall consider any representations made to it in writing by the e-money issuer within that period.

75.4 An EMI may appeal against any decision to the Governor of the Bangladesh Bank.

Appendix 1 Responsibilities of Board Committees

1 Board Risk Management Committee

1.1 Support the board in overseeing the implementation of the EMI's risk management framework, ensuring it effectively identifies, assesses, and manages material risks.

1.2 Support the board in determining the organization's overall risk appetite—the level of risk it is willing to accept in pursuit of its objectives.

1.3 Review and approve key risk management policies and procedures, including internal reporting mechanisms related to risk management.

2 Board Audit Committee

2.1 Support the board in ensuring that there is a reliable and transparent financial reporting process within the EMI.

2.2 Oversee the effectiveness of the internal audit function of the EMI. At a minimum, this must include—

2.2.1 reviewing and approving the audit plan, scope, procedures and frequency;

2.2.2 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

2.2.3 establishing a mechanism to assess the performance and effectiveness of the internal audit function.

2.3 Foster quality audits of the EMI by exercising oversight over the external auditor. At a minimum, this must include—

2.3.1 making recommendations to the board on the appointment, removal and remuneration of the external auditor;

2.3.2 monitoring and assessing the independence of the external auditor including by approving the provision of non-audit services by the external auditor;

2.3.3 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;

2.3.4 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

2.3.5 ensuring that senior management is taking necessary corrective actions in a timely manner to address external audit findings and recommendations.

2.4 Review and update the board on all related party transactions.

2.5 Review third-party opinions on the design and effectiveness of the EMI's internal control framework.

Appendix 2 Examples of arrangements excluded from the scope of outsourcing

1 Arrangements which entail procurement of services which are not performed by an EMI by itself in the ordinary course of its e-money business, 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—

1.1 services for the transfer, clearing and settlement of funds or securities provided by an operator of a designated payment system or an approved operator of payment system under the Payment and Settlement System Act, 2024;

1.2 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;

1.3 independent consultancy service (e.g. legal opinions, tax planning and valuation);

1.4 independent audit assessment;

1.5 clearing and settlement arrangement between clearing houses and settlement institutions and their members;

1.6 agent banking;

1.7 trustee arrangement;

1.8 credit or market information services;

1.9 repair, support and maintenance of tangible assets;

1.10 purchase or subscription of commercially available software;

1.11 maintenance and support of licensed software;

1.12 marketing and advertising;

1.13 telecommunication, postal and courier service;

1.14 physical security, premise access and guarding services; and

1.15 catering, cleaning and event services.

Appendix 3 Minimum Requirements on the Outsourcing Agreement

1 The outsourcing agreement shall, at a minimum, provide for the following—

1.1 duration of the arrangement with date of commencement and expiry or renewal date;

1.2 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;

1.3 controls to ensure the security of any information shared with the service provider at all times, covering at a minimum—

1.3.1 responsibilities of the service provider with respect to information security;

1.3.2 scope of information subject to security requirements;

1.3.3 provisions to compensate the EMI for any losses and corresponding liability obligations arising from a security breach attributable to the service provider;

1.3.4 notification requirements in the event of a security breach; and

1.3.5 applicable jurisdictional laws;

1.4 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;

1.5 ability of the EMI and its external auditor, including an agent appointed by the EMI, 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;

1.6 notification to the EMI of adverse developments that could materially affect the service provider's ability to meet its contractual obligations;

1.7 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;

1.8 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;

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

1.10 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;

1.11 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 (in this respect, the primary service provider must provide sufficient notice to the EMI before entering into an agreement with the sub-contractor). Therefore, the outsourcing agreement between the EMI and primary service provider must stipulate the following—

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

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

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

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

Appendix 4 Specification of Capital Requirements

1 Capital requirement

Type of Organization	**Paid-up Capital**
Payment Service Provider	Taka 20,00,00,000.00 (Taka Twenty Crore Only)
Authorized EMI	Must be able to maintain regulatory capital as per Bangladesh Bank's requirement for scheduled banks or financial institutions. No additional capital required.
Dedicated EMI	Taka 50,00,00,000.00 (Taka Fifty Crore Only)

2 Computation of capital funds

Particulars	**Amount**	**Amount**
Equity Capital		
Paid-up ordinary shares/common stock		xxxxxx
Paid-up irredeemable non-cumulative preference shares		xxxxxx
add **Reserves** General reserve fund *less* Intangible Assets[13]	xxxxxx (xxxxx)	xxxxxx
add Returned Earnings (or *less* Accumulated Losses)		xxxxxx
Add: Audited Net Income for the period (or *less* Accumulated Losses)		xxxxxx
Total Equity Capital		**xxxxx**

[13] Including goodwill, capitalized development costs, licenses and intellectual properties.

Appendix 5 Contents of an Exit Plan

1 An exit plan should consist of the following at a minimum

	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. • Policies, procedures and MIS to inform and support decision-making and smooth execution of exit plan
(b)	Exit triggers	• Identification of exit triggers, i.e. factors and indicators/thresholds that will prompt activation/execution of the exit plan. • The exit triggers at a minimum shall include compliance-related indicators, in particular on minimum capital funds, liquidity ratio and the safeguarding of customer funds. • Processes for continuous monitoring of factors and indicators/thresholds.
(c)	Measures to enable an orderly exit from the business while minimizing disruption to third parties, in particular customers and counterparties	• Identification of possible actions that can be undertaken under different scenarios. • Identification of possible funding sources to credibly 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 Bangladesh 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 responsible for ensuring the effective coordination and execution of the communication and engagement strategy

2 An EMI may take into consideration the following factors in determining the exit triggers—

2.1 Financial-related indicators which include but not limited to—

2.1.1 Significantly low return on equity for a continuous time period; or

2.1.2 Significantly high cost-to-income ratio for a continuous time period.

2.2 Operational-related indicators which include but not limited to—

2.2.1 Prolonged and/or frequent unscheduled downtime of e-money system.

2.2.2 Multiple successful cyber-attack incidences; or

2.2.3 Breaches of customer information with monetary impact to customer.