



CENTRAL BANK OF
TRINIDAD & TOBAGO

PAYMENT SYSTEM OPERATOR

APPLICATION FORM

-
- Interbank Payment System Operator (IPSO) Licence
 - Non-Interbank Payment System Operator (NIPSO) Registration

APPLICATION FORM: AUTHORISATION TO OPERATE A PAYMENT SYSTEM (INTERBANK PAYMENT SYSTEM OPERATOR LICENCE OR NON-INTERBANK PAYMENT SYSTEM OPERATOR REGISTRATION)

This Application Form is to be completed by any legal entity seeking authorisation from the Central Bank of Trinidad and Tobago (“Central Bank”) to establish and operate a payment system in Trinidad and Tobago.

Pursuant to Section 36(cc) of the Central Bank Act, Chap. 79:02 (“CBA”) and in accordance with the Sections 93(2) and 94(1) Financial Institutions Act, Chap. 79:09 (“FIA”), [Payments System Guideline No. 1 - Licensing and Operation of Interbank Payment Systems \(“Guideline No. 1”\)](#) and [Payments System Guideline No. 2 - Registration and Operation of Non-Interbank Payment Systems \(“Guideline No. 2”\)](#), applicants seeking authorisation as a Payment System Operator (“PSO”) are required to submit this Application Form and all supporting documentation to the Central Bank.

PART A: INSTRUCTIONS FOR COMPLETING THE APPLICATION FORM

1. It is important to read the applicable **legislation, policies, and guidelines** prior to completing this Application Form.
2. This Application Form must be completed in English, unless otherwise stated.
3. The applicant must provide all applicable supporting, as well as disclose any additional information that may be relevant. Please note that attachments should be provided in a searchable and comment-enabled format and must be provided in English.
4. All sections of this application form should be properly filled out. Please provide accurate, complete, and up-to-date information. Any incomplete information submitted will delay the Central Bank’s consideration of the application.
5. All documents/information (including policies and procedures) provided in support of the application should be tailored to your business model and not be generic templates.
6. Any questions that have a YES and NO box should be ticked or completed as appropriate. If a question is not relevant to your application, please state “not applicable”, and where possible, please explain. Failure to do so may result in an incomplete application.
7. If there are any subsequent changes in the information provided in the application after submission, the Central Bank should be notified immediately. Any relevant

APPLICATION

documentation must also be submitted at this time.

8. Applicants are advised that providing false or misleading information to the Central Bank, in connection with this application, may result in the refusal of the application or subsequent cancellation.
9. All Applicants granted a PSO licence will be required to operate in accordance with the information provided in their application, except where this information is altered with the approval of the Central Bank.
10. The completed **Application Form must be duly signed by a minimum of two (2) directors identifying their current designation within the business.**
11. Submissions of the requisite information and documentation, as detailed below, along with this Application Form, must be sent to PSregistration@central-bank.org.tt.

All information requested under this Application Form is required for the assessment of the Application and will be treated by the Central Bank in accordance with the secrecy and confidentiality obligations set out in Section 56 of the CBA and Section 8 of the FIA.

By signing below, you acknowledge that you have read and understood the information provided above:

PART B: APPLICANT DETAILS**1. APPLICATION CATEGORY***Please select the category of application being submitted.***TICK (☐) WHICH APPLIES**

1. Application for a Licence to Operate an Interbank Payment System (**IPSO**) ☐
2. Application for Registration of a Non-Interbank Payment System (**NIPSO**) ☐
3. Applicant requests the Central Bank to determine the appropriate classification ☐

2. CONTACT PERSON*Please provide details of the person designated by the Applicant whom the Central Bank may contact regarding this application.*

(a) Date of Submission (dd/mm/yyyy):

(b) Name of Contact Person:

(c) Position of Contact Person:

(d) Telephone Number:

(e) Email Address:

3. APPLICATION HISTORY WITH THE CENTRAL BANK

- (a) Has the Applicant ever applied for, or held an interest in, a business that has applied to the Central Bank for approval? **YES** ☐ **NO** ☐
- (b) If **YES**, provide information below, starting from the most recent record.

Date of Application	Type of Registration or Licence applied for	Status of Application (e.g. in progress, approved, withdrawn, rejected)

4. LEGAL AND CORPORATE GOVERNANCE ARRANGEMENTS

(a) Registered Company Name:

(b) Trade name (if different from above):

(c) Registered Business Address:

(d) Is the above registered business address the same as the address of the Company's permanent place of business or mailing address?

