Bengal Commercial Bank PLC.
General Services Division
Head Office

October 03, 2024

Request for Quotation (RFQ) for conducting SWIFT (Society for Worldwide Interbank Financial Telecommunication) CSP (Customer Security Program) Assessment 2024 for Bengal Commercial Bank Ltd.

1.1 Scope of works

Bengal Commercial Bank Limited (Hereinafter referred to as "the Bank") wishes to receive bids from the bonafide firms for conducting SWIFT CSP Assessment 2024 for Bengal Commercial Bank Ltd. In general, the scope of assessment includes CSP Assessment based on SWIFT Independent Assessment Framework to assess the effectiveness of implementation of all mandatory and advisory controls as per CSCF v2024. Moreover, the assessment will cover the SWIFT architecture at Bengal Commercial Bank Limited, Head Office having centralized Trade Services operation with 02 (two) Authorized Dealer (A.D.) Branches.

The Objectives and Principles of SWIFT CSP is summarized below:

Objectives:

1. Secure the Environment
2. Know and limit access
3. Detect and respond

Principles:

1. Restrict Internet access and protect critical systems from General IT Environment
2. Reduce attack surface and vulnerabilities
3. Physically secure the environment
4. Prevent compromise of credentials
5. Manage identities and segregate privileges
6. Detect anomalous activity to system or transaction records
7. Plan for incident response and information sharing

Assessment Scope

The entire assessment will be conducted onsite at Bank premises or remotely by eligible and experiences vendors in cross-border locations.

In Scope:

Scope of Security Controls:

- Local SWIFT Infrastructure
- Operators PC
- Operators
- Data Exchange Layer
- Middleware Server (Advisory)
- File Transfer Server

Out of Scope:

- Back Office including Middleware client
- General Enterprise IT Environment
- Connections to the SWIFT Network

Assessment must cover all mandatory controls set out in the latest version of the SWIFT Customer Security Control Framework (CSCF) that are applicable to the Bengal Commercial Bank Limited in line with architecture type and infrastructure.

The assessment includes all components in scope of the Bank's SWIFT-related infrastructure as documented in the CSCF. These include the following basic systems, operators and devices where relevant.

• Data Exchange Layer
− The transport of data between the SWIFT infrastructure and the back office first hop, in direct or through Middleware Server(s), is advised for consideration although it is not compulsory

• Local SWIFT Infrastructure
− Secure Zone
− Messaging Interface
− Communication Interface
− SWIFTNet Link (SNL)
− Connector
− SWIFT Hardware Security Modules (HSMs)
− Firewalls, routers and switches within or surrounding the SWIFT infrastructure
− Graphical User Interface (GUI)
− Jump Server
− Virtualisation Platform
− Dedicated Operator PC

• Operators and their General Purpose Operator PCs
The assessment should confirm the architecture type selected and encompass all production, Disaster recovery (DR), and/or backup environments (as applicable) that house any of the above systems, operators or devices.

Once the scope is established, the timing can be determined to ensure that the report will be delivered in time to enable the Bank to submit its associated KYC-SA Attestation into KYC-SA within the normal attestation window - from early July until the year-end deadline of 31December.

Assessment Approach:

- **Planning:** A risk assessment of in scope are in the Bank and review of the control environment.
- **Risk Assessment:** Discussion with the Bank's management and assess its information processing system, internal & external environment, significant events as well as social factors to determine and document areas of risk. Once areas of risk have been identified the next process will be to review the control environment.
- **Gap Assessment and Report:** Help in understanding the impact of a new standards implementation in the business operations as well as provide a detailed specification of requirements.
- **SWIFT CSP Assessment:** Once the gaps have been mitigated, the final CSP assessment will be conducted based on SWIFT Assessment framework.

Other terms & conditions of assessment approach:

As per latest version of SWIFT Customer Security Program, Independent Assessment Framework v2024 1.1 to assess the effectiveness of implementation of all mandatory and advisory controls as per CSCF v2024).
The deadline for assessment report to SWIFT is **31 December 2024**.

1.2 Technical Offer

Vendor should submit technical offer as per specification mentioned in Annexure-A.

1.3 Financial Offer

Vendor should submit financial offer as per prescript format mentioned in Annexure-B.

1.4 Product and Platform

SWIFT Customer Security Program

1.5 Bidder's qualification

The Bidder/Vendor/Assessor has recent (within twelve months) and relevant experience to execute a cyber-security-oriented operational assessment to an industry standard such as PCI DSS, ISO 27001, NIST SP 800-53, SOC2, the NIST Cyber security Framework or simply CSP/CSCF

The lead assessor must hold at least one industry-relevant professional certification and other individuals could hold similar certification:

- PCI Qualified Security Assessor (QSA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- ISO 27001 Lead Auditor
- System Administration, Networking, and Security Institute (SANS) GIAC (Global Information Assurance Certification)

a) The bidder shall possess his own office in Bangladesh and adequately trained and experienced manpower to implement such type of Assessment.
b) This invitation of proposal is open to all companies registered in Bangladesh. The bidder must be a company focusing on independent assessment of Customer Security Programs.
c) The Bidder should submit detail technical and commercial proposal with Assessment plan with assumptions and limitations if any, Assessment Objectives, mandatory and advisory security controls to cover, assessment scope, assessment report
d) The bidder should submit the details of Knowledge transfer/Training plan after completion of assessment.
e) The bidder should have be capable for 24/7 Support, Services and Communication facility.

