BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Currency Processing Business

Applicable to:

Registered currency processors

Issued on: 26 June 2024

BNM/RH/PD 041-1

TABLE OF CONTENTS

PART A OVERVIEW

1. Introduction

1.1 Currency processing business is regulated under the Currency Act 2020 (CA), an Act which provides for the management of currency of Malaysia, regulation of currency processing business and currency processing activities, and for other related matters.

1.2 A registered currency processor (RCP) performs a major fraction of the operations within the currency ecosystem by carrying on currency processing business. Hence, an RCP assumes an important role in ensuring the quality and integrity of currency in circulation.

1.3 To promote RCPs' prudent practice, professionalism, integrity, accountability and transparency, this policy document sets out regulatory requirements which must be adhered to, as well as recommended best practices which should be followed, by an RCP.

1.4 The requirements and recommendations contained in this policy document, which include minimum standards to be observed by an RCP, involve the following areas–

(a) governance;

(b) operational requirements;

(c) risk management and internal control; and

(d) information technology (IT) requirements.

2. Applicability

2.1 This policy document is applicable to a registered currency processor as defined in paragraph 5.2 of this policy document.

3. Legal Provisions

3.1 The requirements in this policy document are specified pursuant to sections 33, 41, 61 and 63 of the CA.

3.2 The guidelines in this policy document are issued pursuant to section 62 of the CA.

4. Effective Date

4.1 This policy document comes into effect on 1 July 2024, except for Parts C and F which come into effect on 1 January 2025.

5. Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the CA unless otherwise defined in this policy document.

5.2 For the purpose of this policy document–

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

“G” denotes guidelines which may consist of statements or information intended to promote common understanding and advice or recommendation that are encouraged to be adopted;

“board” refers to the board of directors of an RCP including a committee of the board where responsibilities of the board as set out in this policy document have been delegated to such a committee;

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

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

“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 policies and operations, and its compliance with relevant laws. This includes the risk management function, the compliance function and the internal audit function or equivalent functions that perform similar roles of risk management, compliance and internal audit, by whatever name called;

“critical business functions” refer to business functions undertaken by RCPs the failure or discontinuance of which is likely to significantly –

(a) impair the RCP’s business operations, financial position, reputation, or compliance with applicable laws; or

(b) impair the RCP’s provision of RCP’s currency processing services to customers;

“**critical system**” refers to any application system that supports the provision of the RCP’s currency processing services, where failure of the system has the potential to significantly impair the RCP’s provision of services to customers, business operations, financial position, reputation, or compliance with relevant laws;

"**currency processing business**" means—

(a) the business of–

(i) collecting currency note or currency coin;

(ii) sorting currency note or currency coin by authenticity and quality; and

(iii) packing currency note or currency coin by quality, quantity and denomination;

by a person for or on behalf of another person; or

(b) any activity declared as currency processing business under section 23 of the CA;

"**customer**" refers to any person to whom an RCP renders the services of currency processing;

"**customer information**" refers to any information, in whatever form, relating to the affairs or the account of any customer of a RCP;

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

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

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

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

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

"outsourcing arrangement" refers to an arrangement whereby a service provider performs an activity on behalf of the RCP on a continuing basis, where the activity constitutes an essential element of currency processing business and would otherwise be undertaken by the RCP on its own;

“outsourced service provider” or “OSP” refers to a service provider appointed by an RCP to perform an activity on behalf of the RCP under an outsourcing arrangement;

“**person**” means any natural person, corporation, statutory body, local authority, society, trade union, co-operative society, partnership or any other body, organisation, association or group of persons, whether corporate or unincorporated and includes the Government and any State Government.