YES ☐ **NO** ☐

(e) If **NO**, please provide the Company's permanent place of business or mailing address:

(f) Telephone Number:

(g) Email Address:

(h) Institution Website Address:

(i) Business Operating Hours:

(j) List of significant shareholders and percentage ownership:

(k) Voting Rights:

(l) Any interim change to ownership and control planned during the application process or within five (5) years following commencement of operations:

YES ☐ **NO** ☐

(m) If **YES**, please provide further details:

4. LEGAL AND CORPORATE GOVERNANCE ARRANGEMENTS

(n) As per your Articles of Incorporation, what is the nature of the products and/or services you are registered to provide?

(o) Additional comments (if required):

(p) Is the Applicant a subsidiary of another company? **YES** ☐ **NO** ☐

(q) If **YES**, please state which company:

(r) Country of origin of ultimate parent company:

(s) Does the Applicant have ownership in other company(ies)? **YES** ☐ **NO** ☐

(t) If **YES**, please state the name and address of subsidiary companies/associated firms/other associated companies:

(u) Financial year end of the Applicant (dd/mm):

(v) Financial year end of the Applicant's parent company (dd/mm) (if applicable):

(w) Is the Applicant's parent company registered with another Regulatory Authority in a different jurisdiction? **YES** ☐ **NO** ☐

(x) If **YES**, please state the name and contact information of the Regulatory Authority:

5a. PAYMENT SYSTEM CLASSIFICATION

(i) Describe the Payment System type and delivery channel e.g. whether electronic fund transfer or payment card-based/internet-based/mobile phone-based or instant payment system.	
(ii) Describe whether the proposed payment system will cover domestic TTD transactions and/ or cross-border transactions.	
(iii) If cross-border transactions are processed, describe the currencies used.	
(iv) Provide details on the direct and indirect participants, as well as eligible participant types.	
(v) Describe the payer and payee relationships	
(vi) Describe whether the system switches, clears, nets, settles or routes transactions.	
(vii) Does the the applicant at any point hold or control participant or customer funds.	YES ☐ NO ☐
(viii) If Yes, please explain.	
(ix) Outline the system's expected operating hours .	
(x) Outline the system's: • maximum transaction value; and • expected annual and peak volumes and values.	
(xi) Describe the associated entities or third parties required to operate the Payment System and their role. For example: • links to other payment systems or FMIs; and • dependence on a commercial bank, central bank, card scheme, correspondent or foreign infrastructure.	

5a. PAYMENT SYSTEM CLASSIFICATION

(xii) Provide a detailed description of the payment system's design, architecture, process flows, and functionality, supported by relevant narratives, diagrams, and flowcharts, addressing each of the following:

- Legal, contractual, and governance relationships among the operator, participants, settlement institutions, service providers, and other relevant stakeholders;
- End-to-end transaction processing flows, including transaction initiation, routing, authorisation, processing, clearing, settlement, and confirmation;
- Clearing and settlement arrangements, including the timing and finality of settlement;
- Funds flows, identifying the movement of funds between parties throughout the transaction lifecycle; and
- Data and messaging flows, including the exchange, processing, storage, and transmission of payment-related information

Note: The Applicant's proposed classification is subject to review and confirmation by the Central Bank. The Central Bank reserves the right to classify the payment system as an IPSO, NIPSO, Systemically Important Payment System, and/or any other category it considers appropriate based on the nature, participants, activities, risks and systemic importance of the payment system.

5b. APPLICATION FEES (WHERE APPLICABLE)

Applicants are required to pay the application fee prescribed by the Central Bank at the time of submission of this application.

Tick (☒) if evidence is attached in submission

Confirm payment of the Application Fee

☐

Insert Payment Details:

- Date of Payment:
- Payment Reference Number:
- Method of Payment:
- Name of Financial Institution:
- Amount Paid: TT\$

Note, the application fee is charged to cover the cost of processing and assessing an application and is non-refundable.

PART C: BUSINESS PLAN

6. PROPOSED BUSINESS PLAN – to be attached with the application and should include the following:

Item	Attached	Document Name
Business overview, concept and proposed scope of activities;	☐	
Business strategy, market analysis, and business and operating model;	☐	
Products and services, including proposed fees and commissions;	☐	
Target users, participants and merchants (as applicable);	☐	
System operating model;	☐	
Staffing and key competencies;	☐	
Critical-service-provider failure provisions;	☐	
Profitability and break-even assumptions;	☐	
Scalability provisions;	☐	
Interoperability provisions;	☐	
Material dependencies (if any);	☐	
Sensitivity and stress scenarios examples and provisions for same (as applicable);	☐	
Recovery, exit and orderly-wind-down strategies/plans;	☐	
Activities performed in-house and activities outsourced;	☐	
A description of any other activities the applicant intends to conduct;	☐	
Implementation roadmap and key milestones;	☐	
Expected transaction volumes and values over a 5-year period;	☐	
Benefits to the financial system and country;	☐	
Other pertinent details;	☐	

