REGULATION ON OVERSIGHT
GUYANA

June,
2018

Contents

REGULATIONS ON OVERSIGHT

made under

THE NATIONAL PAYMENTS SYSTEM ACT

IN THE EXERCISE OF THE POWERS CONFERRED UPON THE BANK BY SECTIONS 3 AND 55 OF THE NATIONAL PAYMENT SYSTEM ACT, THE BANK HEREBY MAKES THE FOLLOWING REGULATIONS:

PART 1

GENERAL PROVISIONS

1. Definitions

In this Regulation:

"bank" shall means a company as defined in the Financial Institutions Act, 1995;

"Bank" means the Bank of Guyana established under the Bank of Guyana Act, 1998;

"Clearing" means the process of transmitting, reconciling and/or confirming funds or securities transfer instructions prior to Settlement and includes the Netting of instructions and the establishment of final positions for Settlement;

"Clearing System" means a set of procedures whereby Participants present and exchange information relating to the transfer of funds or securities

to other Participants through a centralized System or at a single location and includes mechanisms for the calculation of Participants' positions on a bilateral or multilateral basis with a view to facilitating the Settlement of their obligations;

"Direct Participant" means a Participant in a system who is responsible for the settlement of its own payments, those of its consumers and those of indirect Participants on whose behalf it is settling;

"Electronic money" means electronically, including magnetically (or in any other tangible or intangible device, such as a SIM card or a software) stored monetary value issued against receipt of funds for the purpose of making payment transactions and accepted as a means of payment by persons other than the electronic money issuer;

"Financial Institution" means a non-banking financial institution as defined in the Financial Institutions Act 1995;

"Indirect Participant" means a Participant in a System which is responsible only to its Direct Participant for settling the payment input to the System;

"National Payments System" means the whole of the services that are associated with the sending, receiving and processing of orders of payment or transfers of money in domestic or foreign currencies, issuance and management of Payment Instruments, Payment, Clearing and Settlement Systems, including those processing securities, arrangements and procedures associated to those Systems and Services, and Payment Service Providers, including Operators, Participants, and any third party acting on behalf of them, either as an agent or by way of outsourcing agreements, whether entirely or partially operating inside Guyana;

"Operator" means the Bank or any other entity licenced by the Bank to operate a System;

"Participant" means an entity which is recognized in the rules of a System as eligible to send and receive transfers, clear and settle through the System with other Participants either directly or indirectly;

"Payment Card" means a card or other device, including a code or any other means of access to an account, that may be used to obtain money or to make a payment, and includes a debit, credit, and stored-value card;

"Payment Instrument" means any instrument, whether tangible or intangible, that enables a person to obtain money, goods, or services or to otherwise make a payment or transfer money and includes, but is not limited to, cheques, funds transfers initiated by any paper or paperless device (such as automated teller machines, points of sale, internet, telephone, mobile), payment cards, including those involving storage of Electronic Money;

"Payment Service" means services enabling cash deposits and withdrawals, execution of payment transactions, issuing and/or acquisition of Payment Instruments, the provision of remittance services and any other services functional to the transfer of money. This shall also include the issuance of Electronic Money and Electronic Money instruments. The term does not include the provision of solely online or telecommunication services or network access;

"Payment Services Provider" means any entity that is licensed to provide Payment Services;

"Payments System" means any system that consists of a set of instruments, procedures, and rules for the transfer of funds between or among participants and it includes the participants and the entity operating the arrangement.

"Settlement" means the act of discharging obligations by transferring funds or securities between two or more parties;

"Settlement System" means a System established and operated by the Bank used to facilitate the settlement of transfers of funds or financial instruments between two or more parties or any other system which is approved by the Bank for this purpose.

2. Scope of the Regulation

This Regulation applies to the whole of Guyana, and to any payment service provider and payments system operator operating wholly or partially in Guyana.

PART 2

LICENSING TO PROVIDE PAYMENT SERVICES

3. Application for a licence

An applicant for a licence to provide payment services under section 9 of the Act shall submit to the Bank, an application in accordance with Form 1 as set out in the First Schedule which application shall be accompanied by the following documents and evidence:

(a) articles of incorporation and/or articles of association;
(b) evidence that it holds the prescribed level of initial capital required in accordance with regulation 4;
(c) programme of operations;
(d) a business plan for the first three years of provision of the payment service;
(e) a description of the measures which will be taken to safeguard funds of a consumer of the payment service;
(f) Organizational structure with well defined, transparent and consistent lines of responsibility.
(g) a description of the governance arrangements and internal control mechanisms including sound administrative and accounting procedures;

(h) a description of the internal control mechanisms the applicant has established in order to comply with AML/CTF obligations;
(i) procedure for monitoring, handling and following up on security incidents and related customer complaints;
(j) process for filing, monitoring, tracking and restricting access to sensitive payment data;
(k) business continuity plan;
(l) security policy document;
(m) any other information the Bank may require;
(n) Contact details and address of registered office;
(o) Personal Declaration Sheet containing details of each person who effectively directs the business of the applicant;
(p) Name and address of the applicant's external auditor's;
(q) Annual financial statements for the last three financial years where the applicant has been in operation approved by a statutory auditor or audit firm;
(r) A description of the group structure to which the applicant belongs if applicable.