1.6 Documents comprising the bid

a. Technical Description of the deliverables to demonstrate the specified technical requirement
b. Schedule for financial proposal
c. Photocopy of following documents may be submitted with the offer:
    i. Valid Trade License and Company Profile.
    ii. E-TIN, BIN and VAT Certificate
    iii. Name, contact number and e-mail address of the Contact person
    iv. Proof of Experience/Technical Knowledge/Qualifications
    v. List of corporate clients.
d. All signed copy documents, brochure, data sheet, technical specification papers and RFQ of mentioned Products have to be provided by the bidder in the Technical Proposal.
e. The bidders must submit required certified engineer CV along with the proposal.
f. All required documents need to be provided as a proof of evidence to fulfill the need of supplier qualification.

1.7 Bid prices

Bidders shall quote the price excluding VAT and including Tax in Bangladeshi Taka (BDT) for the item. Relate VAT to be borne by the bank.

1.8 Bid validity

Bid shall remain valid for a period of **90 days** from the date of opening of technical proposals. In exceptional circumstances, prior to expiry of the original bid validity period, the Bank may request the bidder to extend the period of validity for a specified additional period. The request and the responses thereto shall be made in writing. A bidder agreeing to the request will not be permitted to modify its bid.

1.9 Sealing and marking of bid

The envelope shall:

1. Be addressed to the Bank at the following address: **Head of General Services Division, Bengal Commercial Bank Ltd., Khandker Tower, Level-5, 94, Gulshan Avenue, Gulshan, Dhaka-1212.**
2. Bidder(s) should submit the financial and technical offer in separate envelope mentioning the name of the offer products and both envelopes must be submitted together in a single envelope.
3. In addition to the above requirements, the envelope shall indicate the name and address of the bidder to enable the bid to be returned unopened in case may be declared "late" pursuant to clause 1.11.
4. If the envelope is not sealed and marked as above, the Bank will assume no responsibility for the misplacement or premature opening of the bid.

1.10 Deadline of bid

The bidder must submit the bids in original (sealed), duly marking the envelope as addressed at the following no later than **3:00 p.m. on October 13, 2024**.

1.11 Late Bids

Any bid received by the Bank after the deadline for submission of bid prescribed in clause 1.10 may be rejected and returned unopened to the bidder.

1.12 Evaluation of proposals

The Bank will choose the offer that will be more comprehensive and that conform the relevant required assessment. Information relating to the examination, clarification, evaluation and comparison of bids and recommendations for the award of a contract shall not be disclosed to bidders or any persons not officially concerned with such process until the award to the successful bidder has been announced.

1.13 Award of Contract

Subject to Clause 1.12, the Bank will award the Contract to the successful bidder.

1.14 Bank's right to accept any bid and to reject any or all bids

Notwithstanding Clause 1.13, the Bank reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action.

1.15 Notification of Award/Work Order

Prior to expiration of the period of bid validity prescribed by the Bank and after successful negotiations (if any), the Bank will notify/issue work order in favor of the successful bidder that his bid has been accepted. The notification of award/work order may constitute the updated terms and conditions and basic formation of the Contract.

1.16 Product Delivery

The successful bidder must complete the assessment project within **30 days after receiving the Work Order / Notification of Awards.**

1.17 Penalty

In case of failure or any kind of delay regarding delivery of the product within due time mentioned in clause 1.14, vendor will be liable to pay 2% of the total work order value, as penalty, to the bank for delaying each week after the due date. Upon reaching the penalty to 10% of total Work Order/Contract value, the performance security as well as the Work Order may be forfeited on sending a letter to the vendor.

However, Bank must be informed for any foreseeable delay due to uncontrolled situation prior to exceed the delivery deadline mentioned in clause 1.16 which may be considered by the bank if situation justify such delay and the decision of purchase committee of the bank will be final.

1.18 Payment

Payment will be made after successfully complete the assessment as well as get accepted from SWIFT.

1.19 Withholding Sales Tax

The bidder is hereby informed that the bank shall deduct Tax at the rate prescribed under the Tax Laws of Bangladesh, from all payments for services rendered by any bidder who signs a contract with the Bank. The bidder will be responsible for all Taxes on transactions and/or income, which may be levied by the bank. If bidder is exempted from any specific VAT & Taxes, then it is requested to provide the relevant documents with the proposal.

1.20 Contact Person(s)

For any query regarding proposal please communicate with following officials:

For technical proposal related queries

Mr. Khandaker Abul Hasnat
International Division
Mob. 01975019437
e-mail: abul.hasnat@bgcb.com.bd

For financial proposal related queries

Mr. Golam Mostafizur Rahman
General Services Division
Mob. 01717768454
e-mail: mostafizur.rahman@bgcb.com.bd

Thanking You.

