BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Governance, Risk Management, and Operations for Money Services Business (MSB)

Issued on: 9 April 2025 BNM/RH/PD 031-16

PART A: OVERVIEW

1. Objective

1.1 The money services business (MSB) industry has continued to evolve in support of the needs of the economy with the provision of services now available through digital channels to complement the traditional branch and agent networks. The myriad of service channels has provided consumers with much easier access and enhanced user experience. Industry players have also strengthened with higher levels of business professionalism and compliance standard. Notwithstanding these positive developments, continuous efforts to further strengthen the industry is important particularly considering the unique and distinct risk nature of MSB, which can be highly susceptible to abuse. Increased use of technology also heightens MSB exposure to it associated risks. In view of this, enhancements to regulatory requirements for the MSB industry, particularly in terms of governance, risk management, operational requirements, and IT requirements, is timely and important to reflect these significant developments.

1.2 Section 36 of the Money Services Business Act 2011 (the Act) requires all MSBs to institute and maintain sound governance and operational arrangements to ensure the professional and prudent conduct of the MSB. The Money Services Business (Duties of Licensees) Regulations 2012 further prescribe key requirements that MSBs must observe to ensure effective and robust internal control systems that promote the safety and integrity of MSB activities. This policy document sets out the minimum standards that MSB must observe in implementing sound governance, appropriate risk management and robust internal control systems for their business. These requirements amongst others will contribute towards strengthening consumer protection and safeguarding the MSB industry from being used as a conduit for illegal activities, money laundering and terrorism financing.

2. Legal Provisions

2.1 This policy document is issued pursuant to section 74 of the Act.

3. Applicability

3.1 This policy document is applicable to MSBs licensed under the Money Services Business Act 2011.

4. Effective Date

4.1 This policy document comes into effect on 9 April 2025.

5. Policy Documents Superseded

5.1 This policy document supersedes the guidelines, circulars and notifications outlined in **Appendix I**.

6. Relationship with Existing Policies

6.1 Where applicable, this policy document must be read together with the Act and other relevant legal instruments and policy documents that have been issued by the Bank, and any subsequent review of such documents, in particular:

(a) The Money Services Business Regulations 2012 on:

(i) Minimum Criteria of a “Fit and Proper” Person (referred to as ‘Fit and Proper Regulations’ in this document);

(ii) Licensing (referred to as ‘Licensing Regulations’ in this document);

(iii) Duties of Licensees (referred to as ‘DL Regulations’ in this document); and

(iv) Remittance Business (referred to as ‘Remittance Regulations’ in this document).

(b) Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions (AML/CFT/CPF and TFS for FIs).

(c) Agent Oversight Framework for Money Services Business.

7. Interpretation

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

7.2 For the purposes of this policy document:

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

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

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

"**annual turnover**" refers to:

(a) for a MSB who carries on money-changing business, the average of its annual value of buy and sell of foreign currencies for the preceding three financial years certified by the auditor of the MSB; or

(b) for a MSB who carries on remittance business, the average of its annual value of inward and outward remittance transactions for the preceding three financial years certified by the auditor of the MSB;

"**Bank**" refers to Bank Negara Malaysia;

"**banking institution**" refers to a licensed bank as defined under the Financial Services Act 2013, a licensed Islamic bank as defined under the Islamic Financial Services Act 2013, and a prescribed development financial institution under the Development Financial Institutions Act 2002;

"control function" refers to a function that has a responsibility independent from business lines to provide objective assessments, reporting and assurance on the effectiveness of a MSB's policies and operations, and its compliance with legal and regulatory obligations;

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

"**customer or user**" refers to any person who uses the MSB's services or systems;

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

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

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

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

"**electronic terminal**" refers to an office[1] where the MSB transaction process[2] is undertaken electronically. This may include self-service machines such as automated self-service kiosks, ATMs, as well as digital MSB platforms via mobile or online channels;

"**framework**" refers to the set of rules and controls governing a MSB's organisational and operational structure, including reporting processes and control functions;

"**highly complex MSB licensee**" refers to a MSB that is:

(a) licenced to conduct remittance business;
(b) approved as a principal that can appoint agent(s);
(c) approved as an e-money issuer[3];
(d) approved to provide services via electronic terminals; or
(e) specified by the Bank as such;

"**industry association**" refers to Malaysian Association of Money Services Business (MAMSB) or any other associations as specified by the Bank;

"**Intermediary Remittance Institution or IRI**" refers to an intermediary institution that receives wire transfers on behalf of a sending remittance company, for onward transmission, to a receiving party that will then disburse to the beneficiary of the wire transfer;

"large MSB" refers to MSB with an annual turnover value exceeding RM100 million;

---

1 For avoidance of doubt, each mobile application or web portal that is unique in substance and can be materially differentiated from one another should be considered as one office, and shall require the necessary approval. Whereas, platforms of similar substance with immaterial differences in particulars, shall be considered as a single office.

2 MSB transaction process refers to the conduct of-
(a) exchange transactions for money changing business;
(b) transfer of funds for remittance business;
(c) import or export of foreign currency notes for wholesale currency business.
For avoidance of doubt, this excludes electronic terminals that only conduct the e-KYC process (as approved by the Bank pursuant to AML/CFT/CPF and TFS for FIs policy document) or booking process.

3 Refers to approved e-money issuers that are subject to the E-money policy document.

"**management**" refers to the Chief Executive Officer and senior officers including Compliance Officer;

"medium MSB" refers to MSB with an annual turnover value of more than RM30 million but not exceeding RM100 million;

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

"outsourcing arrangement"[4] refers to an arrangement whereby a service provider performs an activity on behalf of the MSB on a continuing basis, where the activity would otherwise be undertaken by the MSB;

"person entrusted with prominent public functions" refers to an individual who is currently entrusted with prominent public functions domestically or by a foreign country, with decision-making authority over or with access to state assets and funds, policies and operations, including control over regulatory approvals, and awarding licences and concessions. For the purpose of this policy document, it refers to Heads of State, senior government officials, as well as senior judicial, military or police officials;

"**principal licensee**" refers to a MSB which has obtained the written approval of the Bank to appoint a money services business agent under section 43 of the Act;

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

"service provider" refers to a group affiliate or external entity, providing services to a MSB under an outsourcing arrangement; and

[4] For avoidance of doubt, a principal-agent arrangement is not considered as an outsourcing arrangement.

"small MSB" refers to MSB with an annual turnover value not exceeding RM30 million.

PART B: GOVERNANCE

8. Governance Arrangement

S 8.1 A MSB shall establish an appropriate governance framework, which is effective and transparent, to preserve the integrity and professionalism of its business, which includes, among others, the following:

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

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

(c) segregation of duties and internal control arrangements to prevent mismanagement, fraud, as well as abuse of the MSB for illegal activities.

S 8.2 Notwithstanding 8.1(b) above, for small MSB where there is no effective separation between the board, owners and management, internal controls put in place shall inculcate good corporate culture that reinforces ethical, prudent, and professional behaviour.

9. Board of Directors

S 9.1 The board shall set out the mandate, responsibilities, and procedures of the board and its committees (if any), including the matters reserved for the board's decision.

9.2 Board Responsibilities

S 9.2.1 The board has the overall responsibility for promoting the sustainable business growth and financial soundness of the MSB, ensuring fair and honest dealings with consumers, and preventing mismanagement, fraud, and abuse of the MSB for illegal purposes. In fulfilling this role, the board shall:

(a) approve the risk appetite, business plans, and other initiatives which would individually or collectively, have a material impact on the MSB's risk profile. For such approvals, the board shall also take into

consideration the MSB's capacity and ability to ensure full compliance with regulatory requirements;

(b) oversee the selection, appointment and performance of management on an ongoing basis, in achieving the business objectives set by the board and in meeting the legal and fiduciary duties of the MSB. This includes:

(i) ensuring the CEO is fit and proper, competent and capable to effectively manage the business in compliance with relevant laws and regulations; and

(ii) appointing a Compliance Officer who has an adequate working knowledge and can effectively support the MSB's compliance with AML/CFT/CPF requirements. For this purpose, the Compliance Officer shall, at minimum, meet the requirements as outlined in Appendix II.

(c) ensure the appropriate policies and processes (including standard operating procedures) as well as systems and controls to manage risks in its business are put in place. The board should establish a process to facilitate periodic review of the policies, processes, systems and controls to ensure they remain relevant;

(d) oversee the implementation of the MSB's governance framework and internal control policies, and periodically review whether these remain appropriate in light of material changes to the size, nature, and complexity of the MSB;

(e) promote timely and effective communication between the MSB and the Bank on matters that are affecting or may affect the safety, soundness and integrity of the MSB;

(f) ensure the management provides adequate reporting to the board on timely basis on the MSB's overall business performance which include the business trend, the profile of customers and business partners[5], the reputation of the business within the industry and the standard of service provided to customers, as well as compliance with MSB regulatory and AML/CFT/CPF requirements;

[5] Business partners refer to any business relationships that are established by the MSB with other parties in relation to its money services business.

(g) ensure any rectification measures taken by management arising from any board concerns or supervisory findings by the Bank relating to the operations of MSB are satisfactorily addressed in a timely manner;

(h) exercise reasonable due diligence to ensure that an external auditor appointed by the MSB is professionally competent and fulfils the requirements stipulated in the DL Regulations. This includes checking and confirming the track record of the auditor, either by engaging the auditor itself or by checking with relevant governing body or associations prior to engaging the services of the external auditor;

(i) ensure that the MSB is formally registered as a member of an industry association of MSB; and

(j) avoid any decisions or actions that would expose the MSB to legal and reputational risks such as allowing any part of the MSB or property of the MSB to be used for unauthorised activities or facilitate unauthorised access to information relating to the MSB's business for personal advantage.

G 9.2.2 In addition to paragraph 9.2.1, the board is encouraged to ensure that the MSB's Compliance Officer be duly certified/accredited by relevant recognised certification/ accreditation bodies as having acquired the knowledge required to effectively perform the AML/CFT/CPF compliance function in a MSB.

S 9.3 In addition to paragraphs 9.1 and 9.2, the board of a medium MSB and large MSB shall:

(a) establish a code of ethics to ensure proper conduct of business at all times;

(b) appoint a dedicated[6] Compliance Officer to perform the compliance function for the MSB; and

(c) ensure they remain updated on good risk management practices. This includes participating in the Money Services Business Directors' Education Program (MSB-DEP) or similar programs as specified by the Bank, within the timeline in Appendix III.

[6] For the avoidance of doubt, the Compliance Officer shall be primarily responsible for the compliance function and is not allowed to assume the role of the CEO at the same time.

9.4 Board Appointments

S 9.4.1 A director shall fulfil the minimum fit and proper criteria set out in paragraph 11 at the time of appointment and on a continuing basis.

S 9.4.2 A director of MSB shall not be an active politician or a person entrusted with prominent public functions domestically or by a foreign country.

9.5 Composition of the Board

S 9.5.1 The board and board-level committees (if any) shall be of a size and composition that promotes effective deliberation and oversight, proportionate to the scope and complexity of the MSB activities.

S 9.5.2 In situations[7] where the board composition is not able to provide effective deliberation and oversight, including where the MSB is left with only one board member due to the demise of a member or any other unforeseen circumstances, the MSB shall make an application to the Bank within three (3) months to appoint new board member(s).