4. Initial capital requirement

(1) The amount of initial capital required to be licensed as payment system provider and at all times shall be as set out in the Second Schedule.

(2) The Bank may amend the prescribed capital requirement as set out in the Second Schedule from time to time in consultation with the stakeholders.

5. Operational Plan)

The Operational Plan to be provided by the applicant shall include the following information:

(a) an identification and description of the type of payment service the applicant intends to provide;
(b) a description of the execution of the different payment services, detailing all parties involved, and including for each payment service provided:

i. a diagram of flow of funds;
ii. settlement arrangements;
iii. draft contracts between all the parties involved in the provision of payment services including those with payment card schemes, if applicable;
iv. processing times.

(c) a copy of the draft payment service contract, which governs the execution of payment transactions;
(d) the estimated number of different premises from which the applicant intends to provide the payment services;
(e) a description of any ancillary services to the payment services;
(f) a declaration of whether or not the applicant intends to grant credit and, if so, within which limits;
(g) a declaration of whether or not the applicant provides or intends to provide payment services in other countries;
(h) A description (including diagrams) of the IT infrastructure, capabilities and configuration of the operating system used by the applicant;
(i) Description of how data security and integrity will be maintained;
(j) Applicant's data protection policy.

Business plan

The business plan to be provided by the applicant shall contain:

(a) an executive Summary which briefly describes the applicant's organisation and the business concept;

(b) a marketing plan consisting of:
i. an analysis of the company's competitive position in the payment market segment concerned;
ii. a description of the payment service consumers, marketing materials and distribution channels;

(c) where available for existing companies, certified annual accounts for the previous three years, or a summary of the financial situation for those companies that have not yet produced annual accounts;
(d) a forecast budget calculation for the first three financial years that demonstrates that the applicant is able to employ appropriate and

proportionate systems, resources and procedures that allow the applicant to operate soundly;

(e) information on own funds, including the amount and detailed breakdown of the composition of initial capital.

6. Measures to safeguard the funds of payment service users

Where the applicant safeguards the payment service users' funds through depositing funds in a separate account in a bank or through an investment in secure, liquid, low-risk assets, the description of the safeguarding measures shall contain:

(a) a description of the investment policy to ensure the assets chosen are liquid, secure and low risk, if applicable;

(b) the number of persons that have access to the safeguarding account and their positions and functions;

(c) a description of the administration and reconciliation process to ensure that payment service users' funds are insulated in the interest of payment service users against the claims of other creditors of the payment service provider, in particular in the event of insolvency;

(d) a copy of the draft contract with the bank .

7. Organizational Structure

The applicant shall provide a description of its organisational structure including-

(a) a detailed organisational chart, showing each department, including the name of the person(s) responsible, in particular those in charge of internal control functions;

(b) descriptions of the functions and responsibilities of each department;

(c) an overall forecast of the staff numbers for the next three years;

(d) a description of relevant outsourcing arrangements consisting of:

i. the identity and geographical location of the outsourcing provider;

ii. the identity of the persons within the payment service provider that are responsible for each of the outsourced activities;

iii. a clear description of the outsourced activities and their main characteristics;

iv. a copy of draft outsourcing agreements;

(e) a description of the use of branches and agents, where applicable, including:
   i. a schedule of the off-site and on-site checks that the applicant intends to perform, at least annually, on branches and agents and their frequency;
   ii. the IT systems, the processes and the infrastructure that are used by the applicant's agents to perform activities on behalf of the applicant;
   iii. in the case of agents, the selection policy, monitoring procedures and agents' training and, where available, the draft agency contract;

(f) an indication of the payment system(s) that the applicant intends to access, if applicable.

8. Governance, Internal Controls and Risk Management

The applicant shall provide a description of the governance, internal controls and risk management procedures, which demonstrate that these procedures are appropriate, sound, and adequate, including:

(a) the identification of the types of risk and the measures in place to monitor, control or manage such risks
(b) description of internal organisation of work and the process of decision-making on payment system operation and risk management, and a description of reporting to the legal person's competent body on the provision of payment services, providing clear and direct lines of responsibility and accountability;
(c) the identity of the person(s) responsible for the internal control functions;
(d) the composition of the management body;
(e) a description of the way outsourced functions are monitored and controlled so as to avoid an impairment in the quality of the payment service provider's internal controls;
(f) a description of the way any agents and branches are monitored and controlled within the framework of the applicant's internal controls.