Kamrul Ahmed Ovi	**Md. Monzur-A-Moula**	**Dr. Md Rafiqul Islam**
AVP, International Division	Head of General Services Division	DMD & CTO

Annexure-A

TECHNICAL & FUNCTIONAL SPECIFICATION OF THE SYSTEM

Business & Functional Performance Requirements of the System

The Firm needs to demonstrate that the Online Real Time Remittance Management Software (RMS) meets all business & functional performance requirements as set forth by BGCB. These business & functional requirements are generally included but not limited to:

RESPONSE GUIDELINES

The bidder is requested to address all requirements given in the request for proposal. With the requirements given in the table form:

SL	Requirement	Description	Compliance/Non-Compliance/Require Modification/3rd Party Software
0x.x	Requirement name	Description information of the requirement	The bidder's response here

The bidder is requested to describe how the proposed RMS meets the requirements of BGCB and submit supporting documents as a proof:

Key Word	Respond Criteria	Description
CO	Compliance	Indicates that desired criteria / functionality is fully met in the proposed solution
NC	Non-compliance	Indicates that desired criteria / functionality cannot be made available in the proposed solution
CR	Customization Required	Indicates that the desired criteria / functionality is available by customization in the proposed solution
TP	3rd Party Software	Indicates that desired criteria / functionality is available with a 3rd Party Solution

Remarks: **Bidders may explain how they propose to provide the desired functionality / meet the criteria in an additional page at the last of this page.**

Technical Assessment Requirements:

Mandatory and Advisory Security Controls	Control Objective	Vendor response
1. Restrict Internet Access and Protect Critical Systems from general IT Environment.		
1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	
1.2 Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator level operating system accounts	
1.3 Virtualization or cloud Platform Protection	Secure virtualization platform and virtual machines (VM's) hosting SWIFT related to the same levels as physical systems.	

1.4 Restriction of Internet Access	Restrict Internet access from operator PCs and other system within the secure zone.	
1.5 Customer Environment Protection		
2. **Reduce Attack Surface and Vulnerabilities**		
2.1 Internal Data Flow Security	Ensure the confidentiality, integrity, and authenticity of application data flows between local SWIFT related applications.	
2.2 Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updated, and applying timely security updates aligned to the assessed risk.	
2.3 System Hardening	Reduce the cyber-attack surface of SWIFT related components by performing system hardening.	
2.4A Back-Office Data Flow Security	Ensure the confidentiality, integrity, and mutual authenticity of data flows between SWIFT infrastructure components and the back office first hop they connect to.	
2.5A External Transmission Data Protection	Protect the confidentiality of SWIFT related data transmitted or stored outside of the source zone as part of operational processes	
2.6 Operator session confidentiality and Integrity	Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.	
2.7 Vulnerability Scanning	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon	
2.8 Outsourced critical data activity protection	Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	
2.9 Transaction Business Controls	Restrict transaction activity within the expected bounds of normal business.	
2.10 Application Hardening	Reduce the attack surface of SWIFT related components by performing application hardening on the SWIFT certified messaging and communication interfaces and related applications.	
2.11A RMA Business Controls	Restrict transaction activity to validate and approve business counterparties	
3. Physically Secure the Environment		
3.1 Physical Security	Prevent unauthorized physical access to sensitive equipment, workplace environments, hosting sites, and storage.	
4. Prevent Compromise of Credentials		
4.1 Password Policy	Ensure password are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.	
4.2 Multi-Factor Authentication	Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.	

5. Manage Identities and Segregation of Privileges		
5.1 Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts	
5.2 Token Management	Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used)	
5.3A Staff screening process	Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting in line with applicable local laws and regulations	
5.4 Password repository protection	Protect physically and logically repository of recorded passwords.	
6 Detect Anomalous Activity to Systems or Transaction Records		
6.1 Malware Protection	Ensure the local SWIFT infrastructure is protected against malware.	
6.2 Software Integrity	Ensure the software integrity of the SWIFT related applications.	
6.3 Database Integrity	Ensure the integrity of the database records for the SWIFT messaging interface.	
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	
6.5A Intrusion Detection	Detect and prevent anomalous network activity into and within the local SWIFT environment.	
7. Plan for Incident Response and Information Sharing		
7.1 Cyber Incident Response Planning	Ensure a consistent and effective approach for the management of cyber incidents.	
7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.	
7.3 A Penetration Testing	Validating the operational security configuration and identify security gaps by performing penetration testing.	
7.4 A Scenario Risk Assessment	Evaluate the risk and readiness of the organization based on plausible cyber-attack scenarios.	

Annexure-B

Format for Financial Offer:

SL	Product Description	Qty	Unit price excluding VAT & including Tax	Total price excluding VAT & including Tax
1	**Conducting SWIFT (Society for Worldwide Interbank Financial Telecommunication) CSP (Customer Security Program) Assessment 2024 for Bengal Commercial Bank Ltd.**	1 lot		
Total price excluding VAT & including Tax				

Note:

1. All prices are excluding VAT & including AIT. Related VAT to be borne by the Bank.
2. Modification of the financial offer format is not acceptable.