PART D: CHECKLIST OF REQUIRED SUPPORTING DOCUMENTATION

Applicants are advised that all documents/information requested by the Central Bank must be submitted in support of their applications. Checklist as follows:

7. INCORPORATION/ COMPANY DOCUMENTS

A certified copy of the Company's documents as filed with the Registrar of Companies:	Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
(a) Certificate of Incorporation and/or Certificate of Continuance	☐	
(b) Articles of Incorporation	☐	
(c) By-laws	☐	
(d) Annual Return	☐	
(e) Notice of Directors /Notice of Change of Directors	☐	
(f) Notice of Secretary / Notice of Change of Secretary	☐	
(g) Notice of Address / Notice of Registered Office Address	☐	
(h) Return of Beneficial Interest in the Shares of a Company or any other constituent document, including any amendments.	☐	
(i) Operating Rules and Regulations	☐	
(j) Data Protection and User policies	☐	
(k) Provide a legal opinion on the following: - the legal basis for each material system activity; - the enforceability of the system's rules and contracts; - settlement finality and irrevocability; - enforceability of netting arrangements, where relevant; - insolvency treatment of unsettled and settled transactions; - enforceability of collateral, guarantees and loss-allocation arrangements; - conflict-of-laws analysis for cross-border systems (as applicable); - description of how changes in law will be monitored.	☐	

8. GOVERNANCE ARRANGEMENT/ GROUP AND ORGANISATIONAL STRUCTURE

		Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
8.1	In accordance with the Corporate Governance Guideline , a detailed Organisational Chart of the Applicant outlining and identifying: • Members of the Board of Directors • Senior Management • Staff	☐	
8.2	Completed Personal Questionnaire and Declaration (PQD) forms for Shareholders, Directors and each named Officer referenced on the Organisational Chart, accompanied by supporting documentation (in original or certified form), including the following in accordance with the Fit and Proper Guideline–October 2019 : • Certificate of Character from the Police Services of Trinidad and Tobago or Overseas Law Enforcement Clearance Report dated within six (6) months of this application; • Certified (or notarised, as applicable) coloured copy of a valid Photo Identification (National Identification card, Driver's Permit or Passport); and Up-to-date Curriculum Vitae or Resume for Directors/Officers (signed by the individual).	☐	
8.3	Corporate Controller's information on Acquirers, significant and controlling shareholders, directors and senior management of the Applicant, inclusive of a Group Chart showing all the Applicants in the Group that are either owned or controlled by the Applicant's Acquirer, controlling and significant shareholder, highlighting the percentage of ownership.	☐	
8.4	Completed Corporate Questionnaire and Declaration (CQD) form for the Applicant accompanied by supporting documentation (in original or certified form).	☐	

APPLICATION

8. GOVERNANCE ARRANGEMENT/ GROUP AND ORGANISATIONAL STRUCTURE

		Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
8.5	Policies and Procedures regarding: (a) Conflict-of-interest policies (b) Data Protection and user policies (c) Participant on-boarding and exit rules (d) Participant access criteria	☐	
8.6	In addition to the above an Applicant from an overseas jurisdiction seeking to establish a subsidiary in Trinidad and Tobago, should provide the following information: (a) Country of Incorporation (b) The Regulator in country of incorporation (if applicable) - i. Name ii. Address iii. Certified copy of license to operate iv. Letter of no objection from the Regulator List of all countries the Applicant operates from, including the details of respective Regulators.	☐	

APPLICATION

9. FINANCIAL OPERATIONS

		Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
9.1	Copies of Audited Financial Statements (Balance Sheet, Income Statement and Cash Flow Statement) - for the last three (3) years (where applicable);	☐	
9.2	Projected financial statements (Balance Sheet, Income and Cash Flow Statements) for the first three (3) years of operations; and	☐	
9.3	Management accounts for the operating period, no more than three (3) months prior to the submission of the Application.	☐	

10. CAPITAL AND RESERVES

(a) Issued share capital	TT\$
(b) Paid-up share capital	TT\$
(c) Capital reserves	TT\$
(d) Retained earnings	TT\$
(e) Other	TT\$

11. SOURCE OF FUNDS

Please provide information and documentary evidence. *Note, evidence should be reflected in a bank statement of a licensed financial institution or a deposit-taking institution under the FIA.*

Source of Funds*	Name of Institution/ Individual	Amount received (or to be received)
		TT\$
		TT\$
		TT\$
		TT\$

* Examples may include Applicant, Loan from financial institutions, Loan/Investment from family or friends, Angel Investor/Venture Capital, Crowdfunding, Initial Public Offering, Initial Coin Offering, Grant or government incentive, Others (Please specify).