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

(a) the duration of time from the disruption to the activation of the BCP; and

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

“**registered currency processor**” or “**RCP**” refers to a person registered under section 26(1) of the CA to carry on currency processing business;

“**senior management**” refers to the Chief Executive Officer (CEO) and senior officers of an RCP; and

“senior officer” refers to a person, other than the CEO or a director, concerned with the operation or management of an RCP such as having the authority and responsibility for planning, directing or controlling the activities of an RCP, including the Chief Operating Officer, Chief Financial Officer, members of decision-making committees and persons performing key functions such as risk management, compliance and internal audit.

6. Related legal instruments and policy documents

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

(a) Currency (Registration Requirement) Order 2021 [P.U.(A) 127/2021] (CRR Order); and

(b) Policy Document on Quality and Integrity of Currency issued on 12 September 2023.

PART B REGISTRATION REQUIREMENTS

7. Currency (Registration Requirement)

S 7.1 When carrying on its currency processing business, an RCP shall at all times comply with the requirements under the CRR Order, as amended from time to time.

PART C GOVERNANCE

8. Governance arrangements

S 8.1 An RCP shall establish appropriate governance arrangements, including the following, which are effective and transparent to ensure continued integrity of its business:

(a) a board and senior management consisting of people with calibre, credibility and integrity;

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

(c) segregation of duties and control function to reduce the potential for mismanagement and fraud to occur.

9. The Board

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.

S 9.2 The board shall bear the overall responsibility for promoting sustainable business growth and financial soundness of the RCP, and preventing mismanagement, fraud, and abuse of the RCP 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 RCP's risk profile;

(b) oversee the selection, appointment and performance of the senior management on an ongoing basis, in achieving the business objectives set by the board and in meeting the legal and fiduciary duties of the RCP. For this purpose, the board shall–

(i) ensure adequate assessment[1] (including fulfilment of the requirement under paragraph 11.1 of this policy document) is conducted prior to the appointment of a senior management officer;

(ii) ensure the senior management appointed is competent and capable of effectively managing the business in compliance with relevant laws; and

(iii) appoint a head of control function who has adequate working knowledge and can effectively support the RCP's compliance;

(c) ensure that effective oversight and risk management mechanisms are put in place and are periodically reviewed for continued effectiveness. For this purpose, the board shall–

(i) ensure appropriate policies, processes (including standard operating procedures), systems and controls to manage risks in its business are put in place. The board shall establish a process for facilitating periodic review of the policies, processes, systems and controls to ensure they remain relevant and up-to-date;

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

(iii) ensure effectiveness of the audit function by reviewing and ensuring appropriate audit scope, procedures and frequency of audits;

(iv) ensure the senior management provides adequate reporting to the board on a timely basis on the RCP's compliance with relevant laws; and

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

(d) oversee the management of the RCP's control function by–

(i) ensuring an effective risk management framework that is appropriate to the nature, scale and complexity of the business is put in place by the RCP;

[1] The board may authorise the delegation of the assessment or decision-making to an accountable person deemed fit by the board. Nonetheless, the board shall remain accountable for such assessments and decisions.

(ii) ensuring that control functions are established within the RCP and sufficiently resourced with officers[2] who are accorded with the appropriate stature, authority and independence;

(iii) ensuring the appointment of officers who have adequate working knowledge and can effectively support the RCP's internal control framework; and

(iv) where the risk management officer and compliance officer are the same person or where such an officer performs the responsibilities of other control functions except for internal audit, being satisfied that a sound overall control environment will not be compromised by the multiple responsibilities performed by the same officer.

Board appointments

S 9.3 An RCP shall only appoint as its director, a person who has been assessed by the RCP to have complied with paragraph 11.1 of this policy document.

S 9.4 An RCP shall not have a director who is an active politician. For the purpose of this paragraph, "active politician" means an individual who-

(a) is a member of any national or state legislative body; or

(b) is an office bearer of, or holds any similar position in, a political party, including an individual who holds *de facto* power or control within the political party,

in or outside Malaysia.

Composition of the Board

S 9.5 The board and its committees (if any) must be of a size and composition that promote effective deliberation and encourage active participation of all directors.