S 9.5.3 In promoting an effective system of checks and balances[8] and ensuring adequate focus is given to broader issues related to a MSB's business objectives and strategy, the board of a medium and large MSB shall ensure the following:

(a) at least one third of board members are independent from day-to-day management of the MSB business. Notwithstanding this, the Bank may require a MSB to increase the representation of independent directors in the board if it deems necessary; and

(b) board comprise of members with an appropriate mix of knowledge, skills, and experience to be able to provide direction and effective oversight to the business of the MSB.

[7] The situation may arise either from MSB's own assessment or as requested by the Bank.

[8] An effective system of checks and balances is important to ensure the board can take an objective view of the operations of the MSB and management's performance, and direct appropriate changes where needed.

G 9.5.4 For small MSBs where there is no effective separation between the board, owners, and management, the MSB is encouraged to appoint an external auditor to provide independent assurance on compliance with regulatory requirements.

S 9.5.5 Notwithstanding paragraph 9.5.4 above, the Bank reserves the right to require such MSB to appoint an external auditor to meet the requirements of the paragraph. In such circumstances, the cost of the audit shall be borne by the MSB.

9.6 Board Meetings

S 9.6.1 A director shall devote sufficient time and commitment to prepare for and attend board meetings.

S 9.6.2 For a medium MSB and large MSB:

(a) a director shall attend at least 75% of the board meetings held in a financial year;

(b) a director shall not appoint another person to attend or participate in a board meeting on his/her behalf. This includes appointing alternate directors; and

(c) the quorum for board meetings shall be represented by at least half of the board members.

G 9.6.3 A small MSB is strongly encouraged to also adopt expectations in paragraph 9.6.2 to inculcate professional and proper board meeting practices.

S 9.6.4 The board shall ensure that appropriate safeguards are instituted to preserve the confidentiality of all board meetings, regardless of whether such meetings are conducted physically or virtually.

S 9.6.5 The board shall ensure that clear and accurate minutes of board meetings are maintained to record the attendance and decision of the board, including key deliberations, rationale for each decision made, status of rectification measures/actions taken, any significant concerns or dissenting views and actions directed by the board which requires subsequent monitoring and follow up by the board.

10. Chief Executive Officer (CEO)

S 10.1 The CEO is primarily responsible for managing the day-to-day business operations of the MSB and has a key role in ensuring that the operations of the MSB is carried out ethically and professionally with integrity. In this regard, the specific responsibilities of the CEO shall include the following:

(a) ensure that internal policies, processes, systems and controls are effectively implemented and properly communicated to the relevant employees. This includes establishing clear procedures, effective reporting and information systems, and appropriate lines of authority and accountability for key business activities;

(b) promptly inform the board of any material lapses in controls which could expose the MSB to legal, financial, reputational, technology, or cyber risks;

(c) ensure that corrective actions taken are effective and implemented in a timely manner;

(d) ensure employees are competent, professional and provided with relevant training such as on money services business operations and regulatory requirements, AML/CFT/CPF requirements and customer service in managing the daily business operations. The CEO shall be responsible to ensure that suitable background checks are conducted on prospective employees. The CEO should also ensure that those with responsibility for managing any part of the business (e.g. branch managers) meet the fit and proper criteria as required under the Act and elaborated in this policy document;

(e) monitor closely the staff’s performance and ensure they understand and apply the knowledge acquired in carrying out their respective roles and functions accordingly;

(f) develop appropriate AML/CFT/CPF policies and procedures for the operations of the MSB, which takes into account the level of risk exposures based on appropriate factors such as its location, profile of customers, and size or volume of transactions performed;

(g) ensure compliance with applicable regulatory requirements and laws[9] in all aspects of the business, and institute effective systems and processes for monitoring compliance, including by branches and agents of the MSB, on an ongoing basis;

(h) respond to supervisory requests for information and address any supervisory concerns of the Bank in a timely manner;

(i) ensure proper, accurate and complete records of all business transactions, including any reports required to be submitted to the Bank; and

(j) avoid any actions that would expose the MSB to legal and reputational risks which include allowing any part of the MSB or property of the MSB to be used for any unauthorised activities or facilitate unauthorised access to information relating to the MSB's business for personal advantage.

S 10.2 A CEO who is the principal person responsible for the day-to-day business operations, shall devote the whole of his professional time and commitment to the service of the MSB that he is serving in.

S 10.3 Notwithstanding paragraph 10.2, in situation where the MSB is allowed to engage in other business or activity and the CEO is also managing such business, the CEO shall ensure that such activities shall not interfere or pose conflicts with his primary responsibility towards the MSB.

S 10.4 A CEO shall have his principal or only place of residence within Malaysia unless the Bank approves otherwise in writing.

[9] This refers to the Money Services Business Act 2011, and include, but not limited to the Financial Services Act 2013, Islamic Financial Services Act 2013, Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, Companies Act 2016, Personal Data Protection Act 2010, Competition Act 2010, and Unclaimed Monies Act 1965.

S 10.5 A CEO of a medium MSB and large MSB shall participate in the MSB-DEP or similar programs as specified by the Bank, within the timeline in Appendix III, to ensure adequate level of competency.

10.6 Appointment of acting person during the CEO's absence

S 10.6.1 In the event that the CEO is absent from duties, the board shall ensure proper arrangements are in place for business operations to remain properly run and managed. In this regard, the board shall ensure the following:

(a) to appoint an acting person to oversee the MSB's day-to-day business operations in the event that the CEO will be absent from his/her duties for a consecutive period of more than seven (7) working days; and

(b) to identify a new CEO in accordance with the requirements under the Fit and Proper Regulations and obtain prior written approval from the Bank for the appointment, in cases of a prolonged absence of the CEO for a consecutive period of more than three (3) months.

S 10.6.2 For the purpose of meeting the requirements in paragraph 10.6.1 (a), the acting person shall be empowered by the board to be able to effectively act on matters relating to the MSB operations. In relation to this, the board shall:

(a) appoint a qualified person at the director or management level to assume the acting role;

(b) clearly define any limits to the authority of the acting person; and

(c) notify the Bank in writing within fourteen (14) days on the appointment of the acting person, with the following information:

(i) duration and reason for the CEO's absence; and

(ii) name, current designation, contact number and e-mail address of the acting person.

10.7 Conflict of interest

S 10.7.1 In the event of any conflict of interest between the director and/or the CEO with the activities of the MSB, the director or CEO shall disclose such conflicts in accordance with the law and internal policies of the MSB, and shall always act in the best interests of the MSB**.**

11. Fit and Proper

G 11.1 In determining whether a person meets the minimum criteria of a "fit and proper" person, the Bank will also consider the relevant factors set out in this policy document to form a judgment on whether a person meets the fit and proper criteria. Where any of the factors below exist, due consideration will also be given to the surrounding circumstances of a case (for example, period of time passed since the event occurred) to determine whether a person would still meet the fit and proper criteria.

G 11.2 In determining whether a "person is of probity, personal integrity and good reputation" as outlined in the Fit and Proper Regulations, relevant factors assessed by the Bank will include whether the person has:

(a) been subject to any disciplinary or criminal proceedings of a nature that raises reasonable concerns regarding his character and professional integrity;

(b) contravened or failed to comply with any legal and regulatory requirements or standards, including requirements and obligations under tax, immigration and customs laws;

(c) been associated, as a controller or through a position of significant influence, with any business that has been investigated, disciplined, suspended or reprimanded by a regulatory body, professional body, trade association, court or tribunal;

(d) been involved in any deceitful, unlawful, or improper business practices. This includes allowing any facilities (including financial facilities) belonging to the person to be used for such purpose;

(e) been dismissed, asked to resign or has resigned from employment because of questions about his honesty and integrity;

(f) owned or managed any business or association whose registration, authorisation, membership or licence to operate has been refused, revoked, withdrawn or terminated;

(g) acted unfairly or dishonestly in his dealings with his customers, employer, auditors and regulatory authorities;

(h) shown objection to, or disregard for or acts in a manner contradictory to, actions required by regulatory authorities to address matters of concern to the regulator; and

(i) been a party to any action or decision of the board or management of a MSB which exposed the MSB to significant reputational, financial, or legal risks.

G 11.3 In determining whether a "person has managed his financial affairs properly and prudently", as outlined in the Fit and Proper Regulations, relevant factors assessed by the Bank will include whether the person:

(a) has taken on excessive debt beyond his means to repay the debt;

(b) is able and willing to meet his financial commitments, including any debt obligations, in a timely manner without substantial hardship; and

(c) has been subjected to legal actions to recover debts owed by him.

PART C: OPERATIONAL REQUIREMENTS

12. Local Incorporation

S 12.1 A MSB shall be a company incorporated under the Companies Act 2016 [*Act 777*].

13. Restriction of Business

S 13.1 A MSB shall only offer money services business activities according to the type of its licence unless prior written approval of the Bank has been obtained pursuant to section 19 of the Act for the MSB to undertake any other business.

G 13.2 In assessing such requests, the Bank will consider, among others, the business synergies and benefits to consumers, the associated risks arising from the new business and risk mitigation plans.

14. Conduct of Business

14.1 Issuance of receipts

S 14.1.1 A MSB shall display prominently at its approved offices a notice in the format below informing its customers to request for a receipt.

Notice to Customer
Issuance of receipts is a requirement under the Money Services Business Act 2011. Please insist on a receipt for your transaction.

Notis kepada Pelanggan
Pengeluaran resit adalah satu keperluan di bawah Akta Perniagaan Perkhidmatan Wang 2011. Sila minta resit bagi transaksi anda.

S 14.1.2 Further to section 27 of the Act and DL Regulations, a MSB shall ensure that all customer receipts issued by its respective offices (such as head office, electronic terminals, branches, and agents) are serialised in a sequential order. This may include a series of numerical or alphanumerical identifiers, that can facilitate easy tracking while also enabling the MSB to ensure completeness of the transaction records.

S 14.1.3 A MSB shall ensure that all business transactions undertaken at its offices are fully accounted for and supported by receipts issued. This includes payment made via electronic channels such as debit card, credit card, and online transfer.

14.2 Display of information of business

S 14.2.1 A MSB who is approved by the Bank to appoint agent(s) shall issue a certificate of appointment to its agent(s).

S 14.2.2 A MSB shall ensure that its agent(s) displays the certificate of appointment prominently at its premises to facilitate customers' verification of the legitimacy of the agent to conduct MSB.

S 14.2.3 A MSB shall prominently display the membership logo of the industry association at all its offices. For MSB with agents, the MSB shall ensure that its agents also display the membership logo at their premises.

G 14.2.4 A MSB conducting business via electronic terminals should refrain from displaying the full copy of its licence digitally on any of its electronic terminals to minimise risk of forgery. Notwithstanding this, in facilitating the customer to verify authorisation of the company, MSB may consider providing information of its nearest physical premises to facilitate validation process by the customer or relevant links to its webpage that can confirm the status of the MSB[10].

S 14.2.5 A MSB that offers its service through electronic means or temporary premises (e.g., mobile kiosk, temporary booth, counter) approved by the Bank, shall prominently display information of its business in the manner set out in Appendix IV, including the means for customers to verify the authorisation by the Bank of the services offered.

[10] This may include list of regulated entities published by the Bank on the Bank's website.

14.3 Exchange Rate Quotation

S 14.3.1 The exchange rates quoted by a MSB for all MSB transactions with its customers shall be based on the prevailing market rates when the transactions are executed. However, a MSB may set its dealing spread[11] on buying and selling of currencies.