12. RISK MANAGEMENT

Risk Management policies and/or frameworks (in accordance with the Central Bank's Guidelines) inclusive of:		Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
(a)	Enterprise Risk Management:	☐	
	i. Information and Communications Technology Risk Management	☐	
	ii. Business Continuity	☐	
	iii. Cyber Resilience (based on the Central Bank's Cybersecurity Best Practice Guideline)	☐	
	iv. Cyber Risk	☐	
	v. Operational Risk	☐	
	vi. Liquidity risk management	☐	
	vii. Credit risk management	☐	
	viii. Participant-default risk management;	☐	
	ix. Operational risk management;	☐	
	x. Fraud risk management;	☐	

APPLICATION

	xi. General Business risk management	☐	
(b)	Internal Controls	☐	
(c)	AML/CFT Framework	☐	
(d)	Third-Party Dependency Risk	☐	
(e)	Clearing and Settlement Risks	☐	

(f) Additional comment (if required):

13. INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

	Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
Information and Communications Technology. (Please see Appendix 3.)	☐	

APPLICATION

14. OUTSOURCING/ THIRD PARTY SERVICES ARRANGEMENTS

		Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
14.1	Board approved Outsourcing Policy and Procedures that guides the development and approval process for the outsourcing of material activities. The Outsourcing Policy must align with the principles set out in the Central Bank's Guideline for the Management of Outsourcing Risk .	☐	
14.2	Details of services outsourced to related companies within the Applicant's Group Structure, where applicable.	☐	
14.3	List of all its outsourcing contracts, which also identifies the material outsourced services.	☐	
14.4	Copies of Executed or Draft Agreements and Terms of Use for each outsourced activity/Applicant (partners, providers).	☐	

15. CLEARING AND SETTLEMENT ARRANGEMENTS

	Tick (☑) if attached in submission	Please indicate Document Name(s) and Page Number (s)
Describe the Clearing model. Include following details: - gross or net; - bilateral or multilateral; - batch or real-time; - calculation and cut-off times; - returns, rejects and exceptions; - reconciliation process.	☐	

15. CLEARING AND SETTLEMENT ARRANGEMENTS

Describe Settlement model. Include the following:		
• settlement agent; • settlement account structure; • settlement asset and currency; • frequency and timing; • value date; • finality point; • irrevocability point; • settlement confirmation; • failed-settlement handling; • end-of-day procedures.		
Provide details on risk controls (as applicable)		
• Prefunding • net debit caps; • collateral; • loss-sharing; • liquidity facilities; • concentration limits; • participant exposure monitoring; • settlement-agent exposure; • back-up settlement arrangements.		
Provide the following legal documentation:		
• settlement-agent agreement; • participant agreements; • scheme or operating rules; and • vendor agreements.		
Settlement procedures accompanied by:		
(a) details on the management of settlement risk;		
(b) a detailed diagram on the Applicant's settlement process, including all participants;		
(c) information on the Applicant's clearing and settlement times;		
(d) Description of services including acceptance, clearing, switching, routing, settlement agent, funding of settlement, notification of settlement by agent, notification of settlement to participant.		
(e) Description of the processing of returns:		
• Responsibility of the participant including submission timelines.		
• Responsibility of the operator.		
• Notification to beneficiary.		
(f) Management of clearing disputes and settlement disputes.		

APPLICATION

(g) The list of the system's	☐	
• Participants; and	☐	
• Users	☐	
(h) Rules on settlement finality and irrevocability;	☐	
(i) Any other related details on operating procedures; and	☐	

16. PARTICIPANT DISCLOSURE, ACCESS AND MARKET CONDUCT (WHERE APPLICABLE)

	Tick (☑) if attached in submission	Please indicate Document Name and Page Number (s)
<i>Participant Conduct</i>		
<i>Provide details on participant conduct and disclosure requirements including:</i>	☐	
i. participant disclosures regarding participant rights and obligations;	☐	
ii. fees and discounts;	☐	
iii. service levels;	☐	
iv. operating hours and cut-off times (settlement windows);	☐	
v. transaction limits;	☐	
vi. exception processing;	☐	
vii. participant complaints and dispute resolution;	☐	
viii. returns (including chargebacks and reversals), where relevant;	☐	
ix. user or customer recourse where the operator has a direct-facing role;	☐	
x. public disclosure of system rules and key procedures	☐	
<i>Provide details on participant access to the payments system:</i>	☐	
i. participant categories;	☐	
ii. eligibility criteria;	☐	
iii. financial, operational and technical entry standards;	☐	

iv. application and approval process; v. reasons for refusal; vi. onboarding testing and certification; vii. ongoing compliance monitoring; viii. participant limits; ix. suspension, restriction and exit; x. orderly migration of transactions and obligations; xi. appeal or review process; xii. direct and indirect participation; xiii. tiering and sponsorship arrangements; xiv. public disclosure of access criteria.	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
--	--	--