S 9.6 The board shall be composed of suitable members with an appropriate mix of skills, experience and knowledge to effectively carry out their responsibilities.

G 9.7 The board may include non-executive directors, including independent directors.

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

Board meetings

S 9.8 An RCP shall ensure a person appointed as its director must be able to devote sufficient time to their roles and maintain a sound understanding of the business of the RCP as well as relevant market and regulatory developments.

S 9.9 The board must meet regularly, whereby the number and frequency of board meetings must be commensurate with the size and complexity of the RCP's operations, to review the performance of the RCP, including the status of its compliance with relevant laws, and to deal with any issues pertaining to the operations of the RCP.

S 9.10 The board must ensure that clear and accurate minutes of board meetings are maintained to record the decisions of the board, including key deliberations, rationale for each decision made, and any significant concerns or dissenting views.

10. Senior management

S 10.1 An RCP shall only appoint as its senior management, a person who has been assessed to have complied with the requirements specified in paragraph 11.1 of this policy document.

S 10.2 An RCP that is involved in a business or activity other than currency processing business shall appoint a dedicated senior officer with relevant expertise and experience to assume the role of the head of currency processing business.

S 10.3 The senior management primarily responsible for managing the day-to-day business operations of the RCP must ensure that the operation of the RCP is carried out ethically, professionally and with integrity. In this regard, the specific responsibilities of the senior management shall include the following:

(a) ensure effective policies and procedures are established and implemented for, among others, the following areas:

(i) risk management and appropriate controls to manage and monitor risks;

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

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

(b) oversee the formulation and effective implementation of any business or strategic plan, including strategic technology plans and associated technology policies and procedures;

(c) ensure a robust assessment is conducted on any deviationsfrom legal requirements as well as the RCP's internal policies and procedures. This includes addressing any supervisory concerns and the progress of remedial actions taken to address them, with material information to be reported to the board in a timely manner; and

(d) effectively manage the internal control framework of the RCP by–

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

(ii) establishing a control function in accordance with paragraph 15.4.2 of this policy document;

(iii) providing sufficient resources for the control function, including officers with the appropriate competencies and experience; and

(iv) ensuring that the person performing the control function is kept informed of any organisational developments to facilitate the timely identification of compliance risk.

S 10.4 The senior management shall consist of individuals with the appropriate skill set and experience to adequately support the RCP's business. This includes individuals from IT related functions to provide guidance on the technology plans and operation to ensure the RCP's compliance with the IT requirements under Part F.

S 10.5 The senior management shall ensure adequate allocation of resources as well as appropriately skilled and competent staff to support all critical functions.

11. Fit and proper

S 11.1 An RCP shall assess and ensure that its directors and senior management are persons that fulfil the criteria as stipulated in the CRR Order.

S 11.2 An RCP shall notify the Bank in writing together with the assessment made pursuant to paragraph 11.1 of this policy document on–

(a) new appointment of its directors or senior management within fourteen (14) days after the date of such appointment; or

(b) existing appointment of its directors and senior management within fourteen (14) days after the effective date of this policy document.

PART D OPERATIONAL REQUIREMENTS

12. Opening and closing of cash processing centre (CPC)

Opening of CPC

S 12.1 In relation to the opening of an RCP's CPC, the RCP shall –

(a) ensure the CPC premises comply with the requirement outlined in the CRR Order; and

(b) notify the Bank in writing on the opening of the CPC with the following information at least 30 calendar days before the date of opening of the CPC, together with attestation that the premises to be opened has complied with paragraph 12.1(a) of this policy document:

(i) address of the CPC;

(ii) target customer;

(iii) processing and storage capacity (volume in pieces);

(iv) head of CPC; and

(v) contact details.

Closing of CPC[3]

S 12.2 An RCP shall establish appropriate plans for the closing of its CPC and orderly exit, including its communication strategy with other relevant stakeholders[4] to mitigate any unintended consequences.