9. ***Compliance with Anti-Money Laundering/Countering Financing of Terrorism obligations***

The Applicant in order to comply with all Anti Money Laundering /Countering Financing of Terrorism obligations shall have a documented Anti-Money Laundering/Countering Financing of Terrorism Policy which will include the following information:

(a) the applicant's assessment of the money laundering and terrorist financing risks associated with its business, including the risks associated with the applicant's customer base, the products and services provided, the distribution channels used and the geographical areas of operation;
(b) the measures the applicant has or will put in place to mitigate the risks and comply with applicable AML/CFT obligations, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;
(c) the systems and controls the applicant has or will put in place to ensure that its branches and agents comply with applicable AML/CFT requirements;
(d) arrangements the applicant has or will put in place to ensure that staff and agents are appropriately trained in AML/CFT matters;
(e) the identity of the person in charge of ensuring the applicant's compliance with AML/CFT obligations, and evidence that their anti-money laundering and counter-terrorism expertise is sufficient to enable them to fulfil this role effectively;
(f) the systems and controls the applicant has or will put in place to ensure that its AML/CFT policies and procedures remain up to date, effective and relevant;
(g) the systems and controls the applicant has or will put in place to ensure that the agents do not expose the applicant to increased money laundering and terrorist financing risk;

10. Procedure for monitoring, handling, and following up on security incidents and security-related customer complaints

The applicant shall provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints to be provided by the applicant, which shall contain-

(a) organisational measures and tools for the prevention of fraud;
(b) details of the individual(s) and bodies responsible for assisting customers in cases of fraud, technical issues and/or claim management;
(c) reporting lines in cases of fraud;
(d) the contact point for customers, including a name and email address;
(e) the procedures for the reporting of incidents;
(f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

11. Process for filing, monitoring, tracking and restricting access to sensitive payment data

The applicant shall provide a description of the process in place to file, monitor, track and restrict access to sensitive payment data including-

(a) a description of the flows of data classified as sensitive payment data;
(b) the procedures in place to authorise access to sensitive payment data;
(c) a description of the monitoring tool;
(d) the access right policy;
(e) a description of how the collected data are filed;
(f) the IT system and technical security measures that have been implemented;
(g) identification of the individuals/bodies with access to the sensitive payment data;
(h) an explanation of how breaches will be detected and addressed;
(i) an annual internal control programme in relation to the safety of the IT systems.

12. Business continuity Plan

1) The applicant shall maintain at all times a plan of action establishing the procedures and systems necessary to restore safe and efficient operations of the payment system in the event of any disruption to the processes of the payment system.

2) The applicant shall provide a description of the business continuity arrangements, including-

(a) a business impact analysis, including the business processes and recovery objectives;
(b) the identification of the back-up site, access to IT infrastructure, and the key software and data to recover from a disaster or disruption;
(c) an explanation of how the applicant will deal with significant continuity events and disruptions;
(d) how to test the business continuity and disaster recovery plans;
(e) a description of the measures to be adopted by the applicant, in cases of the termination of its payment services.

13. Security policy document

The applicant shall have a customer security policy document that includes -

(a) a detailed risk assessment of the payment service(s) the applicant intends to provide, which shall include risks of fraud and the security control and mitigation measures taken to adequately protect payment service users against the risks identified;
(b) a description of the IT systems;
(c) the physical security measures and mechanisms of the premises and the data centre of the applicant;
(d) the customer authentication procedure;

(e) an explanation of how safe delivery to the legitimate payment service user and the integrity of authentication factors, such as hardware tokens and mobile applications, are ensured, at the time of both initial enrolment and renewal;

(f) a description of the systems and procedures that the applicant has in place for payment transactions and the identification of suspicious or unusual transactions.
(g) a description of the process in place to file, monitor, track and restrict access to sensitive payment data

14. Beneficial Ownership

1) A person who holds or will hold 5% or more of the shares of the applicant will be considered as a qualifying holder in the applicant's capital.

2) For the purposes of the identity and evidence of the suitability of all persons that have or will have qualifying holdings in the applicant's capital, the applicant shall submit the following information, where applicable:

   (a) personal details of each person;

   (b) certificate of incorporation or registration;

   (c) contact details, including the address of its registered office;

   (d) corporate documents;

   (e) a list containing details of each person who effectively directs the business of the legal person;

   (f) the shareholding structure;

   (g) audited financial statements for the last three financial years, where the legal person has been in operation for that period;

   (h) a description of the group to which the applicant belongs, if applicable;

   (i) a detailed curriculum vitae stating the education and training, previous professional experience and any professional activities or other functions currently performed;

   (j) a statement, accompanied by supporting documents, containing:

      i. any criminal conviction or proceedings;

      ii. any civil or administrative investigations, decisions, measures or sanctions against the person in matters of relevance to the assessment or licence;

      iii. any bankruptcy, insolvency or similar procedures;

      iv. any pending criminal investigations;

      v. any refusal, withdrawal, revocation or termination of registration, licence or licence to carry out trade, business or a profession;

(k) the current financial position of the person, including details concerning sources of revenues, assets and liabilities.