S 14.3.2 In setting the dealing spread, a MSB shall strictly avoid any anti-competitive behaviours that are in breach of the Competition Act 2010, which include, but not limited to, undertaking predatory pricing and colluding with other MSB.

S 14.3.3 The exchange rate used for the final transaction shall not be less favourable than the exchange rate disclosed to customers.

S 14.3.4 A MSB shall obtain the Bank's written approval prior to engaging in forward exchange transactions with its customers.

15. Transparency in Dealings

S 15.1 All information disclosed to customers shall be clear, visible, and not misleading.

S 15.2 A MSB shall provide adequate information on how customers can lodge a complaint in respect to its provision of service. Such information should include the following:

(a) contact details of the person responsible or complaints unit of the MSB;
(b) information on channels for lodging complaints e.g. by email, phone; and
(c) response time in addressing the complaints.

G 15.3 In respect to paragraph 15.2, a MSB may provide the information in the receipt, affixed at the MSB's premises or on the MSB website.

[11] The spread refers to the percentage difference the between buying and selling rate of the foreign currencies.

S 15.4 A MSB shall provide clear information on procedures for the cancellation of transactions by customers. If the cancellation of a transaction is due to the MSB's failure[12] to honour the transaction performed with or on behalf of customers, the MSB shall refund the customer's funds in full without undue delay which shall not exceed seven (7) days from the date of cancellation of the transaction.

16. Opening and Maintaining of Bank Account

S 16.1 A MSB shall open and maintain one or more bank accounts under its name with banking institutions for the conduct of the MSB business.

S 16.2 No personal bank account of the directors, employees or any other persons shall be used by the MSB for the conduct of its MSB business.

S 16.3 The MSB's bank account(s) shall be used strictly for the conduct of the MSB business only.

17. Business Hours

S 17.1 A MSB shall operate its business for a reasonable number of hours in a day based on the market it serves to ensure reliable service and convenient access by its customers.

G 17.2 Notwithstanding paragraph 17.1, in ensuring easy access by the customer, a MSB operating at a physical office should operate within normal business hours.

[12] For avoidance of doubt, this includes MSB's own failure or failure attributed to any other parties involved in the process of honouring the MSB transaction such as service providers and correspondent agents.

18. Opening or Relocating an Office

S 18.1 A MSB shall establish an office in Malaysia to facilitate smooth and effective communication with the Bank.

S 18.2 In applying for an approval to open or relocate a temporary office, a MSB shall, where necessary, state the duration of such operations in addition to the required information as prescribed in DL Regulations.

S 18.3 A MSB shall notify the Bank in writing of the date of commencement and address of its new office, at least fourteen (14) days before commencing the operation at the new location.

19. Sharing of Premises

S 19.1 Where a MSB plans to carry on its business in a premises shared with other businesses, the MSB shall notify the Bank prior to the sharing of such premises.

S 19.2 A MSB that shares premises with other businesses, regardless of whether such other businesses are related to or not part of the MSB, shall ensure that:

(a) the MSB is physically separated from the other businesses and clearly identifiable by customers through proper signage;

(b) any funds and property belonging to the MSB are completely segregated from the other businesses conducted at the same premises; and

(c) proper controls are in place to prevent unauthorised access to the MSB's business, including its systems, records, and funds.

20. Closure of Office

S 20.1 A MSB shall notify the Bank prior to any temporary closure or planned suspension of services that exceeds seven (7) days.

S 20.2 A MSB which temporarily closes any of its offices or suspends services provided by its agents, shall affix a written notification on the outside of the affected office to inform customers of the period of closure. The notification shall include providing alternative contact details for customers to reach to address issues arising from such disruptions, if relevant.

S 20.3 Notwithstanding paragraph 20.1 and 20.2, a MSB operating via electronic terminals which temporarily suspends its services shall:

(a) notify their customers in advance or on an immediate basis, in any possible manner for any suspension of service including suspension of service arising from scheduled temporary system unavailability or unexpected disruptions to the system. The notification shall include providing alternative contact details for customers to reach to address issues arising from such disruptions if relevant; and

(b) implement appropriate measures to ensure minimal disruption time to the electronic services provided to the customers.

S 20.4 A MSB shall notify the Bank prior to any permanent closure of its offices, including arising from surrender of license under section 16 of the Act, or termination of services of its agents. The notification shall state the reasons and the effective date of the closure or termination.

S 20.5 In respect to paragraph 20.4, a MSB shall ensure that the business signages are removed from the offices or the premises of the agents no later than one (1) business day from the effective date of the permanent closure or agent termination as notified to the Bank.

21. Licence and Fee

21.1 Renewal of licence

S 21.1.1 A MSB shall renew its licence by submitting a written application to the Bank no later than two (2) months before the expiry of its licence. The application shall include information as prescribed in the Licensing Regulations.

21.2 Timing to return licence to the Bank

S 21.2.1 A MSB shall return the licence to the Bank within fourteen (14) days from:

(a) the effective date of business closure arising from voluntary surrender of licence pursuant to section 16 of the Act;

(b) the date of expiry of the licence;

(c) the date the refusal to renew the licence takes effect under subsection 9(10) of the Act; or

(d) the date the revocation of the licence takes effect under subsection 12(6) of the Act.

21.3 Refund of fee

S 21.3.1 There shall be no refund of any annual fee or processing fee paid pursuant to section 8 of the Act by the Bank to any person, in the event a licence is revoked, or not renewed by the Bank, or surrendered to the Bank before the expiry of the licence.

22. Advertisement

S 22.1 A MSB and its agent shall ensure that any advertisement issued or published directly or indirectly through a service provider in respect of the business is fair and clear, contains information that is accurate and relevant, and should not be misleading or deceptive to customers and the public. The information contained in the advertisement shall be consistent with the level of services offered by the MSB.

S 22.2 In facilitating easy identification and verification by customers, the advertisement at minimum, shall incorporate information which includes but are not limited to the following:

(a) name and contact details of the MSB / agent; and

(b) type of money services business being offered.

S 22.3 A MSB is not allowed to use the logo and the name “Bank Negara Malaysia”, including any abbreviations in advertisements or any other marketing and promotional materials, including on its signboard, website, letterhead, business card, poster, brochure, leaflet, banner, and bunting.

23. Outsourcing

S 23.1 A MSB shall remain responsible and accountable for any services outsourced to a service provider under an outsourcing arrangement.

S 23.2 In embarking into an outsourcing arrangement, a MSB shall:

(a) obtain the board’s approval to outsource any functions related to money services business. The board shall be accountable in ensuring effective oversight and governance of the outsourcing arrangements. Such outsourcing arrangements shall be supported by a robust risk management framework to ensure compliance with relevant laws, regulations, and prudential requirements related to the outsourced activities;

(b) identify and have in-depth and holistic understanding of potential risks arising from the outsourcing arrangement. The scope and nature of services and operations to be performed by the outsourced service provider should not compromise the controls and risk management of the MSB; and

(c) have arrangements in place to monitor and ensure the continuity of the services outsourced[13]. At a minimum, this shall include contractual terms and conditions governing obligations and responsibilities of all parties (such as contractual parties’ termination rights and a minimum period to execute the termination provisions), and appropriate reporting and support mechanisms. Notwithstanding, the arrangement shall not limit the Bank’s ability to exercise its regulatory or supervisory powers, particularly on timely and unrestricted access

[13] Where relevant, this should be read together with paragraph 29.7 on Business Continuity Management.

to systems, information or documents relating to the outsourced arrangement. This includes the ability to conduct on-site inspections on the service provider, as well as to obtain any reports or findings made in relation to the outsourced function.

S 23.3 A MSB shall obtain the Bank's written approval prior to:

(a) implementing its material outsourcing arrangements; or

(b) making significant changes to an existing material outsourcing arrangement.

S 23.4 For the purpose of paragraph 23.3, material functions are functions that fulfil the following guiding principles:

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

(b) the outsourced function may impact the security, confidentiality, and integrity of customers information; or

(c) significantly influences the ability of MSBs to achieve its strategic and business objectives.

S 23.5 For the avoidance of doubt, the following functions are deemed as material MSB functions which require prior written approval from the Bank before MSB may outsource such functions:

(a) compliance, including key sub-functions such as, but not limited to, customer data protection, customer fund management, and AML/CFT/CPF transaction monitoring;

(b) finance and treasury;

(c) product management and development; and

(d) internal audit.

S 23.6 In making an application pursuant to paragraph 23.3, a MSB shall at minimum, provide the following information to the Bank:

(a) the function being outsourced;

(b) party outsourced to;

(c) rationale for the outsourcing arrangement or significant changes to be made to an existing material outsourcing arrangement; and

(d) any other information as the Bank may specify.

Notwithstanding the above, a MSB shall continue to maintain relevant information on all its outsourced functions, which shall be made available to the Bank upon request.

S 23.7 Without limiting to the generality of paragraph 23.5, small and medium MSBs are not required to obtain prior written approval from the Bank to embark on outsourcing arrangements for the internal audit function.

S 23.8 A MSB shall terminate the outsourcing arrangements with a service provider, at any time as the Bank may instruct.

24. Requirements on Using a System Offered by a Service Provider

S 24.1 In addition to the requirements in paragraph 23, a MSB that uses a system offered by a service provider, where it is connected to the MSB's internal network of systems, shall:

(a) clearly specify the responsibilities and expectations of the system service provider, including establishing user access rights at the service provider's end, and recourse available to the MSB where the agreed terms of service are not met;

(b) conduct appropriate due diligence at the point of considering new service level agreements (SLA) and renewing or renegotiating existing SLAs, to assess the ability of the system to perform the service in a manner that fully satisfies requirements specified by the Bank. This shall include the following:

(i) maintenance of robust and reliable management information system as stipulated under paragraph 30.2; and

(ii) remittance system requirements stated in paragraph 25.2, for MSB that conducts remittance business;

(c) review recent reports on independent security audits performed on the system; and obtain assurance that such audits are conducted at least once every three years. If there are material findings in the

independent security audit report, the MSB shall not use the system until the identified gaps are fully rectified to the satisfaction of the MSB and in compliance with requirements in this policy document; and

(d) ensure that the system service provider can protect the confidentiality of customers' information and to ensure that such information is not used or disseminated for any other purposes.

This shall be read together with paragraph 30.1.2 accordingly.

25. Specific Requirements to Conduct Remittance Business

25.1 Customers' Fund Management

S 25.1.1 Further to section 37 of the Act, a MSB which carries on remittance business shall ensure that customers' funds can be reconciled with the total liabilities relating to its remittance business at all times[14].

G 25.1.2 A MSB is encouraged to open a designated account in the form of a trust account to further safeguard customer funds.

25.2 Use of Remittance System

S 25.2.1 A MSB which carries out remittance business shall ensure that its remittance system is robust with features that fulfils the requirements prescribed in the Remittance Regulations and has the ability to:

(a) capture end-to-end transaction information including the names of the recipient and sender, amount involved, date and time of transaction, status of transaction, location of both recipient and sender, and other necessary information;

(b) control access such that access is only granted relevant to its purposes, particularly for systems developed by a service provider;

(c) trigger any breaches of the transaction limit prescribed in the Remittance Regulations;

(d) detect duplicate registrations of customers and prompt alerts upon detection;

[14] In respect to funds allowed to be withdrawn from a MSB's designated account as per section 37(3)(c) of the Act, this shall include foreign exchange gains recognised upon settlement with the correspondent agent.