S 12.3 An RCP shall notify the Bank in writing and consult the Bank at least 30 calendar days before the closure of its CPC, together with information as set out in the Appendix.

13. Outsourcing arrangement

S 13.1 An RCP shall remain responsible and accountable for any services performed by an outsourced service provider (OSP).

S 13.2 For an outsourcing arrangement, an RCP shall ensure–

(a) the OSP that performs the collection of currency note or currency coin for or on behalf of the RCP has fulfilled the requirement stipulated in paragraph 2 of the Schedule of the CRR Order;

[3] Including relocation of CPC outside of the original CPC's state.
[4] For example, the RCP's customers and the local authorities.

(b) availability of sufficient expertise within the RCP to oversee and manage the outsourcing relationship; and

(c) the scope and nature of services and operations to be outsourced would not compromise the controls and risk management of the RCP. The RCP shall ensure the following:

(i) the outsourcing of such processes does not take away the critical decision-making function of the RCP;

(ii) the outsourcing of such processes does not threaten strategic arrangements, flexibility needed by the RCP on important areas and control of the RCP;

(iii) the outsourcing of such processes would not impair the reputation, integrity, and credibility of the RCP; and

(iv) processes are in place for the RCP to retain the ability to comply with relevant laws on the outsourced functions.

S 13.3 An RCP shall conduct appropriate due diligence on the OSP at the point of considering new outsourcing arrangements and when renewing or renegotiating existing outsourcing arrangements with the OSP.

S 13.4 An RCP shall identify and have an in-depth understanding of potential risks[5] arising from the outsourcing arrangements with the OSP. The scope and nature of services and operations to be performed by the OSP should not compromise the risk management and internal controls of the RCP.

S 13.5 In relation to the requirement specified in paragraph 13.4 of this policy document, an RCP shall ensure that the outsourcing arrangements with the OSP are established in a manner which do not affect–

(a) the RCP’s ability to effectively monitor the OSP and execute its BCP; and

(b) the RCP’s ability to promptly recover data in the event of the OSP’s failure that would critically impact or disrupt the RCP’s operations.

S 13.6 An RCP shall exercise effective oversight on the OSP.

G 13.7 For purposes of complying with paragraph 13.6 of this policy document, an RCP may consider the following:

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

[5] Including operational, financial and IT related risk

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

(c) ensure data residing in the OSP is recoverable in a timely manner;

(d) ensure any critical systems hosted by the OSP have strong recovery and resumption capabilities, and can facilitate an orderly exit in the event of failure or unsatisfactory performance by such OSP; and

(e) to have a contingency plan or arrangements to secure business continuity in the event the arrangement with the OSP is suddenly terminated or fails to provide necessary support[6]. The contingency plan shall be periodically reviewed to ensure that the plan is up-to-date and remains appropriate for timely implementation.

[6] Including insolvency or lack of resources issue.

PART E RISK MANAGEMENT AND INTERNAL CONTROL

14. Risk management framework

S 14.1 An RCP shall establish a risk management framework taking into account its size, scope and complexity of business to facilitate identification, measurement and continuous monitoring of all relevant and material risks.

S 14.2 In establishing the risk management framework, the RCP shall–

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

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

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

S 14.3 An RCP shall periodically review the framework for continued effectiveness and be supported by a robust management information system that facilitates the timely and reliable monitoring and reporting of risks.

S 14.4 An RCP shall establish risk monitoring and reporting requirements, which include periodic reporting to the board and senior management on the assessment of material risks affecting the RCP, to ensure risks are managed and mitigated in a timely manner. The reports must be readily available to the internal audit function of the RCP and the Bank.

S 14.5 An RCP is required to effectively manage and control all material risks associated with the conduct of currency processing business, taking into account the size, scope and complexity of its business activities.

S 14.6 An RCP shall establish appropriate processes, systems and controls that are approved by the board to manage risks in its business. These shall be properly documented and reviewed by the senior management and the board regularly to ensure its effectiveness.