15. Identity and suitability assessment of directors and senior managers

For the purposes of the identity and suitability assessment of directors and senior managers of the payment service provider, the applicant shall provide the following information-

(a) personal details;
(b) details of the position for which the assessment is sought, including the letter of appointment, contract and a description of the individual's key duties and responsibilities;
(c) evidence of knowledge, skills, and experience, which shall include a curriculum vitae containing details of education and professional experience;
(d) evidence of reputation, honesty, and integrity, which shall include:
    i. criminal records and relevant information on criminal investigations and proceedings, relevant civil and administrative cases, and disciplinary actions;
    ii. a statement as to whether criminal proceedings are pending;
    iii. information concerning investigations, enforcement proceedings or sanctions by a supervisory authority that the individual has been directly or indirectly involved in.

16. Granting the licence

If the Bank determines that the applicant does not satisfy the requirements for licensing established in the National Payment System Act and in this Regulation, the Bank shall inform the applicant in writing of its refusal to grant a license no later than [3] months after receipt of the application, stating the reasons for the refusal.

Part 3

Consumer protection

17. Terms and conditions of Payment Services

(1) Each payment service provider shall have standard terms and conditions in relation to the carrying out of any payment service.

(2) Each payment service provider shall make available copies of the standard terms and conditions referred in paragraph (1) at its branches and agents that provide payment services.

(3) The terms and conditions referred in paragraph (1) shall be disclosed at the time the customer contracts for a payment service without charge and shall be in writing, in clear and concise language and shall include, to the extent applicable-

(a) the consumer's liability for unauthorized payment service and notice of the advisability of prompt reporting of any loss, theft, or unauthorized use of a card, access code or other means of access;

(b) the telephone number and address of the person or office to be notified in the event the customer believes that an unauthorized Payment Service has been or may be effected or in case of any loss or theft of a card, code or other means of access;

(c) the procedures to verify that the consumer had made the notification under paragraph (b) and when such notification was made;

(d) the maximum execution time for any kind of payment to be executed;

(e) the type and nature of the payment service which the consumer may initiate, including any limitations on the frequency or amount of such payment service;

(f) all applicable fees and charges for making a payment service transfer or for the right to make such payment service;

(g) the consumer's right to stop payment of a preauthorized payment service and the procedure to initiate such a stop;

(h) the consumer's right to receive information of a payment service;

(i) a summary of the error resolution procedures and the consumer's rights thereunder;

(j) the payment service provider's liability to the customer and refund policy;

(k) the circumstances under which the payment service provider will in the ordinary course of business disclose information concerning the consumer's account to third parties; and

(l) a notice to the consumer that a fee may be imposed if the consumer initiates a transfer from an automated teller machine or other electronic terminal that is not operated by the issuer of the card or other means of access.

(m) availability of Payment Service User statement

18. Notifications to customers of changes in the terms and conditions

(1) The payment service provider may vary or modify the terms and conditions of a payment service in relation to:

(a) imposing or increasing charges;

(b) increasing the customer's liability for losses;

(c) adjusting the transaction limits on the use of a payment instrument; or

(d) any other change that would result in greater cost or liability for the customer or decreased access to the customer's account

(2) The payment service provider shall notify the customer of any changes in the terms and conditions required to be disclosed under paragraph (1) through:

(a) notice in the periodic statement of account; and

(b) to one or more of the following channels-

i) notice at ATM, POS, SMS, email or other electronic terminals;

ii) notice on the website owned or controlled by the payment service provider, with respect to transactions conducted via the internet;

iii) voice communication, with respect to transactions conducted entirely by voice communications (including an automated voice response system by telephone);

iv) notice at its branches; or

v) any other mode it deems suitable.

(3) In accordance with section 30 (3) of the Act a consumer must be notified at least 21 days prior to the effective date of any change in any term or condition of the consumer's account.

(4) Notwithstanding paragraph (2), advance notice need not be given when changes are necessitated by an immediate need to restore or maintain the security of a payment service system or an individual account. The Bank shall require subsequent notification if such a change is made permanent.

19. Complaint procedure

(1) Any payment service provider shall establish appropriate procedures, to handle consumer complaints, including-

(a) the lodgment; and

(b) the investigation and resolution of any complaint made by a consumer on matters covered by this Regulation or other Regulations implementing the National Payments System Act.

(2) The complaint procedure shall contain information relating to the right of a consumer to refer the complaint to the Bank, or any other body authorized by the Bank, if he is not satisfied with the outcome of his complaint.

(3) The complaint procedure shall meet, at minimum, the following elements:

(a) ensuring the organization has appropriate capacity and deploys the resources necessary to respond to complaints;

(b) designating a senior management team within the organization that is responsible for complaint handling;

(c) providing clients with a free, easily-accessible, efficient, timely and impartial complaint handling process;

(d) reviewing and auditing the complaint-handling process with a view to make improvements if needed.

(4) Any Payment Service Provider shall keep a record of complaints and their resolutions, so that aggregate data on the type, frequency and resolution of such complaints can be made available to the Bank or any other body authorized by it as and when required.