Consumer Protection and Disclosure Policy End-user/consumer protection, where the Payment System Operator has direct customer interaction or its rules establish customer-recourse arrangements (in accordance with the Central Bank's Market Conduct Guideline) addressing: (a) privacy Rules/Policy; (b) consumer charges and/or fees associated with the service; (c) information that will facilitate consumers' understanding of the system's rules and procedures; (d) the risks that consumers will face from their usage of	☐ ☐ ☐ ☐			
--	--	--	--	--



APPLICATION

each of the applicant's products and services; and				
(e) consumer complaints and dispute resolution.	☐			
(f) consumer recourse where the operator has a direct-facing role;	☐			

WHERE DOCUMENTS REQUIRED FOR SUBMISSION HAVE NOT BEEN PROVIDED BY THE APPLICANT, PLEASE PROVIDE A LIST AND REASONS FOR THE EXCLUSION.

PART E: DECLARATION

We, certify, on behalf of declare that:

(NAME OF APPLICANT IN BLOCK CAPITALS)

- (a) We are aware that the Central Bank may refuse the application for a Payment System Operator (“PSO”) if the Applicant fails to satisfy the Central Bank that the Applicant (including its officers, employees and controlling or significant shareholders) are fit and proper persons.
- (b) We have read and understood the Central Bank’s [Fit and Proper Guideline](#) (“F&P Guideline”) and in submitting this form, we are satisfied that the Applicant (including its officers, employees and controlling or significant shareholders) meets the fit and proper criteria stated in the F&P Guidelines.
- (c) We acknowledge that the Applicant is required to establish, maintain and implement appropriate policies and procedures in relation to its obligations as a registered or licensed PSO, and that such documentation shall be made available to the Central Bank upon request.
- (d) We undertake to notify the Central Bank, in writing, of any material changes to or affecting the completeness or accuracy of the information provided in this application and supporting documentation within thirty (30) days upon these changes taking place or coming to our attention.
- (e) That all information given in this application is complete and accurate to the best of our knowledge, information and belief and that there are no other facts relevant to this application of which the Central Bank should be made aware.
- (f) We acknowledge that knowingly or recklessly giving the Central Bank information which is false or misleading may be a criminal offence.

(This Declaration to be signed by two (2) Directors of the company)

Name	Designation	Signature	Date (dd/mm/yyyy)

PART F: APPENDIX**APPENDIX 1:****SAMPLE APPLICATION LETTER – INTERBANK PAYMENT SYSTEM**

From: (Applicant's Name and Registered Address)

To: Governor of the Central Bank
Central Bank of Trinidad and Tobago
Eric Williams Plaza, Independence Square,
PO Box 1250,
Port of Spain.

Dear Sir,

Application for Interbank Payment System Operator Licence

We hereby submit an application for a licence to operate an **Interbank Payment System** in accordance with the requirements of Section 93(2) and 94(1) of the Financial Institutions Act, 2008.

The required documentation and details of the payment of the application fee are enclosed.

We declare to the best of our knowledge that the information furnished is true, correct and complete.

Name:

Designation:

Company Seal:

Date:

Place:

APPENDIX 2:**SAMPLE APPLICATION LETTER - NON-INTERBANK PAYMENT SYSTEM OPERATOR**

From: (Applicant's Name and Registered Address)

To: Governor of the Central Bank
Central Bank of Trinidad and Tobago
Eric Williams Plaza, Independence Square,
PO Box 1250,
Port of Spain.

Dear Sir,

Application to Register as a Non-Interbank Payment System Operator

We hereby submit an application to register as a **Non-Interbank Payment System Operator** in accordance with Section 36(cc) of the Central Bank Act, Chapter 79:02.

We declare to the best of our knowledge that the information furnished is true, correct and complete.

Name:

Designation:

Company Seal:

Date:

Place:

APPENDIX 3:**INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) OUTSOURCING
QUESTIONNAIRE****Instructions:**

1. This **Questionnaire** is to be completed by officers who have direct knowledge of the institution's technology operations and systems. The response should be verified by the officer's superior.
2. The most recent information should be provided. For items that are not applicable, please indicate with "N/A".
3. Attachments should be included where appropriate.