S 14.7 The risk management measures that must be observed by the RCP to address specific risk associated with conduct of currency processing business include, but are not limited to the following –

(a) theft and robbery;

(b) accidents due to negligence of cash handlers or failure of equipment and machines;

(c) failure to comply with relevant laws; and

(d) mismanagement resulting losses of monies or key information held in trust for customers.

15. Internal control

15.1 Internal policies and procedure

S 15.1.1 An RCP is required to put in place appropriate processes, systems, and controls which shall include, at a minimum, the following:

(a) written internal policies and processes (including standard operating procedures), as well as systems and controls to manage risks on the conduct of currency processing business to –

(i) ensure compliance by staff with internal policies and relevant laws;

(ii) ensure professional conduct in dealings with customers; and

(iii) detect and escalate material operational lapses to senior management and the Board;

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

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

(ii) procedures to support reconciliation and consolidation of currency processing at the CPC to ensure all currency processing are properly captured; and

(iii) procedures to support record keeping of currency processing at all CPC to ensure compliance with standards issued by the Bank;

(c) policies to ensure proper management of cash at the CPC, which include, but are not limited to the following:

(i) setting of holding limit of cash at the RCP's respective CPC;

(ii) ensuring that only authorised personnel are allowed to process cash and handle machines; and

(iii) putting in place procedures to track and record the stock and movement of cash; and

(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 / value transactions.

15.2 Maintenance of Records

S 15.2.1 An RCP shall maintain all relevant records and documents relevant to currency processing business to provide a comprehensive view of the company's financial standing, governance and operations, for a minimum period of seven (7) years.

G 15.2.2 An RCP may maintain the records in any of the following forms:

(a) original documents;

(b) duplicate copies of the original documents;

(c) scanned form; and

(d) digital or electronic form.

S 15.2.3 An RCP shall establish a reliable management information system that is secure and robust to support its business operations and capable of performing functions which include, but are not limited to the following:

(a) the system must be able to record the processing activities and facilitate the aggregation of processing activities with customer across its branches for purposes of monitoring compliance with internal and regulatory limits;

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

(c) record details of transactions and generate reports on processing value and volumes for purposes of identifying, monitoring and reporting suspicious processing activities.

S 15.2.4 An RCP shall put in place adequate controls to protect key information and records maintained in the system to prevent access or alterations of records by unauthorised person.

15.3 Proper segregation of duties and functions to ensure check and balance

S 15.3.1 An RCP shall put in place proper segregation of duties and functions for critical operational functions, including cash processing, management and record keeping, to prevent the likelihood of mismanagement or fraud.

S 15.3.2 In a situation where the staff of a RCP is allowed to undertake several roles, dual controls[7] must be instituted and the same person shall not be placed in charge of roles[8] that could lead to potential conflicts of interest.

[7] Dual control is the practice of ensuring that no one person has complete control of an activity. For example, where a person is assigned to process currency and keep custody of the currency, following control should be considered–

(a) assign a checker to verify task perform under currency processing; or

(b) impose additional authentication tool i.e. password and thumbprint for the access to vault.

[8] For illustration, staff in charge of collection / distribution must not be the same person in responsible for cash custody / stock management.

15.4 Control function

G 15.4.1 The board and senior management are encouraged to create an environment, which–

(a) promotes the RCP and its officers to comply with relevant laws;

(b) adopts relevant risk management practices; and

(c) encourages ethical conduct that underlies the legal requirements.

S 15.4.2 An RCP shall establish control function in line with the following requirements–

(a) the RCP to provide the board with an independent assessment that the RCP is operating in compliance with its own internal policies (including the effectiveness of risk management and control systems) and with the relevant laws;

(b) the RCP shall organise its control function in a manner that provides assurance that compliance and risk are managed effectively, taking into account the size, nature of operations and complexity of its business;

(c) the control function must be independent of the business lines in order to carry out its role effectively. As such, RCP must ensure 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;

(d) the RCP must have adequate staff to perform an internal audit, compliance function, regular reviews on the premises and reporting directly to the board; and

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

15.5 Business continuity management (BCM)

S 15.5.1 The board and senior management are responsible for ensuring identification and implementation of an effective BCM framework within the RCP.