Part 4

Risk management

20. Management of operational and security risks

(1) A payment service provider shall establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services it provides including the establishment and maintenance of effective incident management procedures, including for the detection and classification of major operational and security incidents.

(2) A payment service provider shall provide to the Bank an updated and comprehensive assessment of the operational and security risks relating to the payment services it provides and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

(3) The assessment in paragraph 2 shall be provided—

(a) on an annual basis, or at such shorter intervals as the Bank may direct; and

(b) in such form and manner, and contain such information, as the Bank may direct.

PART 5

LICENSING TO OPERATE PAYMENT SYSTEMS

21. Application for a licence

Any applicant for a licence to operate a payment system under section 9 of the Act shall submit to the Bank, an application in accordance with Form 2 as set out in the First Schedule which application shall be accompanied by the following documents and evidence:

(a) articles of incorporation and/or articles of association;

(b) evidence that it holds the prescribed level of initial capital;

(c) proposal of rules of the system;

(d) a programme of operations;

(e) a business plan for the first five years of operation of the payment system;

(f) a description of its structural organization;

(g) a description of governance arrangements and internal control mechanisms;

(h) process for filing, monitoring, tracking and restricting access to sensitive payment data;

(i) business continuity arrangements;

(j) a security policy document;

(k) identity and suitability of persons who have a direct or indirect interest or holding;

(l) identity and suitability of directors and senior managers; and

(m) any other information the Bank may require.

22. Capital Requirement

(1) The amount of initial capital required to be licensed as a payment system operator and at all times shall be as set out in the Second Schedule.

(2) The Bank may amend the prescribed capital requirement as set out in the Second Schedule from time to time in consultation with the stakeholders.

23. Programme of operations

The programme of operations to be provided by the applicant shall include the following information:

(a) an identification and description of the type of system the applicant intends to operate;
(b) the proposed rules and procedures of the system, which shall be clear and comprehensive;
(c) a declaration of whether or not the applicant operates or plans to operate the system in other countries.

24. Business plan

The business plan shall contain data referring to the planned activities of the applicant regarding the operation of system, in particular:

(a) a marketing plan consisting of:
    i. an analysis of the company's competitive position in the payment market segment concerned;
    ii. a description of the payment system participants, marketing materials and distribution channels;
(b) certified annual accounts for the previous five years, or a summary of the financial situation for those companies that have not yet produced annual accounts, where available;
(c) a forecast budget calculation for the first five financial years that demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures that allow the applicant to operate soundly;
(d) information on own funds, including the amount and detailed breakdown of the composition of initial capital.

25. Structural organisation

The applicant shall provide a description of its structural organization, including:

(a) a detailed organizational chart, showing each department, including the name of the person(s) responsible, in particular those in charge of internal control functions;
(b) descriptions of the functions and responsibilities of each department;
(c) an overall forecast of the staff numbers for the next three years;
(d) a description of relevant outsourcing arrangements consisting of:
    i. the identity and geographical location of the outsourcing provider;
    ii. the identity of the persons within the System Operator that are responsible for each of the outsourced activities;
    iii. a clear description of the outsourced activities and their main characteristics;
    iv. a copy of draft outsourcing agreements.

26. Governance arrangements and internal control mechanisms

The applicant shall provide a description of the governance arrangement and the internal control mechanisms, which demonstrate that these management arrangements and internal control mechanisms and procedures are appropriate, sound and adequate, including:

(a) a mapping of the risks identified by the applicant, including risks arising from illiquidity or insolvency of Participants;
(b) the procedures the applicant will put in place to assess and prevent the risks identified subparagraph (a);
(c) the different procedures to carry out periodical and permanent controls;
(d) the accounting procedures by which the applicant will record and report its financial information;
(e) description of internal organisation of work and the process of decision-making on payment system operation and risk management, and a description of reporting to the legal person's competent body on payment system operation, providing clear and direct lines of responsibility and accountability;
(f) the composition of the management body;

(g) description of the method of implementing control activities relating to payment system operation, including internal audits;
(h) the identity of the person(s) responsible for the internal control functions;
(i) a description of the way outsourced functions are monitored and controlled so as to avoid an impairment in the quality of the System Operator's internal controls.

27. Process for filing, monitoring, tracking and restricting access to sensitive payment data

The applicant shall provide a description of the process in place to file, monitor, track and restrict access to sensitive payment data including:

(a) a description of the flows of data classified as sensitive payment data;
(b) the procedures in place to authorise access to sensitive payment data;
(c) a description of the monitoring tool;
(d) the access right policy;
(e) a description of how the collected data are filed;
(f) the IT system and technical security measures that have been implemented;
(g) identification of the individuals/bodies with access to the sensitive payment data;
(h) an explanation of how breaches will be detected and addressed;
(i) an annual internal control programme in relation to the safety of the IT systems.