(e) detect any cancellations, refunds and amendments made to transactions; and

(f) properly segregate duties and functions through a checker/maker function. For example, tellers are assigned to perform transactions and supervisors are assigned to approve or verify the transactions.

S 25.2.2 In cases where more than one remittance system is used, regardless of whether the systems are own systems[15] or a remittance system offered by service provider, the MSB shall ensure that the systems used have the ability to aggregate all remittance transactions related to the same customer conducted across different systems and locations (i.e. head office, branches, agents and electronic terminals) to ensure compliance with the applicable transaction limits.

25.3 Engagement and Arrangement with Correspondent Agents

S 25.3.1 In appointing and engaging the services of a correspondent agent, a MSB which carries on remittance business shall:

(a) perform appropriate due diligence on prospective correspondent agents to ensure that the agents are authorised and recognised in the relevant jurisdictions to offer remittance services;

(b) clearly document in a written contract the responsibilities of the MSB and its correspondent agents which should include, among others, obligations to safeguard the confidentiality of customers' information;

(c) ensure the transmission of remittance instructions between the MSB and its correspondent agents is conducted through the remittance system. No remittance instructions shall be transmitted manually such as through email, telephone calls, messaging platforms including social media, or facsimile; and

(d) establish clearly defined mechanisms for handling any disputes on remittance services effected through such correspondent relationships. This shall include the responsibilities of each party.

[15] Own system is where the MSB has full control of and manages the administration of the remittance system and its database. In the case where the MSB utilises the service of a service provider, the responsibility of the service provider is limited to providing technical support for the maintenance of the system.

25.4 Settlement with Remittance System Service Providers and Correspondent Agents

S 25.4.1 A MSB shall ensure that settlement arrangements with its remittance system service providers and correspondent agents are properly documented and legally enforceable.

S 25.4.2 All settlements between a MSB and its local remittance system service providers shall be in Ringgit.

S 25.4.3 Settlements between a MSB and its foreign remittance system service providers or correspondent agents shall be in foreign currency if the settlement is made outside Malaysia or in Ringgit or foreign currency if the settlement is made in Malaysia through an account maintained with banking institutions.

S 25.4.4 A MSB shall perform reconciliation on the amount payable to its correspondence agents against its outstanding liabilities on a regular basis.

S 25.4.5 A MSB is allowed to execute netting arrangements with its remittance system service providers and correspondent agents to improve cost efficiency, subject to having a robust remittance system in place which can:

(a) reconcile all netting arrangement activities i.e. total outward, inward and net settlement amount; and

(b) detect any cancellations, refunds and amendments made to the transactions.

25.5 Intermediary Remittance Institutions (IRI)

S 25.5.1 A MSB licensed to conduct remittance business shall obtain the board's approval to carry on remittance business as an IRI. Upon such approval, a MSB shall notify the Bank at least twenty (20) business days prior to the provision of the IRI service.

S 25.5.2 In performing the function of IRI in addition to its primary MSB business, a MSB shall:

(a) segregate customer funds arising from its remittance business from those of the IRI business in separate accounts;

(b) ensure systems are able to segregate the activities of its primary MSB business and the IRI business including for recording, reconciliation and reporting purposes;

(c) undertake appropriate due diligence in appointing and engaging the services of its correspondent agents for the IRI business based on well-established procedures, as outlined in paragraph 25.3;

(d) establish policies and procedures to perform ongoing assessment to identify, measure, and mitigate risks associated with the operation of the IRI business; and

(e) ensure the relationship between parties involved in the provision of IRI is governed by a contractual agreement that outlines the obligations of the respective parties.

26. Specific Requirements to Conduct Money-Changing Business

26.1 Conduct of Exchange Transactions

S 26.1.1 A MSB that carries on money-changing business shall ensure that the originator and ultimate recipient of an exchange transaction is the same person.

G 26.1.2 Notwithstanding paragraph 26.1.1, a MSB may deal with a representative authorised by the customer for an exchange transaction.

S 26.1.3 Where the customer authorises a third party/representative to act on behalf of the customer, a MSB shall conduct enhanced due diligence (EDD) on the customer for non face-to-face arrangement in line with the AML/CFT/CPF and TFS for FIs policy document.

S 26.1.4 Where an exchange transaction is performed through a bank account[16] belonging either to the MSB or the customer (e.g. a customer deposits funds for exchange into the MSB bank account), a MSB shall only:

[16] Bank account maintained with any banking institutions.

(a) conduct the transaction with the customer of whom the business relationship has been established, and only upon the MSB having access to the records or information of the customer;

(b) receive funds for an exchange transaction from the customer's bank account and shall not accept deposit of such funds from third party accounts; and

(c) deposit funds arising from an exchange transaction into the customer's bank account and shall not accept instructions to deposit such funds into third party accounts.

S 26.1.5 Consistent with paragraph 14.3.1, all exchange transactions shall be performed at the prevailing market rate of exchange, including for advance orders where the settlement period for funds to be exchanged shall not exceed two (2) business days.

26.2 Sourcing and Clearing of Currencies

S 26.2.1 A MSB shall source and clear[17] its currency notes and coins only from licensed currency wholesalers, licensed money changers, and banking institutions, unless with written approval from the Bank.

S 26.2.2 A MSB shall have appropriate alternative arrangements in place for currency sourcing to mitigate risks arising from any disruptions to the supply of major currencies transacted.

27. Specific Requirements to Conduct Wholesale Currency Business

27.1 Import and export of currencies

S 27.1.1 Any import and export of Ringgit notes and coins by MSB requires prior approval from the Bank.

[17] For the purpose of the paragraph, 'source and clear' means 'buy and sell' of foreign currencies for the purpose of re-selling to clients.

S 27.1.2 A MSB which carries on wholesale currency business shall make or receive payment for all the settlement of its import and export of currency only via banking institutions, or licensed remittance service providers[18].

S 27.1.3 A MSB which carries on wholesale currency business shall have appropriate alternative arrangements in place for currency sourcing to mitigate risks arising from any disruption to the supply of major currencies transacted.

27.2 Import and export of currencies via cash couriers

S 27.2.1 In importing and exporting currency notes and coins via cash couriers, a MSB which carries on wholesale currency business, upon approval from the Bank where relevant, shall:

(a) maintain proper records/documents on import and export transactions conducted through cash couriers. Such records shall include (where applicable) but are not limited to the following:

(i) details of the cash courier, e.g. name, nationality, passport number and relevant document for verification (e.g. copy of passport);

(ii) authorisation document/letter from the principal (employer) of the cash courier;

(iii) copy of declaration form No. 22 (issued by the Royal Malaysian Customs Department); and

(iv) receipt of transaction (from counterparty).

(b) make available the records/documents to the Bank, upon request; and

(c) submit a monthly transaction report to the Bank on the import and export transactions through cash couriers[19].

[18] Licensed remittance service providers that provide business-to-business remittance services within the permissible limit.

[19] Information to be reported shall be on the appointed representative of an entity/counterparty that the MSB is conducting the transaction with.

PART D: RISK MANAGEMENT AND INTERNAL CONTROLS

28. Risk Management Framework

S 28.1 A MSB shall establish a risk management framework taking into account its size, scope and complexity of business to facilitate the identification, measurement, and continuous monitoring of all relevant and material risks.

(a) The framework shall be supported by a robust management information system that facilitates the timely and reliable reporting of risks.

(b) The officer that is responsible for risk management shall report to the board and senior management on a regular basis on the assessment of material risks affecting the MSB and ensure the material risks are monitored and effectively mitigated on an on-going basis.

(c) Risk reports shall be readily available to the internal audit function of the MSB, the Bank and other regulatory authorities upon request.

29. Internal Controls

29.1 Internal Policies and Procedures

S 29.1.1 A MSB shall establish written internal policies and procedures on the conduct of its activities, which at minimum shall include:

(a) standard operating procedures (SOP) for the MSB operations to ensure compliance by staff with internal policies and regulatory requirements as well as professional conduct in dealings with customers. The SOP shall also include control procedures and processes for detecting and escalating material operational lapses to management and the board.

(b) policies on branch oversight which include, but are not limited to the following:

(i) mechanisms for monitoring and reporting of the business performance and compliance levels at the branches to head office;

(ii) procedures to support reconciliation and consolidation of business transactions at the branches to ensure all business transactions undertaken by the MSB are properly captured; and

(iii) procedures to support the aggregation of business transactions by a customer at all business premises of the MSB to ensure among others compliance with AML/CFT/CPF requirements on customer due diligence and reporting of suspicious transactions, and compliance with the remittance transaction limits of a customer.

(c) Policies to ensure proper management of cash at all its business premises, including:

(i) setting of the holding limit of cash including foreign currencies, at its respective offices, taking into account the size, scope and risk profile of the business;

(ii) ensuring that only staff of the MSB are allowed to perform transactions and handle cash for the MSB; and

(iii) putting in place procedures to track and record currencies and movement of cash, where the records shall reflect the actual amount of physical currencies maintained at each office. In this respect, currencies retained at the MSB premises shall be for the purposes of MSB business only.

(d) Policies to ensure clear levels of authority are assigned to staff to conduct business transactions in accordance with the risk profile of the transactions. For example, higher level approval may be required for higher risk transactions which include but are not limited to the following:

(i) large transactions based on thresholds set by the MSB;

(ii) non-face-to-face transactions[20] conducted through bank accounts; or

(iii) instructions received over e-mail, fax, or telephone by existing customers.

(e) Policies on the introduction of new products and services. In this respect, a MSB is required to have proper procedures to conduct risk assessment on the offering of new products/services. The procedures shall at a minimum cover the following:

[20] For the avoidance of doubt, MSB shall adhere to relevant requirements on non-face-to-face transaction as specified under AML/CFT/CPF and TFS for FIs policy document for new customers that have not been on-boarded.

(i) compliance with legal and regulatory requirements; and

(ii) Impact on the MSB's overall risk profile including money laundering, terrorism financing and proliferation financing (ML/TF/PF) risk, business risk, conduct risk[21], technology, and cyber risks (where applicable).

29.2 Maintenance of Proper Accounting Practices

S 29.2.1 A MSB shall ensure that all business transactions (cash and non-cash) are properly recorded, and can be accounted for and reconciled with relevant source documents (e.g. receipts; invoices; purchase orders; bank and financial statements). In respect to this, a MSB shall:

(a) maintain and regularly update its financial accounts to ensure that it is accurate and reflects the latest financial position;

(b) ensure that the financial accounts are prepared in accordance with the Malaysian Financial Reporting Standards set by the Malaysian Accounting Standards Board;

(c) ensure that the external auditor appointed by the MSB fulfils the requirements as stipulated in the DL Regulations and notify the Bank on the appointment of its external auditor according to the format as attached in Appendix V; and

(d) where a MSB outsources its accounting function, the board and management remain responsible to ensure that the accounts properly reflect the financial position and performance of the MSB and are in compliance with the relevant regulatory requirements. In this regard, the board and management are expected to be able to explain material financial transactions, understand the basis on which the financial accounts have been prepared and ensure that source documents used to prepare the accounts are complete and accurate.