S 15.5.2 An RCP shall undertake a structured risk assessment process to–

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

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

G 15.5.3 For purposes of paragraph 15.5.2 of this policy document, the RCP is encouraged to carry out a business impact analysis (BIA) on an annual basis and whenever there are material changes to the RCP's business activity, as this forms the foundation of developing the BCP.

S 15.5.4 An RCP shall determine the MTD and RTO for each critical business function. The goal is to develop a BCP that details the procedures and the minimum level of resources required to recover the critical business functions within the recovery timeframe and maintain services at an acceptable level.

S 15.5.5 An RCP shall develop an effective BCP and disaster recovery plan (DRP) for at least all critical business functions.

S 15.5.6 To ensure the comprehensiveness of its BCM, the RCP shall ensure its OSP has an effective BCP and DRP and implements relevant safeguards to ensure continuity of the material[9] outsourcing arrangements, with the objective of minimising the business disruptions.

S 15.5.7 The BCP and DRP of the RCP and its OSP must be tested regularly to ensure the functionality and effectiveness of the recovery strategies and procedures, preparedness of staff and other recovery resources.

S 15.5.8 An RCP shall put in place a robust BCP that sets out contingency arrangements to ensure continuity of critical business functions[10] and safe keeping of important information relating to its 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 currency processing data to ensure 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 timely manner; and

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

[9] In assessing whether an outsourcing arrangement is material, an RCP may take into consideration the following factors:

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

b) aggregate exposure to a particular service provider in cases where the RCP outsources multiple activities to the same service provider; or

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

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

16. Fraud risk management

S 16.1 An RCP shall put in place an effective mechanism, processes and procedures for mitigating fraud risk and for facilitating fraud prevention, fraud detection and fraud monitoring which include, but are not limited to the following[11]:

(a) necessary processes and procedures to enable authentication by customers based on the risk profile of customers and transactions, to effectively mitigate and manage potential risk identified;

(b) the fraud risk management measures shall be reviewed periodically to ensure proactive actions are taken to address any inadequacies in such measures;

(c) fraud incidents and their assessment shall be reported to the board and senior management in a timely manner if the impact is significant; and

(d) reporting to the Bank shall be made in a timely manner if the impact is significant and in accordance with the fraud reporting requirement as issued by the Bank.

G 16.2 In relation to paragraph 16.1 of this policy document, an RCP may consider putting in place real time fraud detection and monitoring, effective early detection of unusual transactions and mechanism to halt or delay fraudulent or suspicious transactions.

[11] In assessing the significance of the impact an RCP may take into consideration the impact towards RCP's provision of services to customers, business operations, financial position, reputation, or compliance with relevant laws.

PART F Information Technology (IT) Requirements

17. Technology risk management

S 17.1 An RCP shall establish a Technology Risk Management Framework (TRMF), to safeguard the RCP's information infrastructure, systems and data, which shall be an integral part of the RCP's risk management framework in relation to currency processing business.

G 17.2 An RCP is encouraged to include the following in the TRMF:

(a) a clear definition of technology risk;

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

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

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

(e) risk measurement and assessment approaches and methodologies;

(f) risk controls and mitigations[12]; and

(g) continuous monitoring so as to detect and address any material risks in a timely manner.

G 17.3 An RCP is encouraged to 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 RCPs' 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[13], where necessary.

S 17.4 An RCP must deploy preventive and detective technology controls to mitigate technology risk to systems and must regularly monitor the effectiveness of

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

[13] 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.

these controls to ensure that they remain responsive to manage the risks from evolving cyberattack.