28. Business continuity arrangements

The applicant shall provide a description of the business continuity arrangements, including:

(a) business impact analysis, including the business processes and recovery objectives;
(b) disaster recovery and back-up arrangements, including the identification of the back-up site, access to IT infrastructure, and the key software and data to recover from a disaster or disruption;
(c) how to test the business continuity and disaster recovery plans;
(d) a description of the measures to be adopted by the applicant, in cases of the termination of its operation of the system.

29. Security policy document

(1) The applicant shall provide a security policy document including:

(a) a detailed risk assessment of the system the applicant intends to operate, which shall include the security control and mitigation measures taken to adequately protect participants against the risks identified;

(b) a description of the IT systems;

(c) the physical security measures and mechanisms of the premises and the data centre of the applicant, such as access controls and environmental security;

(d) the security of the payment processes; and
(e) a data security policy document.

30. Identity and suitability assessment of persons with qualifying holdings

For the purposes of the identity and evidence of the suitability of all persons that have or, in the case of licence, will have qualifying holdings in the applicant's capital, the applicant shall submit the following information, where applicable:

(a) name;

(b) registration certificate;

(c) contact details, including the address of its registered office;

(d) corporate documents;

(e) a list containing details of each person who effectively directs the business of the legal person;
(f) the shareholding structure;

(g) annual financial statements for the last three financial years, where the legal person has been in operation for that period, approved by a statutory auditor or audit firm).

(h) a description of the group to which the applicant belongs, if applicable;

(i) a detailed curriculum vitae stating the education and training, previous professional experience and any professional activities or other functions currently performed;

(j) a statement, accompanied by supporting documents, containing:

i. any criminal conviction or proceedings;

ii. any civil or administrative investigations, decisions, measures or sanctions against the person in matters of relevance to the assessment or licence;

iii. any bankruptcy, insolvency or similar procedures;

iv. any pending criminal investigations;

v. any refusal, withdrawal, revocation or termination of registration, licence or licence to carry out trade, business or a profession;

(k) the current financial position of the person, including details concerning sources of revenues, assets and liabilities.

31. Identity and suitability assessment of directors and senior managers

For the purposes of the identity and suitability assessment of directors and senior managers, the applicant shall provide the following information:

(a) personal details;
(b) details of the position for which the assessment is sought, including the letter of appointment, contract and a description of the individual's key duties and responsibilities;
(c) evidence of knowledge, skills and experience, which shall include a curriculum vitae containing details of education and professional experience;
(d) evidence of reputation, honesty and integrity, which shall include:
    i. criminal records and relevant information on criminal investigations and proceedings, relevant civil and administrative cases, and disciplinary actions;
    ii. a statement as to whether criminal proceedings are pending;

iii. information concerning investigations, enforcement proceedings or sanctions by a supervisory authority that the individual has been directly or indirectly involved in.

32. Granting the licence

If the Bank determines that the applicant does not satisfy the requirements for licensing established in the National Payment System Act and its implementing regulations, the Bank shall inform the applicant in writing of its refusal to grant a license no later than [3] months after receipt of the application, stating the reasons for the refusal.

Part 6

Rules of the system

33. Rules of the system

A system operator shall establish written rules for the governance and operation of the payment system which shall stipulate the following-

(a) the operator of the system;

(b) the settlement agent of the system and the method for ensuring the finality of payments;

(c) the participants in the system;

(d) the criteria for access and participation in the system and the conditions for exclusion from the system;

(e) the rights and obligations of the participants and the operator of the system;

(f) the method of transmission and delivery of payment instructions, their form and structure;

(g) the method of transmission and the form of payment instructions and settlement instructions;

(h) the method of securing data against misuse;

(i) the method of settlement of payment instructions submitted to the system;

(j) the principle of operation of the system;

(k) the moment of acceptance of an order by the system, the period during which the payment system will accept orders, and the time when payment instructions become irrevocable;

(l) the currency or currencies in which the system operates;

(m) the point of time when the settlement is considered final and irrevocable;

(n) arrangements to permit settlement to be made in the event of the failure of a participant.

34. Access and participation criteria

(1) A System Operator shall establish and publicly disclose non-discriminatory access and participation criteria to the System. It shall review the criteria at least annually.

(2) Participation in the payment system may be restricted only to the extent necessary to safeguard against financial, operational, business and other risks, and to preserve the safety and efficiency of the System.

(3) The rules of the system may not determine or lead to:

(a) restrictions regarding participation in other payment systems;

(b) a discriminatory position regarding rights and obligations related to participation in the payment system;

(c) restrictions based on the type of a payment service provider.

(4) If A System Operator denies access to an entity, it shall give reasons in writing for this, based on a comprehensive risk analysis.

(5) A System Operator shall monitor participants' compliance with the System's access and participation criteria on an ongoing basis.

(6) A System Operator shall establish and publicly disclose non-discriminatory procedures to facilitate the suspension and orderly termination of a participant's right of participation where the participant fails to comply with the access and participation criteria.

(7) A System Operator shall review:

(a) the criteria established in paragraph (1), and
(b) the procedures established in paragraph (6)

at least annually.