29.3 Maintenance of Records

S 29.3.1 Further to section 28 of the Act, a MSB shall also maintain all relevant business records to provide a comprehensive view of the company's

[21] This refers to risk arising from a MSB's business conduct and practices that could result in poor financial consumer outcomes and have a negative reputational and/or financial impact on the MSB.

operations and financial standing[22]. This requirement shall also apply to other business records, in cases where the MSB is allowed to undertake other non-MSB business.

G 29.3.2 A MSB may maintain the records in any of the following forms:

(a) in the form of original documents;

(b) duplicate copies of the original documents;

(c) in scanned form;

(d) in digital or electronic form; and

(e) maintained on microfiche.

S 29.3.3 A MSB shall put in place adequate controls to ensure key information and records are protected against access by unauthorised parties or unauthorised alterations of records.

29.4 Establishment of Complaints Handling Function

S 29.4.1 A MSB shall establish a complaint handling function proportionate to the nature, scale, and complexity of the MSB. This function shall have sufficient independence from the function involved in direct interaction with customers, such that it can effectively handle complaints raised by customers.

G 29.4.2 The function may be performed either by a designated staff or a designated unit.

S 29.4.3 A MSB shall formulate clear procedures to handle complaints, including escalation processes to the relevant level of authority depending on the severity of cases.

29.5 Proper Segregation of Duties and Functions to Ensure Checks and Balances

S 29.5.1 A MSB shall put in place proper segregation of duties and functions for critical operational functions to avoid mismanagement or fraud.

[22] This includes maintaining relevant financial information as stipulated under the Companies Act 2016.

S 29.5.2 In a situation where staff of a MSB is allowed to undertake several roles, the same person should not be placed in charge of roles[23] that could lead to potential conflicts of interest with dual controls also instituted where necessary.

29.6 Control Function

S 29.6.1 A MSB shall organise its control function in a manner that provides assurance that compliance and risk management are managed effectively, taking into account the size, nature of operations and complexity of the business.

S 29.6.2 The control function shall be independent of the business lines in order to carry out its role effectively. As such, a MSB shall ensure that the control function is not placed in a position where actual or potential conflicts may arise in respect of, amongst others, scope of responsibilities and reporting lines.

S 29.6.3 The control function shall be established in line with the following expectations:

(a) the board shall ensure that regular reviews are conducted by the control function to provide the board with an independent assessment on the following:

(i) compliance with the MSB's internal policies and applicable legal and regulatory requirements;

(ii) quality of controls including adequacy and effectiveness of risk management, internal controls and governance processes;

(iii) reliability, integrity and continuity of the management information system;

(iv) reliability including integrity, comprehensiveness and timeliness of the financial reports, management information and accounting records; and

[23] As an illustration, staff handling business transactions and record keeping for cash and currencies held for sale shall not oversee cash custody and currencies held for sale management.

(v) effectiveness of processes for the escalation of material breaches and gaps relating to the operations, controls and compliance of the MSB to the board in a timely manner.

(b) Structure of the MSB's control function shall commensurate with the type and size of the company, as follows:

Type of MSB	Expectations
• Large MSBs	Control function shall be performed by internal dedicated person/unit
• MSBs approved as a 'principal licensee' and/or carries out remittance as an intermediary remittance institution	
• Medium and small MSB[24]	Control function can either be performed by: (a) its non-executive director; (b) internal dedicated person/unit; or (c) a third-party service provider

29.7 Business Continuity Management

S 29.7.1 A MSB shall put in place a robust business continuity plan (BCP) that sets out the contingency arrangements to ensure the continuity of critical business functions[25] and safe keeping of important information relating to the business. This is to address risk of system disruptions and natural catastrophes resulting in operational failures, business disruptions and loss of key transaction records. The BCP shall include the following key features:

(a) procedures for the regular back up of customer information and business transaction data to ensure that information is not lost and can be retrieved in the event of a system failure or natural disaster;

(b) clear policies and procedures needed for staff to respond to system and operational failures in order to resume business operations in a

[24] In the case where a medium MSB or small MSB is also a principal licensee and/or carries out remittance as an intermediary remittance institution, the more stringent expectation shall apply.

[25] Including functions that are outsourced to service providers.

timely manner. For example, the BCP should outline procedures to be followed by the staff with respect to conducting and recording transactions in the event of a system breakdown, which may include rejecting transactions which are categorised as high risk by the MSB, based on the “red flags” established for the purpose of AML/CFT/CPF compliance;

(c) instructions to ensure all information of transactions taking place during the disruption period is properly recorded and promptly captured into systems once the systems have been restored to full functionality;

(d) for MSB that carries on remittance business using a system offered by a service provider or correspondent agents, the MSB shall conduct appropriate assessments to satisfy themselves that the system will be able to provide uninterrupted access to all remittance transactions performed for the MSB; and

(e) for MSB that offers its services via electronic terminals, the MSB shall institute appropriate measures to ensure minimal downtime to its electronic services.

29.8 Safety and Security Measures in Conducting Money Services Business Operations

S 29.8.1 A MSB shall install at all its offices where physical MSB transactions are carried out with customers:

(a) a counterfeit-detection machine to facilitate detection of counterfeit currencies from being used for exchange; and

(b) a CCTV system.

G 29.8.2 Notwithstanding paragraph 29.8.1, a MSB is encouraged to install a CCTV system in all its other offices for enhanced security.

S 29.8.3 A MSB shall institute proper processes and controls of the CCTV system, which shall at a minimum include the following:

(a) installation of the CCTV cameras at appropriate locations, in a manner that the camera is able to clearly capture, monitor and record the relevant areas where MSB activities take place. This shall include recording of the MSB customers, customer areas, safe/vault and other

cash handling areas as well as the entrance/exit of the business premises;

(b) ensure all images captured and recorded by the CCTV cameras are visible and clear;

(c) ensure the CCTV system at a minimum is equipped with the following functions to:

(i) view, replay and retrieve all information contained in the CCTV system;

(ii) enable information recorded in the CCTV system to be copied or exported to any common external data storage devices[26] or cloud storage, and played on common media players to allow viewing of the CCTV records; and

(iii) implement control measures to prevent the CCTV system from being manipulated or misused by any unauthorised parties.

(d) ensure the information captured in the CCTV system is maintained for a minimum period of sixty (60) days to enable an audit trail on the operations and conduct of money services business unless otherwise specified by the Bank;

(e) ensure the timing of the CCTV recording is properly set, synchronised and is consistent with the time and date of the MSB activities that take place at the business premises;

(f) ensure the CCTV system is properly maintained and operates under good working condition for effective surveillance and monitoring of MSB operations;

(g) institute adequate controls to prevent unauthorised alterations of records and access by unauthorised parties, by limiting system access only to relevant personnel to ensure proper accountability for the assigned functions;

(h) clearly record all activities relating to the maintenance and recalibration of the CCTV system (including system upgrading or reformatting) in the system's maintenance log. Any system recalibration shall be reported to the CEO; and

[26] This includes external hard drive, pen drive, digital video disc (DVD) and compact disc.

(i) ensure that all information in the CCTV system is available upon request by the Bank.

PART E: IT REQUIREMENTS

This part of the policy document is categorised into 2 sections, as follows:

(a) Section 1 (which covers paragraph 30) comprises of general IT requirements that apply to all MSBs.

(b) Section 2 (which covers paragraphs 31 to 34) comprises of additional IT requirements that apply only to MSBs that are classified as "Highly Complex". The additional requirements are divided under 4 sub-sections, namely Technology Risk Management, ration, Technology Audit, and Internal Awareness and Training.

SECTION 1

30. General IT Requirements

30.1 Technology risk management

S 30.1.1 A MSB shall establish a sound internal technology risk framework, IT policies and procedures including the governance arrangements and oversight on the IT system operations, business continuity management, and all relevant security controls that commensurate with its risk profile.

S 30.1.2 A MSB shall establish controls to mitigate technology risk to systems, online portals and/or mobile applications. At a minimum, a MSB's technological eco-system shall be equipped with the following controls to manage the risks from malware, phishing or data leakage:

(a) its internal network, if any, is protected by a firewall;

(b) all servers and workstations are installed with anti-virus with the latest virus signature update;

(c) the system uses the latest and most secure encryption communication channel;

(d) effective security patch management[27] to safeguard its system from intrusion and data loss, which includes regular updates of all types of IT inventories with the latest security patches;

(e) implement a sound user access management policy including that only

[27] A MSB shall consider leveraging on effective IT inventory management system to ensure it is able to record and monitor the security patch versions for all its IT peripherals.

authorized system administrators are provided access to its database for administrative duties, segregation of data access between user profiles and documented procedures for access control and authorization;

(f) ensure proper controls over the management of user IDs, whereby each user ID shall be unique and passwords shall not be shared among staff;

(g) implement appropriate physical access control to the MSB's IT equipment (eg. physical access controls to its servers, firewalls, routers and switches). The access control should include identification, authentication and authorization of the user (internal and external users[28]) accessing IT equipment;

(h) conduct continuous training and awareness programmes to promote cyber hygiene[29] and undestanding on cyber security risks[30];

(i) for the MSBs who subscribe to services offered by a third-party service provider, the following controls to safeguard themselves in the service level agreement (SLA) should be established:

(i) clearly defined roles and responsibilities between the MSB and the service provider;

(ii) arrangements for disaster recovery and backup capabilities, where applicable;

(iii) written undertaking by the service provider on compliance with secrecy provisions under relevant legislation. The SLA shall clearly provide that the service provider is bound by confidentiality provisions stipulated under the contract even after the engagement has ended;

(iv) clearly affirm the MSB's ownership of its data stored on the service provider's system; and

(v) arrangements to secure business continuity in the event of exit or termination of the service provider.

[28] External users include service providers, auditors, etc.

[29] Examples of good cyber hygiene includes usage of strong password, ensuring user's password are not written and posted on the workstations, sharing of IDs and passwords, etc.

[30] Examples of cyber security risk includes phishing attacks, malware attacks, social engineering, ransomware, trojan viruses, etc.

(j) for online portal and mobile platform, at a minimum, the following controls to safeguard the system and the customers shall be established:

(i) mechanism to authenticate system users based on the MSB's technology risk appetite (e.g. login authentication);

(ii) mechanism to notify customers (e.g. via SMS) of all online transactions performed and completed;

(iii) mechanism to clear the web-browser cache used by the user when logging out from the account of the MSB's website for online transactions;

(iv) ensure the MSB's core system(s), including the online portal, mobile application and network system are equipped with audit trail capabilities. This includes tracking the IP address source for data movement through the online portal as well as IP address and geo-location sources for data movement via a mobile device;

(v) mechanism to prevent sensitive information from being stored on the user's mobile device;

(vi) provide sufficient information to customers to create awareness on risks associated with online and mobile application transactions; and

(vii) multi-factor authentication for online transactions.

30.2 Maintenance of Robust and Reliable Management Information System

S 30.2.1 A MSB is required to establish a secure and robust management information system to support the MSB's business operation. The system shall have the capability to perform at minimum, the following functions:

(a) detect and capture any alterations made to the information maintained in the system;

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

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

S 30.2.2 Upon commencement of the operation, a MSB is required to ensure the system is continuously operating in a sound and robust manner with at a minimum the following controls:

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

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

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

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

SECTION 2

31. Technology Risk Management

S 31.1 A MSB shall establish the Technology Risk Management Framework (TRMF), which is a framework to safeguard the MSB's information infrastructure, systems and data, and to manage its cyber security risks as an integral part of the MSB's risk management framework.

