REQUEST FOR PROPOSAL NO. 003-2022

PROVISION OF E-CASHBOOK CYBER SECURITY ASSESSMENT

Trinidad & Tobago International Financial Centre

Management Company Limited (TTIFCMCL)

15th Floor, Tower D

International Waterfront Centre

#1 Wrightson Road, Port of Spain

30th November 2022

TABLE OF CONTENTS

1.0 ABOUT TTIFCMCL 2

1.1 RFP Background 2

1.2 RFP Objective 3

2.0 INSTRUCTIONS TO BIDDERS 3

2.1 Project Designate for Communications 3

2.2 Examination of RFP 4

2.3 RFP Clarifications 4

2.4 Addenda 4

2.5 Proposals 4

2.5.1 Required Information 5

2.5.2 Additional Information 6

2.6 Conflicts of Interest 7

2.7 Additional Disclosures 8

3.0 SCOPE OF WORKS 9

4.0 SCHEDULE OF EVENTS 11

4.1 Request for Proposal (RFP) Schedule 11

4.2 Submission of Proposals 11

4.3 Basis of the Evaluation 11

4.4 Evaluation Criteria 12

4.5 Contract Award and Notification 12

APPENDIX A 13

1.0 ABOUT TTIFCMCL

The Trinidad and Tobago International Financial Centre Management Company Limited (TTIFCMCL) was established in 2008 by Cabinet Minute No. 2647 and incorporated on November 6, 2008.

Our Vision

To be the driver of digital financial services adoption across all sectors leading Trinidad and Tobago in becoming the regional premier location for FinTech-enabled services.

Our Mission

The continuous expansion of the Financial Services Sector through the integration and application of Financial Technology thereby improving service delivery for the citizens, the ease of doing business and increasing financial inclusion.

The TTIFCMCL aims to act as the first point of contact, facilitator, and 'resourceful ally' for all stakeholders, related to Trinidad and Tobago becoming a 'Cashless society' and a 'FinTech-enabled Financial Services Hub'. In keeping with our objectives and to continue the accelerated drive towards the digitalisation of payments across Ministries, Departments and Agencies (MDAs), the TTIFCMCL developed an automated electronic solution, known as the TTIFCMCL's e-cashbook, to facilitate the reconciliation of revenue collected by the Government. This e-cashbook aims to bring funds to account digitally and comply with the guidelines as communicated by the Treasury Division (TD) and set out in the Exchequer and Audit Act 69.01.

1.1 RFP Background

This Request for Proposal (RFP) was developed to augment the assessment framework of the Trinidad and Tobago Cyber Security Incident Response Team (TTCSIRT) and thereby provide an independent security and vulnerability assessment of the TTIFCMCL's e-cashbook as a critical solution component in bringing revenue to account electronically by Ministries, Departments and Agencies (MDA's) within the Government of the Republic of Trinidad and Tobago (GoRTT). The vulnerability assessment (VA) should entail internal and external testing to assess the effectiveness or ineffectiveness of the security infrastructure installed within the e-cashbook

The RFP is therefore designed to procure a combined Technical and Financial Proposal ("Proposal") from a firm with specialist skills in developing and conducting Vulnerability Assessment and Penetration Testing (VAPT), as the TTIFCMCL seeks to develop, evaluate, and

test the security and vulnerability of its e-cashbook. A robust methodology and framework are required to ensure industry best practices are employed.

For this assessment, the framework should be designed utilising the methodological guidance of the core OWASP Application Security Verification Standard (ASVS), with Level 2 as the baseline, to allow for useful international comparisons. A country-specific analysis would also be required to provide the methodological guidance necessary to inform best practices.

1.2 RFP Objective

The TTIFCMCL invites proposals for the provision of services for the design, execution, and management of a VAPT to establish a holistic understanding of the level of security within the TTIFCMCL's e-cashbook. The objective of the RFP is to:

a) Perform Application Security Assessment utilising the OWASP ASVS, which comprises a VAPT.
b) Identify whether multiple lower or medium-risk vulnerabilities constitute a higher risk rating when exploited together.
c) Perform both internal and external penetration testing from a remote location.
d) Perform penetration testing and vulnerability assessments against web applications using manual testing techniques to identify technical and business-logic-related vulnerabilities. Identified vulnerabilities should follow the OWASP issue classification framework.
e) Provide a follow-up assessment in the event that breaches are identified during testing and ensure such issues have been appropriately addressed.
f) Perform automated assessments using industry-leading scanning tools based on the application type and the access provided.