Part 7

Management of Risks

35. Legal soundness

A System Operator shall-

(a) establish system rules and procedures and enter into contracts, which are clear and consistent with the applicable law in Guyana;

(b) be able to specify the applicable law, rules, procedures and contracts for the operation of the system to the Bank, participants, and, where relevant, participants' customers, in a clear and understandable way.

36. Framework for the comprehensive management of risks

(1) A system operator shall establish and maintain a sound risk-management framework to comprehensively identify, measure, monitor and manage the legal risk, credit risk, liquidity or operational risk, and other risks.

(2) The risk-management framework shall:

(a) include the system operator's risk-tolerance policy and appropriate risk-management tools;

(b) assign responsibility and accountability for risk decisions;
(c) address decision-making in emergency situations relating to the System.

(3) A system operator shall develop risk-management tools that are robust and proportionate to the identified level of risk.

(4) A system operator shall define the System's critical operations and services, including identifying specific scenarios that may prevent it from being able to provide these critical operations and services as a going concern and assess the effectiveness of all options for recovery or an orderly wind-down.

(5) Based on the assessment established in paragraph 4, a system operator shall prepare a plan for the System' recovery or an orderly wind-down.

(6) A system operator shall review:

(a) the risk-management framework established in subsection 2,
(b) the System's critical operations and services established in paragraph 4; and

(c) the recovery and orderly wind-down plan established in paragraph 5 at least annually.

37. Credit risk

(1) An operator shall assess, monitor and effectively manage credit risk generated by participants and the operator itself in the process of payments, clearing and settlement process.

(2) The measurement and monitoring of credit exposures shall take place throughout the day, using timely information and appropriate risk-management tools.

38. General business risk

(1) A system operator shall establish robust management and control systems to identify, monitor, and manage general business risks.

(2) A system operator shall hold sufficient liquid net assets to:

(a) cover possible business' losses, thus guaranteeing the continuation of business and services even in cases these losses become materialised; and
(b) ensure a recovery or regular procedure to close the critical operations and services.

39. Operational risk

(1) A System Operator shall establish-

(a) a robust framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risk;
(b) service level and operational reliability objectives and policies designed to achieve those objectives;
(c) comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats;
(d) a business continuity plan that addresses events posing a significant risk of disrupting the System's operations.

(2) A System Operator shall review annually or with greater frequency as the circumstances may require -

(a) the objectives and policies established under paragraph 1(b); and
(b) the physical and information security policies established under paragraph 1(c).

(3) A System Operator shall identify critical participants based, in particular, on payment volumes and values and their potential impact on other participants and the System as a whole, in the event of a significant operational problem experienced by such participants.

(4) A System Operator shall identify, monitor, and manage the risks that critical participants might pose to the System's operations.

40. Communication procedures and standards

A system operator shall use or accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement and recording.

41. Disclosure of rules, key procedures, and market data

(1) A system operator shall adopt clear and comprehensive rules and procedures that are fully disclosed to participants. Relevant rules and key procedures shall also be publicly disclosed.

(2) A system operator shall disclose clear descriptions of the system's design and operations, as well as the System operator's and participants' rights and obligations, so that participants can assess the risks they would incur by participating in the system.

(3) A system operator shall provide all necessary and appropriate documentation and training to facilitate participants' understanding of the System' rules and procedures and the risks they face from participating in the System

(4) A system operator shall publicly disclose the System's fees at the level of individual services it offers. The system operator shall provide clear descriptions of priced services for comparability purposes.

(5) A system operator shall also, at a minimum, disclose basic data on transaction volumes and values.

42. Minimal requirements

The Bank provides for the establishment of minimal requirements for the operation of systems

Part 8

Settlement

43. Final settlement

A system operator shall guarantee the clear and safe final settlement, at least until the end of value date and, whenever needed or preferably, shall ensure the intraday settlement or at real time.

44. Participant-default rules and procedures

(1) A system operator shall establish a definition of participant default in the System rules and procedures, which shall include, at a minimum, a participant's failure to meet its financial obligations when they fall due, as a result, inter alia, of operational reasons, breach of agreement, or the commencement of insolvency proceedings against such participant.

(2) A system operator shall have default rules and procedures that enable it to continue to meet its obligations in the event of a participant default, which address the replenishment of resources following a default.

(3) A system operator shall be prepared to implement its default rules and procedures, including any appropriate discretionary procedures provided for in its rules.

(4) A system operator shall publicly disclose the key aspects of the rules and procedures outlined in paragraph 2.

(5) A system operator shall test and review the System rules and procedures outlined in paragraph 2 at least annually or after any material changes to the System affecting those rules and procedures.

45. Money settlement

(1) The operator shall ensure that final settlement takes place in the Bank's accounts, where practicable and available.

(2) If the settlement through the Bank's accounts is practically impossible, the operator shall minimise and strictly control the credit and liquidity risk, which arise from the use of commercial banks' accounts for settlement.

46. Payment versus payment

A System Operator that settles transactions which consists in the settlement of interrelated obligations (for example securities or foreign exchange transactions), shall eliminate principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation also occurs.