General Company Information:**A. Business Model and Objectives**

1. Describe the company's business model relative to the proposed application.

2. What are the company's business objectives?

3. Provide an overview of how technology supports the company's business objectives.

4. Who are the business' primary customers and consumers of the service being proposed?

APPLICATION

1. Does the service proposed include an e-commerce offering? If yes, describe this offering and indicate if there are restrictions on who may use the offering (e.g. residency, location, age, etc.).

B. ICT Risk Management

2. Provide the company's risk management policy, framework and/or procedures which make provisions for the identification, assessment, treatment and reporting of technology-related risk.

3. What governance structures exist to ensure that risks are suitably managed? Considerations include:

- a. Do board committees exist with oversight of the Risk Management function?

- b. Has the organisation defined a risk profile, risk appetite and/or tolerance?

- c. What is the nature, extent and timing of the risk information reported to the Board?

4. Provide the terms of reference for any board or management committees with responsibility for risk management and/or compliance?

APPLICATION

5. Provide a summary of the most recent risk assessment executed and/or current risk register, including but not limited to:
 - a. Description of the key risks identified
 - b. Assessed likelihood, impact and overall rating
 - c. Risk treatment options to reduce the risk to acceptable levels (if applicable)
 - d. Risks requiring further attention

C. System Infrastructure

1. Describe (or provide supporting graphic(s) to show) the technology infrastructure supporting the proposed payment service. Consideration should be given to describing the hardware and software components; the interfaces, communication links & relationships between them; and system users/owners.

2. If not previously provided in other submissions or as a response to other queries, describe (or provide supporting graphic(s) to show) the high-level data and information flows:
 - a. between entities and system components; and
 - b. from the stages of capture through to processing and eventually storage.

3. Indicate where applicable, the communication mediums (e.g. email, physical receipt, electronic statement, etc.) made available to the customers/consumers for each process in the life cycle of the transactions (from initiation to final confirmation).

D. Information Security

1. Provide the relevant policy, framework and/or procedure documents which address matters related to Information Security.

2. Do procedures performed by the company's internal and/or external auditors include IT audit procedures and include at a minimum a review of IT General Controls?
 - a. If yes, provide a copy of the most recent audit report showing relevant details including IT audit findings, management responses (if available) and remediation status.

3. If applicable, provide details as to the nature and extent of insurance coverage for loss events related to information/cyber security incidents.

4. Describe the physical and environmental security controls in place to safeguard the ICT infrastructure.

5. Describe the controls in place to protect your internal network, the proposed payment system and/or the vendor's network from externally originating attacks.

APPLICATION

6. Describe the controls in place to ensure that data at rest on infrastructure either on-premises, owned by the customers/consumers of the service (e.g. mobile phones) or your third-party providers is secure and protected from potential threats, in particular unauthorised disclosure and intentional or unintentional data leakage.

7. Describe the controls in place to ensure that data in transit between your on-premises infrastructure, your customers/consumers of the service and your third-party providers is secure and protected from potential threats, in particular unauthorised disclosure and intentional or unintentional data leakage or modification.

8. If encryption is used as a security measure as part of the proposed payment system, please provide details of the following:
- a. Encryption algorithm(s) in use.
 - b. Key length.
 - c. Controls in place to protect any private keys from exposure (e.g. key management solutions)
 - d. Controls in place to ensure lost/breached keys can be revoked.
 - e. Controls in place to ensure keys remain available and are not lost/rendered inaccessible.
 - f. Controls in place to log and monitor access to keys and restrict access to authorised persons only.

9. Provide the relevant policy, framework and/or procedure documents which address matters related to information security awareness and training.

E. Patch & Vulnerability Management

1. Provide the relevant policy, framework and/or procedure documents which address matters related to patch management and vulnerability management.

2. Have independent security specialists been engaged to assess the security posture of and identify vulnerabilities in the computing environment¹.
 - a. If yes, provide a copy of the most recent assessment/review showing relevant details including but not limited to the scope, methodology and results.

F. Reliance on Third Parties – Service Organisations, Vendors or Related Parties.

1. Is there a formally defined and documented process for managing reliance on Service Organisations, Vendors and/or Related Parties? If yes, please provide supporting evidence; otherwise if no, please explain.

¹ Applications, systems and/or networks both hosted by the applicant and provided via outsourced arrangements.

APPLICATION

2. Describe the extent to which there is reliance on services, products or infrastructure provided by Service Organisations, Vendors and/or Related Parties ².