2.0 INSTRUCTIONS TO BIDDERS

2.1 Project Designate for Communications

The representative designated by the TTIFCMCL for this RFP who will be responsible for all communications or will otherwise deal with bidders is Mrs. Trina Peters-Thompson, Corporate Services Officer. All correspondence about the RFP will be issued by requestforproposals@ttifc.co.tt.

2.2 Examination of RFP

Bidders are responsible for examining, with appropriate care and attention, all instructions in the RFP and are responsible for ensuring that they are aware of all conditions that may, in any way, affect the proposed deliverables and the associated cost. Failure to do so shall be at the sole risk of bidders. No relief will be given for errors or omissions.

2.3 RFP Clarifications

If a bidder believes there are discrepancies in or omissions from the RFP or should the intent or meaning of any provision be unclear or ambiguous, or should any question arise relative to the RFP - the bidder should promptly notify the TTIFCMCL via e-mail using the following address: **electronic mail**: requestforproposals@ttifc.co.tt.

All requests for clarification must be submitted by the date and time indicated in **Section 4.1 - RFP Schedule**. An acknowledgment of all requests for clarification will be sent. Replies to such requests, if necessary, will be in writing, and copies of all questions and answers will be provided to all bidders. No requests for clarification received after the specified date and time will be entertained.

2.4 Addenda

The TTIFCMCL shall, if necessary, issue written addenda changing this RFP at any time prior to the date and time indicated in **Section 4.1 - RFP Schedule** (except for addenda to extend any deadline under this RFP, which may be issued at any time). Addenda will be issued by the project designate for communications to bidders. No changes to this RFP will be effective unless undertaken by an Addendum issued under this paragraph.

Should any addenda be issued by TTIFCMCL with respect to this RFP, bidders are required to submit their proposals with a signed and dated copy of each Addendum.

2.5 Proposals

Responses to this RFP should be prepared in a manner that will facilitate the evaluation and decision-making process and must therefore comply with the requirements of this RFP. Failure to submit the required information may result in the proposal not being evaluated.

2.5.1 Required Information

Proposals that do not include the following in the structure laid out will NOT be evaluated.

- **Table of Contents**
- **Contact information**
  - Bidder registered name and registered address
  - Name and title of a contact person
  - Address and telephone number a contact person
  - E-mail address of a contact person

- **Bidder Information**
  - Bidder profile/brochure.
  - A minimum of three (3) completed Reference Survey Forms with contact name and number (See Appendix A).
  - The Company reserves the right to contact the references provided. The Reference Survey Form should include the Reference's name and contact information on the completed Reference Survey Form (Appendix A). The information collected from references will be kept in the strictest confidence.
  - One (1) bank reference on the respective bank's letterhead.
  - Last three (3) financial statements (audited if available) or Practice Monitoring Status Letter.
  - Description of completed work of a similar nature. Names and contact numbers for client representatives must be provided. Samples should be provided where possible.
  - Résumés outlining work experience and qualifications of key personnel.

- **Company Certificates**

  Proposals **must** be submitted with the following documents (where applicable):
  - Certificate of Incorporation/Continuance
  - VAT Clearance Certificate / or relevant tax clearance form
  - Income Tax Clearance Certificate
  - National Insurance Compliance Certificate

If the requested statutory documents are unavailable by the date of submission, bidders are asked to submit a letter duly signed by a minimum of two (2) Directors advising of the

status of said documents. All statutory documents must be submitted before the award of the contract.