47. Renewal of licence

An application for renewal of licence as a payment service provider shall be made to the Bank at least two months prior to the expiry of licence and shall be:

i. in Form 3 as set out in the First Schedule;

ii. accompanied by any other information as the Bank may require;

iii. submitted with annual renewal fees as set out in the Schedule.

PART 9

ON-GOING OVERSIGHT

48. Cooperation with other authorities

Pursuant to section 5 of the National Payment System Act, the Bank shall cooperate with other public authorities engaged in the regulation and supervision of payment services providers and any other entity directly or indirectly involved in Payment Services and their operation in Guyana, as well as on the regulation, monitoring and supervision of capital markets in Guyana.

Title II

National Payments Council

49. Main Tasks of the Council

The Council main tasks are:

(a) to facilitate the necessary cooperation between all market participants and regulators in the payment area;

(b) to promote common initiatives towards the implementation of the payment system infrastructure;

(c) to play a key role in preparing strategic documents for the overall payment system architecture in Guyana;

(d) to monitor the implementation of payment systems reforms;

(e) to facilitate the sharing of information on economic and business requirements of all parties impacted by the payment system;

(f) to identify the impact of different options on participants business and daily operations and on end-user interests;

(g) to select the main principles and options for system designs;

(h) to endorse the priority and the schedule of individual projects to be launched, financed and implemented;

(i) to promote standardization of procedures and systems;

(j) to promote knowledge of payment system issues in Guyana. To this end, the Council uses any means it might find appropriate (workshops, seminars, website, newsletter, etc.);

(k) to promote cooperation among all institutions active in payment and securities systems within the region and at the international level.

(l) Act as an advisory body to the BoG in the exercise of its oversight function

50. Methodology

(1) The Council prepares ad hoc reports on payment system issues. The reports would not have prescriptive nature. However, they would serve as a reference for the ongoing payment system reforms in Guyana.
(2) The Council establishes ad hoc working groups on payment matters. Working groups may or may not be composed of the totality of the institutions represented in the Council.
(3) The Council reports on its activities to the Payment System Department at the Bank and the top management of the constituting institutions on an annual basis.

51. Structure and composition of the Council

(1) The Council gives representation to all the stakeholders of payment and securities clearance and settlement systems.
(2) The Bank serves as the chairperson and the secretariat of the National Payments Council.
(3) Appointed representatives of the stakeholders are senior managers with an involvement in payment matters. They report directly to the top management of their respective institutions.
(4) The Council has an internal governance structure with a chairperson and deputy(s), an executive body, formal rules to determine the terms and conditions for the appointment of the executive positions, and formal rules to govern the activity of the executive body.
(5) The Council may invite, if needed, other institutions and/or individual experts to participate in its meetings.

Title III

Collecting, processing and analysing data and other information, on-site inspection and reports

52. Collecting, processing and analysing data and other information

(1) ,

(1) A payment service provider or payment system operator shall, within ten days of the end of every calendar month, submit to the Bank in the form as set out in the X Schedule, information regarding (when applicable):

(a) the volumes, values and geographic distribution of each payment service provided by it or payment system operated;

(b) incidents of fraud, theft or robbery;

(c) material service interruptions and major security breaches;

(d) complaints reported, including remedial measures taken, those resolved and those outstanding.

(2) A payment service provider or payment system operator shall every year, within three months of the 31st December, submit to the Bank:

(a) audited financial statements covering their activities together with a copy of the auditor's report;

(b) separate audited financial statements for the payment service provider or system operator;

(c) a system security audit report on payment services or operation of the system; and

(d) any other information required by the Bank with respect to payment services or operation of the system.

53. On-site inspection

(2) On-site inspection shall be conducted by Bank's staff designated by the decision of the Bank's Governor or the person authorised by the Governor.

(3) The supervised entity and its members shall:

(a) enable Bank's staff to conduct inspection smoothly and shall cooperate with them;

(b) enable Bank's staff to inspect its business books, documentation and data required by such persons, in written and/or electronic form, and shall

provide them unimpeded and full access to equipment, databases and computer programs that it uses, and/or to all other information system resources;

(c) enable Bank's staff to conduct on-site inspection of its operations and/or specific activities at its head office, branches and other organisational units;

(d) have an obligation to provide written answers to questions made by the Bank's staff, upon their request, within the deadline laid down in such request, as well as to provide evidence substantiating such answers.

(4) The Bank may engage other persons to be present during on-site inspections in order to provide Bank's staff with appropriate expert support.

54. Report

(1) The Bank may make available to the public reports on relevant aspects of the National Payment System in an aggregate form on a regular basis.

(2) The Bank may provide confidential reports to the supervised entity from time to time and when necessary.

(3) If the report in subsection 2) is concerning the conducted off-site inspection and if, in the course of inspection, the Bank establishes any deficiencies or irregularities in the business operation of the supervised entity, the supervised entity may file its objections within 15 business days from the receipt of such report.