S 31.2 The TRMF should include the following:

(a) clear definition of technology and cyber security risks;

(b) the development of an institutional understanding of the overall cyber risk context in relation to the MSB businesses and operations, its exposure to cyber risks and current cybersecurity posture;

(c) clear responsibilities assigned for the management of technology and cyber security risks at different levels and across functions, with appropriate governance and reporting arrangements;

(d) the identification of technology risks to which the MSB are exposed, including risks from the adoption of new or emerging technology;

(e) the identification of cybersecurity threats and countermeasures including measures to contain reputational damage that can undermine confidence in the MSB;

(f) risk classification of all information assets/systems based on their criticality;

(g) risk measurement and assessment approaches and methodologies;

(h) risk controls and mitigations[31];

(i) continuous monitoring to timely detect and address any material risks;

(j) policies and procedures for timely and secure information sharing and collaboration with other MSBs and the industry association to

[31] The risk controls and mitigation should include, among others, distributed denial of service (DDoS) Attacks, data loss prevention (DLP) and cyber response and recovery (CRR).

strengthen cyber resilience among the MSBs;

(k) control measures on cybersecurity as specified in Appendix VI in order to enhance its resilience to cyber-attacks;

(l) continuously and proactively monitor, detect and prevent any potential compromise of their security controls or weakening of their security posture;

(m) 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;

(n) a clear Data Loss Prevention (DLP) policy, strategy, and SOP in order to ensure that proprietary, customer and counterparty information is identified, classified, and secured. The policy should include the use of appropriate technology to enforce DLP policies and trigger any policy violations;

(o) periodic reviews of its cybersecurity posture and strategy; and

(p) establish a 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.

G 31.3 A MSB should establish an independent enterprise-wide technology risk management function which should be responsible for:

(a) implementing the TRMF;

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

(c) providing independent views to the board and senior management

on third-party assessment[32], where necessary.

G 31.4 A MSB should designate a Chief Information Security Officer (CISO), by whatever name called, to be responsible for the technology risk management function of the MSB. The MSB should ensure that the CISO has sufficient authority, independence, and resources[33]. The CISO should:

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

(b) keep apprised of current and emerging technology risks which could potentially affect the MSB's risk profile; and

(c) be appropriately certified.

G 31.5 The CISO should be responsible for ensuring the MSB's information assets and technologies are adequately protected, which include:

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

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

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

S 31.6 A MSB shall conduct penetration tests:

(a) on their internal and external network infrastructure as well as IT systems including web, mobile and all external-facing applications at least once every three years; or

(b) on related internal and external network infrastructure as well as related IT systems including web, mobile and all external-facing applications, on every occasion a new product or system is introduced into the MSB's IT eco-system.

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

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

(c) The penetration testing shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. A MSB shall engage suitably accredited penetration testers and service providers to perform this function.

S 31.7 A MSB 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. The final penetration test report consisting of the rectifications for all issues identified shall be presented to the board of directors for deliberation and endorsement.

S 31.8 A MSB shall ensure it has adequate capabilities for proactive monitoring of its technology security posture. This activity shall include the detection of 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 this monitoring activities shall be included in the MSB's reviews of its cybersecurity posture and strategy.

S 31.9 A MSB shall immediately notify the Bank of any cyber-incidents affecting the MSB. Upon completion of the investigation, the MSB is also required to submit a report on the incident to the Bank.

32. Technology Operations Management

32.1 Technology Project Management

S 32.1.1 A MSB shall establish appropriate governance requirements commensurate with the risk and complexity[34] 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.

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

G 32.1.2 The risk assessment should identify and address the key risks arising from the implementation of technology projects. These include the risks that could threaten successful project implementation and the risks that a project failure will lead to a broader impact on the MSB's operational capabilities. At a minimum, due regard should be given to the following areas:

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

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

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

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

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

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

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

G 32.1.3 The board and senior management should receive and review timely reports on the management of these risks on an ongoing basis throughout the implementation of significant projects.

32.2 System Development and Acquisition

G 32.2.1 A MSB should establish an Enterprise Architecture Framework (EAF) that provides a holistic view of technology throughout the MSB. The EAF is an overall technical design and high-level plan that describes the MSB'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 MSB plan and structure system development and acquisition strategies to meet business goals.

S 32.2.2 A MSB 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[35]. The policies and practices shall be reviewed at least once every three (3) years to ensure that they remain relevant to the MSB's environment.

G 32.2.3 A MSB is encouraged to deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to support more secure systems development.

G 32.2.4 A MSB should consider the need for diversity[36] in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

G 32.2.5 A MSB should establish a sound methodology for rigorous system testing prior to deployment. The testing shall ensure that the system meets user

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

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

requirements and performs robustly. Where sensitive test data is used, the MSB should ensure proper authorization procedures and adequate measures to prevent their unauthorized disclosure are in place.

G 32.2.6 The scope of system testing referred to in paragraph 32.2.5 should include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, and exception and negative testing, where applicable.

S 32.2.7 A MSB shall ensure any changes to the source code of IT systems are subject to adequate source code reviews to ensure the code is secure and was developed in line with recognized coding practices prior to introducing any system changes.

G 32.2.8 In relation to IT systems that are developed and maintained by service provider, a MSB should ensure the source code continues to be readily accessible and secured from unauthorized access.

S 32.2.9 A MSB shall physically segregate the production environment from the development and testing environment for critical systems. Where a MSB is relying on a cloud environment, it shall ensure that these environments are not running on the same virtual host.

S 32.2.10 A MSB shall establish appropriate procedures to independently review and approve system changes.

S 32.2.11 A MSB shall also establish and test contingency plans in the event of unsuccessful implementation of material changes to minimize any business disruption.

S 32.2.12 Where a MSB's IT systems are managed by service providers, the MSB shall ensure, including through contractual obligations, that the service providers provide sufficient notice to the MSB before any changes are undertaken that may impact the IT systems.

G 32.2.13 When decommissioning systems, a MSB should ensure minimal adverse impact on customers and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

32.3 Cryptography

G 32.3.1 A MSB should promote the adoption of strong cryptographic controls for protection of important data and information which include:

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

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

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

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

G 32.3.2 A MSB should conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect confidentiality, integrity, authentication, authorization, and non-repudiation of information. Where a MSB does not generate its own encryption keys, the MSB should undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments[37], the MSB should consider whether such reliance is consistent with the MSB's

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

risk appetite and tolerance. A MSB should also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.

G 32.3.3 A MSB should ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols should include secret and public cryptographic key protocols, both of which should reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols should be based on recognized international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation should be undertaken in a protected environment, supported by a hardware security module (HSM) or trusted execution environment (TEE).

G 32.3.4 A MSB should store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers should be issued by recognized certificate authorities. The MSB should ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates is legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates should be consistent with the industry's best practices and applicable legal/regulatory specifications.

32.4 Data Centre Infrastructure

S 32.4.1 A MSB which utilizes data centres to host its active critical production systems shall ensure proper management of data centres and specify the resilience and availability objectives[38] of its data centres which are aligned with its business needs.

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

G 32.4.2 The network infrastructure should be designed to be resilient, secure and scalable. Potential data centre failures or disruptions should not significantly degrade the delivery of its money services business services or impede its internal operations.

G 32.4.3 A MSB should ensure that the production data centre that is established includes redundant capacity components and distribution paths serving the computer equipment.

S 32.4.4 A MSB is required to have a strong recovery and resumption capability, such as maintaining a recovery data center to ensure business continuity.

G 32.4.5 A MSB should host its IT systems in a dedicated space intended for production data centre usage. The dedicated space should be physically secured from unauthorized access and is not located in a disaster-prone area. A MSB should also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure.

S 32.4.6 A MSB shall establish proportionate controls, ensure adequate maintenance, and holistic and continuous monitoring of the critical components of the production data centres aligned with the MSB's risk appetite.

G 32.4.7 A MSB is encouraged to appoint a technically competent external service provider to carry out a production data centre risk assessment and set proportionate controls aligned with the MSB's risk appetite. The assessment should consider all major risks associated with the production data centre and should be conducted periodically or whenever there is a material change in the data centre infrastructure. The assessment should, at a minimum, include a consideration of whether paragraphs 32.4.3 to 32.4.6 have been adhered to. For data centres managed by service providers, a MSB may rely on independent third-party assurance reports

provided such reliance is consistent with the MSB'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.

32.5 Data Centre Operations

S 32.5.1 A MSB shall ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory, and network bandwidth.

G 32.5.2 A MSB should involve both the technology stakeholders and the relevant business stakeholders within the MSB in its development and implementation of capacity management plans.

S 32.5.3 A MSB shall establish appropriate monitoring mechanisms to track capacity utilization and performance of key processes and services[39]. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.

S 32.5.4 A MSB shall segregate incompatible activities in the data centre operations environment to prevent any unauthorized activity[40]. In the case where vendors' or programmers' access to the production environment is necessary, these activities shall be properly authorized and monitored.

S 32.5.5 A MSB shall establish adequate control procedures for its data centre operations. These control procedures shall include procedures for batch processing management to ensure timely and accurate batch processes, implementing changes in the production system, error handling, as well as management of other exceptional conditions.

[39] For example, batch runs and backup processes for the MSB's application systems and infrastructure.
[40] For example, system development activities shall be segregated from data centre operations.

G 32.5.6 A MSB is encouraged to undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times.

S 32.5.7 A MSB shall maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes. Backup media shall be stored in an environmentally secure and access-controlled backup site.

G 32.5.8 In regard to paragraph 32.5.7, a MSB should also adopt the controls as specified in Appendix VII or their equivalent to secure the storage and transportation of sensitive data in removable media.

G 32.5.9 Where there is a reasonable expectation for immediate delivery of service, a MSB should ensure that the relevant systems are designed for high availability.

32.6 Network Resilience

G 32.6.1 A MSB should design a reliable, scalable, and secure enterprise network that is able to support its business activities, including future growth plans.

G 32.6.2 A MSB should ensure the network services for its critical systems are reliable and have no SPOF in order to protect its critical systems against potential network faults and cyber threats.

G 32.6.3 A MSB should 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.

S 32.6.4 A MSB shall ensure network services supporting its IT systems are designed and implemented to ensure the confidentiality, integrity and

availability of data.

G 32.6.5 A MSB should establish and maintain a network design blueprint identifying all of its internal and external network interfaces and connectivity. The blueprint should highlight both physical and logical connectivity between network components and network segmentations.

S 32.6.6 A MSB shall ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three (3) years.

S 32.6.7 A MSB 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 MSB from other entities within the group.

G 32.6.8 A MSB is encouraged to appoint a technically competent external service provider to carry out regular network risk assessment and set proportionate controls aligned with its risk appetite. The assessment should be conducted periodically or whenever there is a material change in the network design. The assessment should consider all major risks and determine the current level of resilience.

32.7 Service Provider Management

S 32.7.1 In addition to the requirements in paragraph 23 on outsourcing arrangements, MSBs shall also fulfil the requirements under paragraphs 32.7.2 to 32.8.1 specifically for IT related service providers.

S 32.7.2 The board and senior management of the MSB shall exercise effective oversight and address associated risks when engaging service providers for critical technology functions and systems. Engagement of service providers, including engagements for independent assessment, does not in any way reduce or eliminate the principal accountabilities and responsibilities of the MSB for the security and reliability of technology

functions and systems.

S 32.7.3 A MSB shall conduct proper due diligence on the service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made of the service provider's capabilities in managing the following specific risks:

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

S 32.7.4 A MSB shall ensure its ability to regularly review the service level agreements with its service providers to take into account the latest security and technological developments in relation to the services provided.

S 32.7.5 A MSB shall ensure data residing in service providers are recoverable in a timely manner. The MSB shall ensure clearly defined arrangements with the service provider are in place to facilitate the MSB's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.

S 32.7.6 A MSB shall ensure the storage of its data is at least logically segregated from the other clients of the service provider. There shall be proper controls over and periodic review of the access provided to authorized users.

S 32.7.7 A MSB shall ensure its IT system hosted by 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 service provider.

32.8 Cloud Services

S 32.8.1 A MSB shall fully understand the inherent risk of adopting cloud services. In this regard, a MSB is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment shall specifically address risks associated with the following:

(a) sophistication of the deployment model;
(b) migration of existing systems to cloud infrastructure;
(c) location of cloud infrastructure;
(d) multi-tenancy or data co-mingling;
(e) vendor lock-in and application portability or interoperability;
(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;
(g) exposure to cyber-attacks via cloud service providers;
(h) termination of a cloud service provider including the ability to secure the MSB's data following the termination;
(i) demarcation of responsibilities, limitations, and liability of the cloud service provider; and
(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

S 32.8.2 The risk assessment as outlined in paragraph 32.8.1 shall be documented and made available for the Bank's review as and when requested by the Bank.

S 32.8.3 A MSB shall demonstrate that specific risks associated with the use of cloud services for IT systems have been adequately considered and

addressed. The risk assessment shall address the risks outlined in paragraph 32.8.1, as well as the following areas:

(a) the adequacy of the overarching cloud adoption strategy of the MSB including:
  (i) board oversight over cloud strategy and cloud operational management;
  (ii) senior management roles and responsibilities on cloud management;
  (iii) conduct of day-to-day operational management functions;
  (iv) management and oversight by the MSB of cloud service providers;
  (v) quality of risk management and internal control functions; and
  (vi) strength of in-house competency and experience;

(b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas:
  (i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and
  (ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit;

(c) the degree to which the selected cloud configuration adequately addresses the following attributes:
  (i) geographical redundancy;
  (ii) high availability;
  (iii) scalability;
  (iv) portability;
  (v) interoperability; and
  (vi) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.

G 32.8.4 A MSB should consider the need for a third-party pre-implementation review on cloud implementation that also covers the areas set out in paragraph 32.8.3.

S 32.8.5 A MSB shall implement appropriate safeguards on customer 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 and counterparty information, proprietary data and services hosted on the cloud, if applicable, including the relevant cryptographic keys management.

32.9 Access Control

S 32.9.1 A MSB shall implement an appropriate access control policy for the identification, authentication, and authorization of users (internal and external users such as service providers) to its technology systems. This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorized access.

G 32.9.2 In observing paragraph 32.9.1, a MSB should consider the following principles in its access control policy:

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

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

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

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

(i) system development and technology operations;

(ii) security administration and system administration; and

(iii) network operation and network security;

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

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

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

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

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

S 32.9.3 A MSB shall employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).

S 32.9.4 A MSB shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There shall be appropriate controls in place to check the strength of the passwords created.

G 32.9.5 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, a MSB is encouraged to properly design and implement (especially in high-risk or ‘single sign-on’ systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.

G 32.9.6 A MSB is encouraged to adopt dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system.

S 32.9.7 A MSB shall establish a user access matrix to outline access rights, user roles or profiles, and the authorizing and approving authorities. The access matrix shall be periodically reviewed and updated.

S 32.9.8 A MSB shall ensure:

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

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

32.10 Patch and End-of-Life System Management

S 32.10.1 A MSB shall ensure that IT systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a MSB shall clearly assign responsibilities to identified functions:

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

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

G 32.10.2 A MSB should establish a patch and EOL management framework which addresses among others the following requirements:

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

(b) conduct of compatibility testing for critical patches;

(c) specification of turnaround time for deploying patches according to the severity of the patches; and

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

32.11 Security of Digital Services

S 32.11.1 A MSB shall implement robust technology security controls in providing digital services which assure the following:

(a) confidentiality and integrity of customer and counterparty information and transactions;

(b) reliability of services delivered via channels and devices with minimum disruption to services;

(c) proper authentication of users or devices and authorisation of transactions;

(d) sufficient audit trail and monitoring of anomalous transactions;

(e) ability to identify and revert to the recovery point prior to incident or service disruption; and

(f) strong physical control and logical control measures.

G 32.11.2 A MSB should implement controls to authenticate and monitor all money services business transactions. These controls, at a minimum, should be effective in mitigating man-in-the-middle attacks, transaction fraud, phishing and compromise of application systems and information.

S 32.11.3 A MSB shall implement additional controls to authenticate devices and users, authorise transactions and support non-repudiation and accountability for high-risk transactions or transactions above RM10,000. These measures shall include, at a minimum, the following:

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

(b) both client and host application systems shall encrypt all confidential information prior to transmission over the network;

(c) adopt MFA for transactions;

(d) if OTP is used as a second factor, it shall be dynamic and time-bound;

(e) request users to verify details of the transaction prior to execution;

(f) ensure secure user and session handling management;

(g) be able to capture the location of origin and destination of each transaction;

(h) implement strong mutual authentication between the users' end-point devices and MSB's servers, such as the use of the latest version of Extended Validation SSL certificate (EV SSL); and

(i) provide timely notification to customers that is sufficiently descriptive of the nature of the transaction.

S 32.11.4 A MSB shall ensure the MFA solution used to authenticate transactions are adequately secure, which includes the following:

(a) binding of the MFA solution to the customer's account;

(b) activation of MFA shall be subject to verification by the MSB; and

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

G 32.11.5 A MSB should deploy MFA technology and channels that are more secured than unencrypted short messaging service (SMS).

S 32.11.6 A MSB shall deploy MFA solutions with stronger security controls for higher risk transactions.

S 32.11.7 Such stronger MFA solutions stipulated under paragraph 32.11.6 shall adhere to the following requirements:

(a) payer/sender shall be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction;

(b) authentication code shall be initiated and generated locally by the payer/sender using MFA;

(c) authentication code generated by payer/sender shall be specific to the confirmed identified beneficiary and amount;

(d) secure underlying technology shall be established to ensure the authentication code accepted by the MSB corresponds to the confirmed transaction details; and

(e) notification shall be provided to the payer/sender of the transaction.

S 32.11.8 Where a MSB deploys OTP as part of its stronger MFA solutions, the following features shall be implemented:

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

(b) generation of the OTP from the customer's device and not from the bank's server; and

(c) requiring the customer to physically enter the generated OTP into the application.

G 32.11.9 For money services business transactions below RM10,000, a MSB may decide on proportionate controls and authentication methods for transactions assessed by the MSB to be of low risk. In undertaking the assessment, the MSB should establish a set of criteria or factors that reflect the nature, size, and characteristics of a money services business transaction. Such criteria or factors should be consistent with the MSB's risk appetite and tolerance. The MSB should periodically review the risk assessment criteria to ensure its continued relevance, having regard to the latest developments in cybersecurity risks and authentication technologies as well as fraud trends and incidents.

S 32.11.10 A MSB shall ensure sufficient and relevant digital service logs are retained for investigations and forensic purposes for at least three years.

G 32.11.11 A MSB should ensure that the use of more advanced technology to authenticate and deliver digital services such as biometrics, tokenization, and contactless communication[41] comply with internationally recognized standards where available. The technology should be resilient against

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

cyber threats[42] including malware, phishing, or data leakage.

G 32.11.12 A MSB should undertake a comprehensive risk assessment of the advanced technologies, and the algorithms deployed in its digital services. Algorithms should be regularly reviewed and validated to ensure they remain appropriate and accurate. Where third-party software is used, a MSB may rely on relevant independent reports provided such reliance is consistent with the MSB's risk appetite and tolerance, and the nature of digital services provided by the MSB which leverage on the technologies and algorithms.

G 32.11.13 A MSB should ensure authentication processes using biometric technology are secure, highly resistant to spoofing and have a minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions.

G 32.11.14 A MSB should perform continuous surveillance to assess the vulnerability of the operating system, and the relevant technology platform used for its digital delivery channels to security breaches and implement appropriate corresponding safeguards. At a minimum, a MSB should implement sufficient logical and physical safeguards for the following channels/ devices:

(a) internet application;

(b) mobile application and devices; and

(c) self-service terminal (SST).

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

G 32.11.15 A MSB should adopt the controls specified in the following Appendices for the respective digital delivery channel:

[42] For example, in respect of QR payments, MSBs 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.

(a) Appendix VIII: Control Measures on Internet Application;

(b) Appendix IX: Control Measures on Mobile Application and Devices; and

(c) Appendix X: Control Measures on Self-service Terminals (SST).

33. Technology Audit

S 33.1 A MSB shall ensure that the scope, frequency, and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.

S 33.2 The audit function shall be adequately resourced with relevant technology audit competencies and sound knowledge of the MSB's technology processes and operations.

G 33.3 A MSB should ensure its technology audit staff are adequately conversant with the developing sophistication of the MSB's technology systems and delivery channels.

S 33.4 A MSB shall establish a technology audit plan that provides appropriate coverage of critical technology services, service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post- implementation reviews of new or material enhancements of technology services.

G 33.5 The audit function (in the case of paragraph 33.2) 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.

34. Internal Awareness and Training

S 34.1 A MSB shall provide adequate and regular technology and cybersecurity awareness education for all staff in undertaking their respective roles and measure the effectiveness of its education and awareness programmes. This cybersecurity awareness education shall be conducted at least annually by the MSB and should reflect the current cyber threat landscape.

G 34.2 A MSB should provide adequate and continuous training for staff involved in technology operations, cybersecurity, and risk management in order to ensure that the staff are competent to effectively perform their roles and responsibilities.

G 34.3 A MSB should provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

PART F: OTHER REQUIREMENTS

35. Other Compliance Requirements

S 35.1 A MSB shall notify the Bank in writing, to the Director of the department in charge of oversight/supervision of MSB of any proposed changes to their business or operating model which are significant or changes the risk profile of their business, which includes but are not limited to provision of IRI as well as payment and settlement flow, by providing the details at least twenty (20) business days prior to the effective date of the proposed changes. The Bank reserves the right to impose additional conditions or restrict the proposed changes if the Bank is of the view that the risks of such changes are not adequately mitigated.