- **Technical Proposal**

  The Scope of Work **must** be used to draft the technical proposal and organised in alignment with the evaluation criteria. The respective technical proposals must address all the areas outlined in the Scope of Works in enough detail to allow for a proper evaluation of the proposal and include the following in EACH segment:

  - Overall approach and methodology
  - Detailed project timeline and milestones (GANTT Chart)
  - A plan detailing the type of canvas, methodology, strategy, and timelines for execution of all project milestones,
  - Resources to be allocated
  - The number, role, and expertise of the staff members relevant to this proposal (i.e., those that will be executing the work).

- **Financial Proposal**

  Financial Proposals are to be submitted as a document separate and apart from the Technical Proposals. Bidders are expected to provide one financial proposal **delineated by segment**. All add-on, out-of-pocket, and other costs **must** also be included and identified.

  In addition to a Total Cost, the financial proposal must be structured as follows:

DESCRIPTION OF SERVICES	AMOUNT (TTD)
FRAMEWORK/METHODOLOGY	TT$
TECHNICAL ASSESSMENT	TT$
FINAL REPORT	TT$
TOTAL COST	**TT$**

  Bidders are encouraged to submit competitive financial proposals based on their operating expenses.

2.5.2 Additional Information

1. All pages in the proposal must be numbered.

2. All costs associated with the preparation of a proposal will be entirely at the expense of bidders.
3. Proposals received after the time and date stipulated in **Section 4.1 - RFP Schedule** will be rejected. Requests for extensions will only be granted in exceptional circumstances. Proposals received after the date and time of an extension will be rejected.
4. Quoted fees must cover all the required deliverables and should be provided in as much detail as possible.
5. If quoted fees are discounted, the basis for the discount must be provided.
6. Value Added Tax (VAT) or relevant taxes must be shown separately.
7. Out of Pocket/Administrative Expenses must be shown separately.
8. All fees must be quoted in Trinidad, and Tobago dollars or equivalent (where applicable, assumed exchange rates should be clearly stated) and must be valid for a minimum period of ninety (90) days from the RFP closing date.
9. The terms and schedule of payments must be provided.
10. The evaluation of proposals in response to this RFP should not be interpreted as a commitment to accept any of the proposals submitted.
11. TTIFCMCL reserves the right to cancel this RFP in part or in its entirety without liability for any costs incurred by bidders in preparing and submitting a proposal.
12. TTIFCMCL shall be under no obligation to enter into any discussions or facilitate correspondence for the purpose of seeking clarification to the proposals of each
13. bidder. However, TTIFCMCL reserves the right to request any or all bidders to explain or elaborate on their proposal without incurring any obligations whatsoever.
14. TTIFCMCL does not bind itself to accept the proposal with the lowest cost.
14. TTIFCMCL reserves the right to reject any or all proposals or to accept the proposal that, in its judgment, is deemed to be in its best interest and reserves the right to waive any or all of the requirements stated in this RFP.
15. TTIFCMCL reserves the right to reject a proposal that does not comply with any of the requirements of this RFP.

2.6 Conflicts of Interest

To avoid any conflict of interest, bidders must provide the following:

1. A statement describing any potential conflict of interest or appearance of impropriety relating to other clients of the bidders or officers of TTIFCMCL, which could be created by providing services to TTIFCMCL.
2.

2.7 Additional Disclosures

Details	Yes/ No
1. Have you or your organisation ever operated under a contract in which financial penalties could be incurred?	
2. Have you or your organisation ever been asked to pay financial penalties levied in respect of failure to fulfil the terms of a contract?	
3. Have you or your organisation ever had a contract terminated or your employment determined under the terms of a contract?	
4. Have you or your organisation ever been refused renewal of a contract for failure to fulfill the terms of the contract?	
5. Have you or your organisation failed to complete a contract under any circumstances within the last three years?	
Please indicate whether the following applies to your organisation as a bidder.	
6. Is bankrupt, under administration by the court, has entered into an agreement with creditors, has suspended business activities, or is in any similar position arising from national laws and regulations?	
7. Is subject to proceedings for a declaration of bankruptcy, for an order for compulsory winding-up or administration by the court, an arrangement with creditors, or of any similar proceedings under national law and regulations?	
8. Has been found guilty of professional misconduct by a judgment which has the force of res judicata?	
9. Is subject to ongoing proceedings for professional misconduct?	
10. Has been found guilty of not fulfilling its obligations relating to the payment of national insurance contributions in accordance with the legal provisions of the country of registration/incorporation or with those of Trinidad and Tobago?	
11. Has been found guilty of not fulfilling its obligations relating to the payment of taxes in accordance with the legal provisions of the country of registration/incorporation or with those of Trinidad and Tobago?	
12. Is the subject of any pending litigation and/or regulatory action by any oversight body that could have an adverse material impact on the firm's ability to serve TTIFCMCL?	
If the answer to any of these questions is Yes, please elaborate on a separate sheet.	