18. Technology operations management

Data Centre Infrastructure

S 18.1 An RCP shall ensure proper management of data centres and specify the resilience and availability objectives[14] of its data centres which are aligned with its business needs.

S 18.2 An RCP shall ensure its network infrastructure is designed to be resilient, secure and scalable in a way proportionate to the RCP's business risk and model. Potential data centre failures or disruptions shall not significantly degrade the delivery of its services or impede its internal operations.

Network Resilience

G 18.3 An RCP is encouraged to design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.

G 18.4 An RCP is encouraged to ensure the network services for its critical systems are reliable and have no single point of failure (SPOF) in order to protect the critical systems against potential network faults and cyber threats.

S 18.5 An RCP shall ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.

Access controls

S 18.6 An RCP must implement an appropriate access controls policy for identification, authentication and authorisation of users (internal and external users such as OSP).

G 18.7 In observing paragraph 18.6 of this policy document, an RCP is encouraged to adopt the following:

(a) implement principles of 'segregation of duties' and 'least privilege' when granting access to information assets;

(b) regularly review the access rights of staff and immediately revoke the access rights of a staff who has left the RCP or moved to a new role or position that does not allow access to customer information;

(c) only authorised system administrators are provided access to its database for administrative duties, segregation of data access between

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

user profiles and documented procedures for access control and authorization; and

(d) identify the location of customer information residing in different systems and establish adequate access controls at different levels (i.e. application level, database level, operating system level and network level) to prevent unauthorised access, modification or disclosure by whatever means of customer information to external parties.

S 18.8 An RCP shall establish a password policy to enforce strong password controls for the users' access to IT systems.

Physical security

S 18.9 An RCP shall implement appropriate physical access control to the RCP's IT equipment (e.g. 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[15]) accessing IT equipment.

G 18.10 An RCP is encouraged to conduct continuous training and awareness programmes to promote cyber hygiene[16] and understanding of cyber security risks[17].

Technology Service Provider Management

S 18.11 Where an RCP subscribes to services offered by an OSP, the RCP shall establish the following controls to safeguard themselves in the SLA:

(a) clearly define roles and responsibilities between the RCP and the OSP;

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

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

(d) clearly affirm the RCP's ownership of its data stored on the OSP's system; and

(e) arrangements to secure business continuity in the event of exit or termination of the OSP.

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

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

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

Patch and End-of-Life System Management

S 18.12 An RCP shall ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, the RCP must 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 18.13 An RCP is encouraged to 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.

PART G Other Requirements

19. Other Compliance Requirements

Changes to business model

S 19.1 An RCP shall notify the Bank in writing to the Director of the department in charge of oversight/supervision of RCPs at least 30 calendar days before implementing any proposed changes to their business or operating model which are significant or changes the risk profile of their business.

S 19.2 An RCP shall adopt risk mitigating measures before implementing any change to its business model if the Bank communicates in writing to the RCP that the proposed change to its business model has the risk of impairing the quality or integrity of currency.

Information and data submission[18]

S 19.3 An RCP shall submit the following to the Bank:

(a) its annual audited financial statements no later than three (3) months after its financial year end;

(b) statistical report on the operation of its business on a monthly basis; and

(c) any other information as required by the Bank.

[18] Submission via email at currency@bnm.gov.my unless otherwise stated in the Bank's request.

Appendix: List of information to be submitted to the Bank for notification for closure of currency processing centre (CPC)

1. Information on closure

   Name of registered currency processor:

   Reason for closure:

No.	Affected Customer	Processing volume
1.		
2.		

2. Exit plan as required in paragraph 12.2 of this policy document. At a minimum, the exit plan must include the following–

   a. plausible internal triggers for exiting the business, which demonstrate unsustainable business, inability to fulfil the value proposition for its business or materialisation of risks beyond own risk appetite;

   b. likely options and related measures to be taken for exit that minimises disruption to its customer and the currency ecosystem where it operates;

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

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

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