APPENDIX

Appendix I: Superseded Guidelines / Circulars / Notifications

No.	Details	Issuance Date
1.	Pematuhan Terhadap Peraturan-Peraturan Di Bawah Akta Perniagaan Perkhidmatan Wang 2011 (APPW)	11/07/2012
2.	Pengeluaran Resit Bagi Transaksi Perniagaan Perkhidmatan Wang	23/08/2012
3.	Guidelines on Governance and Operational Requirements on Conduct of Money Services Business	15/10/2012
4.	Guidelines on Risk Management and Internal Controls for Conduct of Money Services Business	6/12/2012
5.	Syarat-Syarat Lesen Di Bawah Seksyen 10(2) Akta Perniagaan Perkhidmatan Wang 2011	23/08/2013
6.	Pematuhan Terhadap Garis Panduan Yang Dikeluarkan Di Bawah Akta Perniagaan Perkhidmatan Wang 2011 (APPW) 1) Sistem Berasaskan Sesawang (Web-based System) 2) Pembaharuan Lesen	19/03/2014
7.	Additional Requirements for the Chief Executive Officer	29/09/2015
8.	Requirements for the Money Services Business Compliance Officer	4/03/2016
9.	Circular on Requirements for the Money Services Business Compliance Officers to Obtain Certification / Accreditation	11/9/2017
10.	Keperluan berkenaan Pengenalpastian Identiti Perniagaan Perkhidmatan Wang Berlesen	18/12/2017
11.	Additional Requirements for the Money Services Business Compliance Officers	22/05/2018
12.	Requirements for Directors and Chief Executive Officers to Attend the Money Services Business Directors Education Programme (MSB-DEP)	22/01/2019
13.	Requirements for Installation of Closed-Circuit Television (CCTV) System at Business Premises for the Conduct of Money Services Business (MSB)	27/05/2019
14.	Governance, Risk Management, and Operations for Money Services Business (MSB)	30/06/2022

Appendix II: Requirements for MSB Compliance Officer

1. The Compliance Officer shall have his principal or only place of residence within Malaysia unless the Bank approves otherwise in writing.

2. A MSB Compliance Officer shall possess sound knowledge on MSB and AML/CFT/CPF requirements. This includes:
   (a) Clear understanding on the Act and Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 and the corresponding policy documents;
   (b) Ability to apply the requirements and effectively implement the appropriate policies and procedures for the MSB operations, particularly with respect to customer due diligence measures, suspicious transaction reporting as well as risk-based assessment and managing ML/TF/PF risks; and
   (c) High awareness on the latest developments in ML/TF/PF techniques and typologies associated with the MSB industry as well as AML/CFT/CPF measures undertaken by the industry.

3. The Compliance Officer shall report to the senior management on a regular basis the findings and analyses of compliance risk.

4. In ensuring that the appointed Compliance Officer is able to effectively carry out his roles and responsibilities, a MSB is required to ensure that the Compliance Officer:
   (a) is registered with the MSB Group of Compliance Officer (GOCO) established by the industry association within a month from his/her appointment;
   (b) successfully completes the accredited AML/CFT/CPF training modules, including the post-training assessments, developed by the GOCO on areas relating to the AML/CFT/CPF framework, customer due diligence process, handling of suspicious transactions as well as risk-based ML/TF/PF risk management; and

(c) attend relevant AML/CFT/CPF training[43] every financial year to ensure continuous learning of the knowledge necessary for the effective execution of the AML/CFT/CPF compliance responsibilities within a MSB company.

5. For the purpose of meeting the requirement in 4(b) and (c) above, the Compliance Officer shall observe the following timelines:

Requirements	Timelines
Complete all mandatory AML/CFT/CPF training modules	Before appointment or within a period of one (1) year from the Compliance Officer's appointment
Attend relevant AML/CFT/CPF training	Minimum one (1) time for every financial year of the MSB

6. A MSB shall notify the Bank in writing within ten (10) working days of the new appointment of the Compliance Officer, including details of the name, contact information (office telephone number, email address), and relevant experience and/or qualifications of the Compliance Officer.

[43] Training can be conducted by MAMSB or other external training providers.

Appendix III: Timelines for CEOs and Directors to Enrol and Complete the MSB-DEP Programme

	Requirements	Timelines
For directors and CEOs appointed: a) Prior to January 2019	Enrol into the programme	By 31 March 2019
	Attend the programme	By 31 December 2022
b) After January 2019	Enrol into the programme	Within 2 months of his / her appointment
	Attend the programme	Within 12 months of the enrolment date

Appendix IV: Display of Information on Business

Display of information for money services business provided through electronic means/temporary premises

	General information	Specific information	Display channel	Means for customer verification
Electronic Means	• Licence number, name of MSB & nature of business • Contact details (principal office address and contact number)	• Information of the licence including business registration number of MSB, type of approved activity, and expiry date of licence • MSB industry association membership number	Electronic platform (e.g. website, mobile app)	Provide address of the Bank's website i.e. *www.bnm.gov.my* for customers to verify the authorisation by the Bank of the business offered
Temporary Premises		Not applicable	Bunting or banner etc.	Present a certified copy of the approval letter from the Bank upon request by customer for verification of the business offered.

Appendix V: Submission Format for Appointment of External Auditor

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Appointment of Auditor

Name of licensee :

Company's business registration no. :

Type of Money Services Business :

Name of auditor (company)	
Address	
Contact Name/ Partner-in-charge	
Telephone No. (Office)	
Telephone No. (Mobile)	
Fax No.	
E-mail Address	

Declaration by Director

I, _____ (name of director), of NRIC / Passport No. _____ as a Director declares that the above mentioned auditor has been appointed with the approval of the Board and the Board is satisfied that the requirements referred to in paragraph 9.2(h) under the Governance, Risk Management, and Operations for Money Services Business policy document have been met.

Signature :

Name :

Date :

Licensee's stamp :

Form should be submitted to the following address:
Pengarah
Jabatan Pemantauan Perkhidmatan Pembayaran
Bank Negara Malaysia

Appendix VI: Control Measures on Cybersecurity

A MSB shall ensure adequate controls and measures are implemented on cybersecurity, including:

1. Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings.
2. Update checklists on the latest security hardening of operating systems;
3. Update security standards and protocols for web services encryption regularly. Disable support of weak ciphers and protocol in web-facing applications;
4. Ensure technology networks including mobile and wireless networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including firewall and Intrusion Prevention System (IPS);
5. Ensure security controls for server-to-server external network connections include the following:
    (a) server-to-server authentication such as Public Key Infrastructure (PKI) certificate or user ID and password;
    (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and
    (c) deploying staging servers with adequate perimeter defence and protection such as firewall, IPS and antivirus;
6. Ensure security controls for remote access to server include the following:
    (a) restrict access to only hardened and locked down end-point devices;
    (b) use secure tunnels such as TLS and VPN IPSec;
    (c) deploy “gateway” server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and
    (d) close all unused/unnecessary remote access ports;
7. Ensure overall network security controls are implemented including the following:
    (a) dedicated firewalls at all segments. All external-facing firewalls shall be deployed on High Availability (HA) configuration and “fail-close” mode activated. Deploy different brand name/model for two firewalls located in sequence within the same network path;

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

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

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

(e) solution to mitigate advanced persistent threats including zero-day and signatureless malware;

(f) capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents; and

8. Synchronise and protect the Network Time Protocol (NTP) server against tampering.

Appendix VII: Storage and Transportation of Sensitive Data in Removable Media

A MSB should ensure adequate controls and measures are implemented for the storage and transportation of sensitive data in removable media, including:

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

Appendix VIII: Control Measures on Internet Applications

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

Appendix IX: Control Measures on Mobile Application and Devices

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

2. In addition to the guidance in paragraph 1, a MSB should also ensure the following measures are applied specifically for applications running on mobile devices used by the MSBs, appointed parties or intermediaries for the purpose of processing customer and counterparty information:
   (a) mobile device to be adequately hardened and secured;
   (b) ensure the capability to automatically wipe data stored in the mobile devices in the event the device is reported stolen or missing; and

(c) establish safeguards that ensure the security of customer and counterparty information (e.g. Primary Account Numbers (PAN), Card Verification Value Numbers (CVV), expiry dates and Personal Identification Numbers (PIN) of payment cards), including to mitigate risks of identity theft and fraud[44].

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

Appendix X: Control Measures on Self-service Terminals (SSTs)

Cash SST

Cash SSTs are computer terminals that may be provided by MSBs such as Cash Deposit Machine that provide cash deposit services to facilitate remittance transactions.

MSBs should ensure the adequacy of physical and logical security and controls implemented on the Cash SST, which includes:

1. Enforcing full hard disk encryption;
2. Retaining cards or block access to Cash SST service when the following are detected:
   (a) exceed maximum PIN tries;
   (b) invalid card authentication value;
   (c) cash SST card unable to eject;
   (d) “deactivated” card status;
   (e) inactive account status such as “Dormant” or “Deceased”; and
   (f) cards tagged as “Lost” or “Stolen”;
3. Ensuring Cash SST operating system is running on a secure version operating system with continued developer or vendor support for security patches to fix any operating system security and vulnerabilities;
4. Deploying Anti-virus (AV) solution for Cash SST and ensure timely update of signatures. Ensure virus scanning on all Cash SSTs is performed periodically;
5. Implementing a centralised management system to monitor and alert any unauthorised activities on Cash SST such as unauthorised shutting-down of OS or deactivation of the white-listing programme;
6. Ensuring effective control over the Cash SST lock and key by using a unique and non-duplicable key to open the Cash SST PC Core compartment as well as ensure proper safekeeping and custody of the key;
7. Installing alarm system with triggering mechanism connected to a centralised alert system to detect and alert bank’s staff of any unauthorised opening or tampering of the physical component of the Cash SST, particularly the access to the Cash SST PC Core;
8. Securing physically the Cash SST PC Core by enclosing the CPU in a locked case;
9. Enforcing firewall and Intrusion Prevention System (IPS) at the MSB’s network to

filter communication between the host server and the Cash SST;

10. Enforcing pairing authentication for key Cash SST components, particularly between cash dispenser and Cash SST controller;
11. Enforcing Basic Input Output System (BIOS) lock-down which includes:
    (a) enabling unique password protection for accessing BIOS. The password should be held by MSBs under strict control;
    (b) disabling external input device and port such as CD-ROM, floppy disk and USB port. The Cash SST operating system can only be booted from the internal hard disk; and
    (c) disabling automatic BIOS update;
12. Ensuring proper configuration and hardening of the OS and application system, which includes:
    (a) blocking any wireless network connection such as Bluetooth, Wi-Fi;
    (b) disabling Microsoft default program system (such as Notepad, Internet browser, Windows shortcut, file download, file sharing and command prompt);
    (c) disabling unnecessary services in the operating system such as the auto-play features;
    (d) concealing Start Bar or Tray Menu;
    (e) enabling cache auto-deletion; and
    (f) disabling key combinations and right-click mouse functions;
13. Enforcing secure system parameter setting, which includes:
    (a) changing defaults password and other system security parameters setting of the Cash SST;
    (b) using a unique system administrator password for all Cash SSTs; and
    (c) using lowest-level privileges for programmes and users system access;
14. Performing scanning and removing any known malware such as Backdoor.Padpin and Backdoor.Ploutus;
15. Enforcing and monitor Cash SST end-point protection such as installing white-listing programmes. The end-point protection programme, at a minimum, should ensure only authorised Cash SST system processes and libraries are installed and executed;
16. Enforcing strict control procedures over installation and maintenance of Cash SST OS and application systems, which includes:

(a) ensuring only authorised personnel have access to gold disk copy (master copy of Cash SST installation software);
(b) ensuring the gold disk copy is scanned for virus/malware prior to installation into Cash SST;
(c) enforcing dual control for installation and maintenance of Cash SST software; and

17. Installing closed-circuit cameras and transaction triggered cameras at strategic locations with adequate lighting in order to ensure high quality and clear closed-circuit television images of cardholder performing a transaction as well as any suspicious activities.

Non-Cash SST

Non-cash SSTs are computer terminals such as desktops, laptops, tablets, cheque deposit machines and automated kiosk that facilitates non-cash remittance transactions services.

A MSB should ensure the adequacy of physical and logical security and controls implemented on the self-service terminals, which includes:

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