3.0 SCOPE OF WORKS

TTIFCMCL wishes to identify a suitable vendor for the design, execution, and management of a VAPT of its e-cashbook solution.

3.1. Key Activities

The TTIFCMCL wishes to Interrogate the solution's defences against adversaries that have circumvented perimeter security, such as individuals with facility access or compromised workstations deployed with Remote Access Tools (RAT). The key testing activities include:

a) Employ web application security assessment against the web applications using a combination of manual and automated testing techniques.
b) Identify vulnerabilities that would allow the exploitation of, or allow unauthorized parties to gain privileged access to, systems and applications in the internal network.
c) Employ targeted testing to simulate threat adversaries which may compromise the network and attempt to move laterally within the TTIFCMCL's network.
d) Execute automated assessments using industry-leading scanning tools based on the application type and access provided.
e) Conduct a manual review to validate high-risk findings identified by the tools stated to check for false-positive results from the automated scanner.
f) Perform penetration testing and vulnerability assessments against web applications using manual testing techniques to identify technical and business-logic-related vulnerabilities.
g) Classify any identified vulnerabilities based on the OWASP issue framework, which should include an associated risk rating and recommendations on resolving the issue.
h) Conduct testing within parameters that facilitate the understanding of whether multiple lower – or medium-risk vulnerabilities constitute a higher-risk rating when exploited together.

The use of the aforementioned testing techniques should facilitate the analysis of potential exploits that may include, inter alia:

a) Common web and web service vulnerabilities. **The utilisation of the OWASP ASVS is strongly preferred.**
b) Password, authentication, and credential replay vulnerabilities.
c) Patching and system hardening vulnerabilities.
d) Firewall and network access control vulnerabilities.
e) Database vulnerabilities (DB2, SQL Server, MySQL, Oracle).

f) Web server vulnerabilities (IIS, WebSphere, Apache, Tomcat).
g) Remote services vulnerabilities (including Telnet, SSH, VNC, PCAnywhere, X-11, trusted hosts, and rlogin).
h) VoIP vulnerabilities.
i) Windows, UNIX, and Linux vulnerabilities.
j) Mail Server vulnerabilities.
k) Gaps in data loss prevention strategies, solutions, and configurations.
l) Gaps in anti-virus/anti-malware configurations, coverage, and operating effectiveness.
m) Gaps or misconfigurations in intrusion detection and prevention and its operating effectiveness.
n) Vulnerabilities in protocols such as Remote Procedure Calls (RPC), Network File Systems (NFS), Server Message Block (SMB), Domain Name Server (DNS), and Simple Network Management Protocol (SNMP).
o) Microsoft Active Directory privilege misconfigurations (e.g., GenericAll, DS-Replication, etc.), Kerberos authentication abuses (e.g., Kerberoasting), Local Administrator Password Solution (LAPS) abuses, Active Directory Certificate Services abuses.
p) Trust relationships, backdoors, and misconfigurations.
q) General enticement information.

3.2. Key Deliverables

The expected deliverables include inter alia:

a) Framework and Methodology.
b) Web Application Security Assessment Methodology.
c) Vulnerability Assessment.
d) Penetration Testing.
e) Detailed written report on findings, explicitly stating recommendations for corrective action.
f) Power-Point presentation, which supports the written report.
g) A Follow-up assessment to ensure that the identified issues have been appropriately addressed.

The selected bidder and the TTIFCMCL will agree on the final structure and contents of the report before its commencement. All related graphs, charts, tables, appendices, and other references must be transposed into an appropriate format.