Name of service organisation, vendor or related party.	Nature of service provided and the internal process/operation it supports.	Critical/Core Service? (Y/N)	Name of service organisation, vendor or related party.
<i>e.g. ACME Cloud Corp</i>	<i>Provided: Infrastructure as a Service</i>		<i>e.g. ACME Cloud Corp</i>

3. Describe for each of the identified parties in **F2** above, the nature and extent of due diligence performed in onboarding the identified party. For example:

- What considerations have been made relative to competence and experience?
- Have Service Organisation Controls Attestation reports been requested and reviewed?
- Have suitable certifications been requested and reviewed (e.g. ISO27001, PCI-DSS, etc.)?
- Have other independent audit or assessment reports been requested and reviewed?
- Have onsite visits/testing for the purpose of assessing suitability been performed?

Name of service organisation, vendor or related party.	Nature and extent of due diligence performed.
<i>ACME Cloud Corp</i>	<i>Reviewed SOC2 for period covering Oct 2018 – Sep 2019.</i> <i>Confirmed ISO27001 certification obtained from competent assessor.</i> <i>Performed suitability analysis as part of contract negotiations.</i>

4. In the course of undertaking the due diligence described in **F3** above, were there any findings of note or issues arising. For example:
- Qualified opinions, adverse findings or emphasis of matter paragraphs in audit reports.
 - Deficiencies in the design or operation of controls reviewed by external assessors.
 - Information on security-related incidents, attacks or breaches.
 - Revocation of relevant certifications (e.g. PCI, ISO, FedRAMP)

² Responses should not be limited to technology related outsourcing.

APPLICATION

Name of service organisation, vendor or related party.	Issues arising from due diligence performed.
<i>ACME Cloud Corp</i>	<i>SOC2 report contained one issue related to a physical control at a European data center. This was deemed not critical for us as our data is housed in US facilities and the finding was low risk.</i>

5. For each of the identified parties in **F2** above, have considerations been made as to the extent of the use of sub-service organisations by the contracted service organisation or vendor.

Name of service organisation, vendor or related party.	Nature and extent of their use of sub-service organisations, as well as considerations on the possible business impact.
<i>e.g. ACME Cloud Corp</i>	<i>ACME Cloud Corp outsources data center management to XYZ Ltd. The contract with ACME ensures any risks from sub-contracting are managed by ACME who puts suitable controls in place.</i>

6. If any of the third parties provide services that are reliant on infrastructure that serves multiple tenants and/or comingles your data in an environment with that of any other entity, describe the controls in place to address the associated risks.

7. If any of the third parties provide software, a web-based service or a service dependent on cryptographic keys, is there an escrow agreement included in the contract to ensure maintenance of the software and/or accessibility of the service in the event of vendor disruption?

APPLICATION

8. Describe the conditions, based on the contractual agreement, under which you may terminate the services provided (e.g. in the event of default, ownership change, insolvency, change of security or serious deterioration of service quality).

a. What controls are in place to identify and/or correct the conditions identified above?

9. Describe the controls in place to ensure that at the end of the service delivery period, or as necessary:

- a. All data (including backups) related to the service can be securely destroyed or removed from the Service Provider's infrastructure.
- b. The service may be transitioned to a new service provider or brought in-house, without disruption to the customers/consumers.

10. For each of the identified parties in **F2** above, describe the nature of the access held by the service provider and the controls to mitigate the risk of unauthorised access. In particular:

- a. Does the provider have access to manage servers, database platforms or other infrastructure components?
- b. Does the provider have access to manage the platforms upon which the service is delivered (e.g. web hosting platforms or development environments)?
- c. Does the provider have access to manage any applications within which your data or that of the customers/consumers of the service sit?
- d. Does the provider have direct data access independent of any of the methods outlined in a-c above?

Name of service organisation, vendor or related party.	Nature of access held by the service provider (inclusive of privileged/remote access)	Controls to mitigate the risk of unauthorised access to sensitive data
<i>e.g. ACME Cloud Corp</i>		

G. Business Continuity, Disaster Recovery & Resilience

APPLICATION

1. Provide the company's Business Continuity/Disaster Recovery (BCP/DR) policy, framework and/or procedures which make provisions for the resilience, recovery and resumption of business processes when operations have been disrupted unexpectedly.

2. Provide details related to the testing of the Company's Business Continuity/Disaster Recovery Plans, inclusive but not limited to the types of testing performed (e.g. tabletop, simulation, full recovery, etc.), the frequency of testing and the most recent results of tests performed.

3. Provide the company's policy, framework and/or procedures which make provisions for the management of the backup data life cycle, which includes the frequency of data backup, data retention period, data storage mechanisms, secure destruction and the restoration testing of backup data.

4. Provide details of the following relative to the proposed system:

Parameter	Comment
Expected system uptime (availability)	99%
Recovery Point Objective	12 hours
Recovery Time Objective	36 hours
Location of offsite backups	Tobago & Cloud
Use of encrypted backup media	Encrypted in cloud & on disk

APPLICATION

5. Describe, or provide supporting evidence to show, the extent to which your BCP/DR process considers the impact of reliance on Service Organisations, Vendors and/or Related Parties.

6. Provide details on the maximum processing capacity expected (e.g. transaction volume, number of concurrent connections, data/operation requests per time interval, etc.).
- a. Has a stress test or other assessment been performed to validate the ability to handle the expected capacity?

- b. What measures are in place to monitor and manage capacity over time, including periodic spikes (e.g. holiday seasons) and potential natural growth?

7. For each of the third parties identified in Question **F2**, complete **Appendix 1.0**.

H. Change & Release Management

1. Provide the company's policy, framework and/or procedures which make provisions for:
- a. The management of all changes (additions, modifications or removals of any software or software components) that could have an impact on the proposed payment system.
- b. The protection of the integrity of the production environment by ensuring changes are released and deployed to the live environment effectively, efficiently and safely.

2. What governance structures are in place relative to the Change & Release process (e.g. Change Advisory Board, Steering Committee, Technical Oversight Committee, etc.)?

3. How are changes (both software and hardware related) to the proposed payment system initiated, authorised and tracked?

4. What is the nature, extent and scope of testing performed prior to having a change approved for the move to the production environment?

5. Who has access to make changes to the production environment? How does the organisation ensure changes are not made to the production environment without proper approval?

6. Describe the controls in place to ensure the computing environments used for systems development, testing, staging and production are logically segregated.

7. What controls are in place to ensure segregation of duties exists in the change management environment?

8. What constitutes an emergency change and how does the process for emergency changes differ from the standard change management process?

9. Describe the nature, extent and scope of measures, both technical and non-technical to ensure all systems and software internally developed are reasonably secured from cyber-attack.

10. Describe the extent to which the customer/consumer as well as other stakeholders (inclusive of the Central Bank) are notified of system changes, inclusive but not limited to new features and functionality as well as changes to operational processes and models.

11. For each of the third parties identified in Question **F2**, complete **Appendix 2.0**

I. Incident Management

1. Provide the company's policy, framework and/or procedures which make provisions for the management of incidents, including but not limited to the handling of IT incidents, including cyber related incidents; maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents.

2. Provide the company's policy, framework and/or procedures which make provisions for the management of problems, including but not limited to how recurring incidents are identified as problems and handled through to resolution and how recurring incidents are prevented and/or reduced.

APPLICATION

3. Using the table below, describe the general nature of incidents (not necessarily every incident, but a high-level view) which may impact the customers/consumers of the proposed payment system and provide supporting details.

General nature of incident	How customer/consumer is notified?	What is the expected timeline for communicating identified incidents?

4. For each of the third parties identified in Question **F2**, complete **Appendix 3.0**.

Appendix 1.0

Name of service organisation, vendor or related party.	Provider has an established BCP/DR Process? (Yes/ No/ NA)	Does the process provide for both data recovery as well as restoration of the service?	How often does the provider perform data backups & test restorations?	<etc.>
<i>e.g. ACME Cloud Corp</i>	<i>Yes</i>	<i>Service Restoration only as ACME only provides infrastructure and not data services</i>		

APPLICATION

Appendix 2.0

Name of service organisation, vendor or related party.	Provider has an established Change & Release Process? (Yes/ No/ NA)	Describe the nature, extent and scope of changes the Provider may make.	Describe the impact the possible range of changes may have on the proposed payment system.	What measures are in place to manage the potential impact of changes made by the service provider?
<i>e.g. ACME Cloud Corp</i>	<i>Yes</i>	- Changes to underlying hardware devices on which service is delivered - Changes to web server administrator panel. - Operating system & database platform upgrades	- Changes to hardware are not expected to have an impact. - Admin panel changes will impact internal operations and not customer-facing services - System or platform changes may require us to update our payment system component XYZ for compatibility	- N/A - None – Admin panel changes are usually cosmetic and of low complexity. - Contracts require the vendor to notify us four weeks prior to major version changes. Our development process and codebase are robust enough to mitigate for all other minor changes

Appendix 3.0

Name of service organisation, vendor or related party.	Provider has an established Incident Management Process? (Yes/No/NA)	Is the Provider contractually obligated to notify of incidents or issues related to the service? What are the timelines?	Does the contract with the Provider detail the liabilities that each party is willing to assume and the insurance available to cover incidents?	Describe the nature of internal procedures designed to address potential incidents with the Provider.
e.g. ACME Cloud Corp	Yes	Yes – if incident is related to information security or a potential or actual breach in an SLA. Timelines are defined in the attached SLA.	Yes	The BCP makes provisions for this. In summary, manual processing arrangements, alternate providers or localised failbacks are available, dependent on the provider/service.