4.0 SCHEDULE OF EVENTS

4.1 Request for Proposal (RFP) Schedule

Activity	Date	Time
RFP Release	30th November 2022	
Deadline for Clarifications	01st December 2022	4:00 pm
Deadline for Addenda	5th December 2022	4:00 pm
Deadline for Submission of Proposal	06th January 2023	4:00 pm
Expected Date for Notification to Bidders	19th January 2023	4:00 pm
Standstill Period	20th – 26th January 2023	4:00 pm
Expected Date for Contract Award	31st January 2023	

4.2 Submission of Proposals

Proposals must be submitted by **06th January 2022 at 4:00pm** via email.
Proposals submitted after this time will NOT be accepted.
Email Address: FST.Proposals@ttifc.co.tt
Subject: Provision of Financial Inclusion Survey

4.3 Basis of the Evaluation

Proposals submitted in response to the RFP will be evaluated by a TTIFCMCL team that will report and make recommendations to TTIFCMCL's management on the proposals received.

If a proposal does not include all of the required information, it may be rejected. If TTIFCMCL determines that a bidder failed to demonstrate that it possesses the technical or financial capability to provide the required service or that a bidder has a litigation history that is of concern to TTIFCMCL, its proposal may be rejected.

4.4 Evaluation Criteria

Proposals will be reviewed objectively and evaluated based on the information requested.

No.	Qualification Criteria	Max Score	Min Score
1.	Approach, Methodology and Project Plan a) Understanding of the assignment **(5 pts)** b) Methodological approach based on the RFP scope **(20 pts)** c) Proposed project plan with project milestones and timelines **(10 pts)**	35	70%
2.	Qualifications and experience a) Firm's experience in Cyber Security **(5 pts)** b) Demonstrates the ability to identify vulnerabilities and potential threats **(10 pts)** c) Demonstrated experience in performing Cyber Security Assessments for Government Entities **(5 pts)** d) Completion of a minimum of 3 projects in last 5 years involving Cyber Security Assessments **(5 pts)** e) Experience and qualifications of the key personnel to be assigned to the project **(5 pts)**	30	70%
3.	Client References (from three Clients)	10	70%
4.	Financial Proposal	25	70%
	Total	100	70%

4.5 Contract Award and Notification

All bidders will be notified of the outcome of the RFP in writing by an authorised representative of the TTIFCMCL. If no challenges are raised during the Standstill Period, the selected bidder will be invited to negotiate the final terms of the project before the signing of a contract - at the end of the Standstill Period.

APPENDIX A

REFERENCES – CLIENT SATISFACTION SURVEY FORM

Instructions:

1. Please have your references complete this form and include it with your submission. (Additional numbered sheets may be used if necessary)
2. Questions should be answered using the Response Options provided only. Failure to do this will result in the response not being accepted.

Print Name and Address of Client:

Name and Position of Official completing the form:

Telephone number: **E-mail address:**

	Questions	**Response Options:** Very Satisfied/ Satisfied/ Neutral/ Dissatisfied/ Very Dissatisfied (give reasons for dissatisfaction)
1	How satisfied were you with the consultant's timelines for the completion of the deliverables?	
2	How satisfied were you with the consultant's adherence to the agreed upon budget?	
3	How satisfied were you with the approach of the consultant to understanding your organisation's needs? (Give an example of what the consultant did to facilitate this.)	
4	How satisfied were you with the consultant's project management approach? (Identify an area where you believe there was a need for improvement if applicable.)	
5	How satisfied were you with the consultant's approach to communication of issues or feedback? (Give an example of this.)	
6	How satisfied were you with the overall support received over the duration of the project?	
7	How satisfied were you with the consultant's recommendations?	

REFERENCES – CLIENT SATISFACTION SURVEY FORM (cont'd)

	Questions	**Response Options:** Very Satisfied/ Satisfied/ Neutral/ Dissatisfied/ Very Dissatisfied (give reasons for dissatisfaction)
8	How satisfied were you with the consultant's performance during the project?	
9	How satisfied were you with the overall value for money spent?	
10	Any other comments or points to note:	

Signature: _____ Date: _____

Please affix the Company stamp: