Ref. Date: MMBL/HO/CSD/RFQ/2023/07/032 Dated: 16/07/2023

Subject: **RFQ (Request for Quotation) for ISO/IEC 27001:2022 (ISMS) Gap Analysis, Remediation of Gaps, Implementation and Certification for Modhumoti Bank**

1. Preface

- Modhumoti Bank Limited hereinafter called "**MMBL**" or "the Bank" issues this Request for Quotation (RFQ) **for Gap Analysis, Remediation of Gaps, Implementation and Certification of ISO/IEC 27001:2022 (ISMS) for Modhumoti bank Limited.**
- Through this RFQ, MMBL invites bidders to propose a contractual arrangement to **provide consultancy to find gaps, assist implementation of ISO/IEC controls and award compliance certificate of ISO/IEC 27001:2022 (ISMS) for Modhumoti Bank Limited.**
- This RFQ consists **of two** groups of products and services. Groups are:
  - **a. Gap Assessment, Documentation, Remediation**
  - **b. Audit and Certification of ISO/IEC 27001:2022 (ISMS)**
- This RFQ is not an offer by the Bank, but an invitation to receive bidder response. No contractual obligation whatsoever shall arise from the RFQ process unless and until a formal contract is signed and executed by duly authorized officers of MMBL and the Bidder.
- The RFQ document can be collected from the address printed in the top sheet of this RFQ document.
- The decision of the Bank would be final and binding on all the bidders to this document. MMBL reserves the right to accept or reject in part or full any or all the offers without assigning any reasons whatsoever.

2. Background

- **Modhumoti Bank Limited** is a private limited commercial bank in Bangladesh. Modhumoti Bank Limited was established on 19 September, 2013. MMBL stands to give the most innovative and affordable banking products to Bangladesh. In 2018, Modhumoti Bank Limited announced plans to focus on becoming a bank for Small Middle Enterprise in rural areas. MMBL is proud to be associated with helping Bangladesh as well as being a leader in the country's banking sector.
- MMBL now has 48 Branches & 47 ATMs all over the country.
- The Bank has currently one data center in Bangladesh located at Khandker tower (Level-7), 94 Gulshan Avenue, Dhaka-1212 which are running in active-active mode and a cold Disaster Recovery Site (DRS) at Uttara. MMBL operates core banking system across its Head Office, Branches, Fast Tracks, Mobile Banking Office etc.
- The Bank provides a wide range of financial products and services spanning deposits, loans, trade finance and money market as well as facilitating financial transactions of customers. It is a primary member of VISA card issuer and acquirer of Credit and Debit cards. It offers Automated Teller Machine (ATM).The Bank also offers payment services through Go SMART app.
- The Bank has a goal to achieve the Certification of ISO/IEC 27001:2022 (ISMS) as soon as possible. In accordance with that, the Bank will find out the gaps against ISO/IEC 27001:2022(ISMS) requirements in the first step. Also the Bank will work to rectify those gaps for achieving the certificates. The Bank is seeking a prime bidder to provide a cost-effective solution for gap assessment and remediation of those gaps for implementing Information Security Controls aligned with ISO/IEC 27001:2022 with a view of extending secure and uninterrupted services to its customers.
- The bidder will also make partnership with an accreditation body which will be responsible for performing ISO/IEC related audits and awarding certification.

3. Scope of Work

3.1 ISO/IEC 27001:2013 Certification Scope

SL.	Item	Details
1.	Data Centers	Khandker Tower (Level-7), 94 Gulshan Avenue, Dhaka, Data Center.
2.	Divisions	ICT Division

3.2 Process approach for ISO/IEC 27001:2022 design and implementation

The process approach should cover:

a) Understanding Bank's information security requirements and the need to establish policy and objectives for information security.
b) Implementing and operating controls to manage an organization's information security risks in the context of the Bank's overall business risks as per ISO/IEC 27001:2022 standard.
c) Monitoring and reviewing the performance and effectiveness of the ISMS
d) Continual improvement based on objective measurement.

3.3 Review of Risk Assessment Process Approach and Methodology

The Bidder has to conduct the detailed review of existing Risk Assessment (RA) across all business functions and processes covered under the scope and prepare and present the RA report to the MMBL management/officials. Under this, the following key steps have to be outlined:

a) Assess and evaluate risks
b) Select, implement and operate controls to treat risks
c) Monitor & review risks
d) Maintain and improve risk controls

This exercise should include the steps outlined below:

- Inventory and classification
- Identify legal and business requirements relevant to the assets
- Valuation of identified assets taking requirements into account as well as impacts of loss of C.I.A.
- Identify threats and vulnerabilities
- Assessment of likelihood threats will result in vulnerabilities getting exploited & calculation of risk
- Evaluate risks against a pre-defined risk scale

3.4 ISMS Development Activities Details

The role of the Bidder for this services process includes the following broad areas and not limited to:

a) Control objectives and control under all domains/clauses as specified in the ISO/IEC 27001 Standard
b) The bidder has to ensure that all these are properly checked, documented and complied.
c) Gap analysis of the Bank against the ISO/IEC 27001 ISMS Standard requirements.
d) Training and awareness of key stakeholders with respect to ISO/IEC 27001:2022 standard.
e) Define the scope: what's in, what are out, including issues like location, assets and so on. Prepare a Statement of Applicability (SOA) document.
f) Compilation of Information Assets Inventories.
g) Risk Assessment- Information Assets.
h) Security Baselining of all IT assets and ensuring implementation of Security Baseline.
i) Create an Information Security Manual (ISMS) and framework.
j) Implement the plan, prepare, review, approve and publish information security policies, procedures, standards and so forth. Identify controls to protecting the IT infrastructure and facilities. Review and improve application security controls as well. Prepare contingency plan and plan its periodic drill.
k) Training and Certification for Bank's five (5) selected personnel for maintenance and improvement of ISO/IEC 27001 Standard by ISO/IEC 27001 Lead Auditor.
l) Only training for Bank's five (5) selected personnel for maintenance and improvement of ISO/IEC 27001 Standard by ISO/IEC 27001 Lead Implementer.
m) Pre-certification internal audit and preparation for the final certification audit.
n) Perform stage -1 and stage -2 audit along with management review to check that everything is in order.
o) Engaging and coordinating with accredited certification bodies.
p) Undergo the formal certification/re-certification assessment of the ISMS by an accredited certification body.
q) Certification.

Note:

If any changes/improvements in ISO/IEC 27001:2022 or any new standards are announced during the project time, and they need to be implemented for certification process, the same needs to be incorporated without any additional cost.

3.5 Statement of Applicability - Approach and Completion

Prepare a Statement of Applicability in consultation with the Bank's officials incorporating changes required due to change in environment/ other factors.

Prepare a statement of exclusion of any control objectives and controls in SOA with the justification for their exclusion.

3.6 Pre-audit Assessment Process Plan and Execution

A pre-audit assessment shall comprise the following three modules, as given below:

a) Gap Analysis – to find gaps between the existing ISMS system and the system required for successful ISO/IEC 27001 ISMS certification.
b) Documentation Audit- to verify documentation compliance against the requirements of the ISO/IEC 27001 standard.
c) Pre-audit by the bidder- to have surety over the established ISMS system before engaging the certification agency for the final certification auditing.

A detailed Assessment and Maturity report to be presented, detailing the information per the selected module and clause. A pre-audit assessment exercise comprises of assessing the maturity of the following:

- ISMS Audit
- Assets Audit
- Business Process Audit
- Security Architecture Audit
- Policies Audit
- Procedures and Systems Audit
- Compliance Report

3.7 Certification Audit Stage Plans & Surveillance Audit Plans

Under this, vendors approach towards obtaining certification to the scope defined and appointment of consultant for ISO/IEC 27001 Certification of Data Center and IT services coordination with MMBL has to be emphasized. The bidder shall:

a) Establish ISMS in line with ISO/IEC 27001:2022 standard
b) Coordinates with MMBL
c) Apply for Certification
d) Plan Pre-Audit visit after document review offsite.
e) Certification Audit On-Site
f) Obtain Certificate
g) For surveillance audit, there should be onsite audit for at least one week. If pandemic situation does not allow onsite audit, MMBL may allow remote audit for the subsequent years.

3.8 Knowledge Transfer & Training for ISO/IEC 27001:2022

The selected Bidder will ensure knowledge transfer to the Bank at every stage of the project to enable the Bank to carry out the work as specified in this RFQ in future after completion of this assignment.

The bidder will also arrange training for ten (10) officials of the Bank on ISMS – Lead Auditor and ISMS – Lead Implementer. The training should be from accredited organizations / authorized training provider.

3.9 Deliverables by Accreditation Body

i. Training and Certification ISO/IEC 27001:2022 Lead Auditor for 5 (five) Officials
ii. Only training for ISO/IEC 27001:2022 Lead Implementer for 5 (five) Officials
iii. Stage 1, Stage 2 and Surveillance Audit and Final Certificate
iv. Inter Auditor training 3 (three) days

3.10 Deliverables by Remediation Partner

i. Gap assessment
ii. Workshop for management and stakeholders
iii. Plan, Policies, Procedures and Processes
iv. Templates and Frameworks
v. Asset Inventory
vi. Check List (daily, weekly, monthly, quarterly, half-yearly, yearly)
vii. Risk assessment framework (including risk appetite and risk tolerance)
viii. Risk assessment report, asset and risk register(s), key risk indicator, risk treatment plan
ix. Documentation Prepare

x. Business Continuity Plan
xi. Mock Audit
xii. Remediation of findings for gap assessment, internal audit, mock audit and stage 1 & 2 audit as well as second and third year surveillance audit
xiii. Recommendation for continuous improvement
xiv. Maturity assessment report
xv. Security Roadmap

Note:
If any additional document or effort is required in ISO/IEC 27001:2022, the same needs to be incorporated without any additional cost.

4. Milestones

Phase	Details and Milestones	Activities	Bidders Response
Phase 1	Current State Study, Statement of Applicability and Asset Compilation.	• Awareness training to IT officials on ISO/IEC 27001 standard. • Define the scope: what's in, what are out, including issues like location, assets and so on. Prepare a Statement of Applicability (SOA) document. • Compilation of Information Asset Inventory.	
Phase 2	Gap Analysis, Documentation, Security Base-lining and Risk Assessment and Treatment, Training	• ISO/IEC Lead Implementer Training and Certification • ISO/IEC Lead Auditor Training and Certification • Review of IT security policy & procedure document with respect to ISO/IEC 27001 Standard and Gap analysis. • Security Baseline of IT assets, systems. • Risk Assessment. • Risk Treatment Plan. • Information Security Manual and Framework. • Prepare contingency plan and plan its periodic drill.	
Phase 3	Implémentation, pre-certification audits, preparation for final audit and maintenance training	• Three (03) Awareness Workshop (Senior Management - 1, Stakeholders - 2) • Pre-certification mock audit and internal audit and preparation for the final certification process. • Perform and information security audit (stage 1 audit) and management review to check that everything is in order.	
Phase 4	Certification	• Stage 2 audit • Certification	
Phase 5	Second year surveillance audit	• Mock audit • Remediation • Workshop for stakeholders • Surveillance audit	
Phase 6	Third year surveillance audit	• Mock audit • Remediation • Workshop for stakeholders • Surveillance audit	

5. Experience

5.1 The Firm responding to this RFQ shall demonstrate their capabilities and experience in providing similar services and similar engagements especially in the financial sector. These services and engagements must be performed by the Firm during the last seven (7) years (minimum 3 similar successfully accomplished projects are required). Furthermore, the Firm shall demonstrate the following specific capabilities:

- Experience in designing, developing, implementing, and successful certification assistance in ISO/IEC 27001:2022.
- Experience in conducting full ISO/IEC 27001:2022 internal audits.
- More than 7 years in the field of information security, governance, risk and compliance in the region of operation.

5.2 Bidder should have Cyber-Security Insurance Coverage in Bangladesh. Relevant evidence should be submitted.

5.3 The Firm should have minimum four (4) resource personnel each with more than five (5) years' experience in ISO 27001:2022 implementation and internal auditing. The bidder should have Certified Professional in their team (HR Declaration and Resource Profiles are to be attached as evidence).

- Minimum 01 (one) nos. of experienced resources with CISSP
- Minimum 02 (Two) nos. of experienced resources with CISA
- Minimum 01 (one) nos. of experienced resources with PCI QSA
- Minimum 10 (Ten) nos. of experienced resources with ISO 27001 Lead Auditor
- Minimum 05 (five) nos. of experienced resources with ISO 27001 Lead Implementor.

5.4 Reference Site

The Bidder should have more than 7 years of experience in Cyber Security and similar kind of work experience in relevant field. He/she shall have CISSP valid certification along with IS0 27001 Lead Auditor / PCI QSA valid certification. List of major customers in last 7 years and their references:

SL. No.	Name and complete address of the customer	Name, designation, telephone, fax, e-mail address of the contact person	Brief scope of work (project summary) Bidder can attach separate paper if required.	Attach reference letter
1				
2				

(Enclose necessary documentary proof)

I/we solemnly declare that the statements made above are correct. I/We agree that any misstatement made by us, if detected later on, shall render our application unacceptable to the Bank.

_____

(Signature)
(Name & designation of Authorized Signatory)
(Name & Address of the Bidder with Seal)

6. Roll out Plan

Stages	Particular	Period (in week)
Step 1	Commencement of assessment work after placing of Work Order / Notification of Award (NOA)	1
Step 2	Submission of required processes/ policies/ plans/ procedures/ templates and methodology as per scope of work	1
Step 3	ISO 27001 Lead Auditor Training and Certification and Implementer only Training	2
Step 4	Gap Assessment (Stage 1 and Stage2) and presentation of executive and detail report	4
Step 5	Three Awareness Workshop (Senior Management - 1, Stakeholders - 2)	1
Step 6	Remediation based on Gap Assessment	8
Step 7	Internal Audit	1
Step 8	Remediation of Internal Audit findings	2
Step 9	Mock Audit, Stage -1 Audit, Remediation of Stage -1 Audit findings, Workshop for preparing Stage -2 Audit	2

Step 10	Stage -2 Audit	1
Step 11	Receive Certificate	2
Step 12	2nd year Mock Audit and remediation	2
Step 13	2nd year officials' lead auditor training, workshop for stakeholders and surveillance audit.	2
Step 14	3rd year mock audit and remediation	2
Step 15	3rd year officials' lead auditor training, workshop for stakeholders and surveillance audit.	2

1st year	25 weeks / 6 Months + Grace period of four (04) weeks = 31 weeks / 7 Months
2nd year	4 weeks
3rd year	4 weeks

7. Quotation Submission Requirements –Sequential Order

7.1 Technical Quotation – Format and Contents:

The bidder shall, at a minimum, address the following points in the Quotation.

i. Table of Contents: The Table of Contents must include all items listed in this section.

ii. Executive Summary: The Executive Summary will condense and highlight the contents of the technical Quotation in such a way as to provide the Bank with a broad understanding of the Bidder's qualifications and approach to meeting the requirements of the RFQ.

iii. Bidder's Background and Experience: Company Overview – the Bidder must include a company summary including company history, office location(s), company size, audited financial statements, and statement of technical areas of expertise. The Bidder must be able to substantiate to the satisfaction of the OFFICE OF COMMON SERVICE DIVISION that the Bidder has sufficient resources to complete the project successfully within the time requirements.

iv. Résumés: The Bidder must include brief résumés for personnel that will be working on the project, if awarded the contract. Proven work experience combined with related education will be means of substantiating expertise.

v. Single Point of Contact: The Bidder must identify a single point of contact for all contract management activities. The Bidder's Project Manager's name and resume must be submitted with the Quotation. The successful Bidder must not change the Project Manager without written / email Bank approval.

vi. Bidder's Project Work Plan: The Bidder must submit a work plan that meets the needs of the RFQ and indicates a thorough understanding of the scope of the work. The Bidder must identify realistic person hours of effort and responsibilities for the deliverable and each work activity in a Gantt Chart format.

vii. Project Management Plan: The Quotation must contain a comprehensive and practical description of the Bidder's plans for project management and control mechanisms, including staff organizational structure, progress reporting, major decision-making, sign-off procedures, and internal control procedures. The Bidder must also indicate flexibility in meeting changes in program requirements and coping with problems.

viii. Project Delays: The Bidder must also describe how project delays will be addressed should they occur. This should include assurances that sufficient resources and knowledgeable, experienced staff are available to meet any the project schedule.

ix. Contract Exceptions: The Bidder must state agreement with all General Provisions. Bidder must furnish any exceptions to the provisions included in the Contract Terms and Conditions be noted in the Executive Summary. Identifying exceptions to the Contract Terms and Conditions does not bind the Bank in any way to accept such changes, but only ensures that discussion and resolution of their acceptance may be deferred until after tentative award is made.

x. Staffing and Project Organization: An Organization Chart must be included with all proposed personnel, including the supervisor level, functional responsibilities, key personnel, and other staff members who will be involved in the project.

xi. Bidder Checklist: The bidder shall submit a checklist in which the bidder shall evaluate their existing offering compared with the RFQ mandatory and optional requirements.

7.2 Financial Quotation - Format and Content: Hard Copy.

8. Evaluation Methodology

8.1 Evaluation Committees:

The Bank will conduct a comprehensive, fair, and impartial evaluation of Quotations received in response to this RFQ. Quotations will be evaluated by the Technical Committee. The Technical Committee is made up of members representing the project subject expertise. The Technical Committee will review and score (if needed) all Quotations and will make the final recommendation to the Purchase Committee.

The Competent authority of the Bank will receive recommendations from the purchase committee and make the final decision.

8.2 Compliance with Mandatory Requirements:

To be considered responsive, a submitted Quotation must meet the minimum and mandatory requirements defined in this RFQ. The minimum requirements are intended to ensure that evaluation of the Technical Quotation can proceed and that the bidder agrees to perform all responsibilities within the RFQ and the Contract Terms and Conditions.

8.3 Technical Scoring and Ranking:

Approach to Contract Performance: The Contractor must describe its:

a) Approach to meeting the mandatory requirements and specifications, as described in the RFQ.
b) Approach in addressing the goals and objectives specified in this RFQ.
c) Approach to a comprehensive and practical plan for project management and control mechanisms, including progress reporting, major decision-making, sign-off procedures and internal control procedures.
d) Approach to how project delays will be addressed, should they occur.
e) Contains assurances that sufficient resources and knowledgeable or experienced staff are available to meet delays.
f) Approach to contract responsibilities.
g) Approach to resolving disputes or disagreements in contract or work requirements.
h) Approach to meeting deliverables and milestone deadlines.
i) Approach to change orders or modifications to work in progress.
j) Oral Presentations, if required. The Evaluation Team will determine, after receipt of the Written / email Quotations, whether selected bidders will be requested to make any oral presentation based on their Quotation. However, the Evaluation Team reserves the right to make an award without requesting an Oral Presentation from any bidder. All oral presentation costs will be the responsibility of the bidder.

8.4 Financial Scoring and Ranking:

Financial Analysis (Financial Quotation shall be under separate cover): The cost will be presented as key deliverables in the form of a project total.

8.5 Final Rankings of Quotations:

The Bank will be the sole authority with respect to the evaluation of Quotations. The firm which best meets the conditions of each of the individual criterion will be awarded the highest preference for that specific criterion. Quotations that provide a complete solution meeting all mandatory requirements and include optional items will be given preference during evaluations. The balance of the Bidders will be rated based on their evaluated preference.

The Bank reserves the right to accept an entire Quotation, a partial Quotation, a single component of a Quotation, or no Quotation at all.

9. Quotation Price Sheet and Signature Page

Financial Statement
(To be submitted on the pad of the bidder)

The undersigned agrees to provide ISO/IEC 27001:2022 (ISMS) Gap Analysis, Remediation of Gaps, Implementation and Certification service to the Modhumoti Bank Limited in accordance with the Request for Quotation, General Provisions, General Terms and Conditions, Special Provisions Information and Financial Offer (Quotation Price Sheet) included with this RFQ.

By Submission of a Quotation, The Bidder Certifies:

9.1 Prices in this Quotation have been arrived at independently, without consultation, communication, or agreement for the purpose of restricting competition.
9.2 No attempt has been made nor will be by the bidder to induce any other person or firm to submit a Quotation for the purpose of restricting competition.

9.3 The person signing this Quotation certifies that he/she is authorized to represent the company and is legally responsible for the decision as to the price and supporting documentation provided as a result of this advertisement.

9.4 Bidder will comply with all government / regulatory requirements, policies, and guidelines.

9.5 Prices in this Quotation have not been knowingly disclosed by the bidder and will not be prior to award to any other bidder.

SL.	Description of Item	Amount in BDT.
Phase: 1	ISO/IEC 27001:2022 (ISMS) Gap Analysis, Remediation of Gaps and Implementation of ISMS for Modhumoti Bank under the scope of this document	
Phase: 2	ISO/IEC 27001:2022 (ISMS) Stage 1 & Stage 2 audit with final certification and surveillance	
Phase: 3	Surveillance Audit for second (2nd) and	
Phase: 4	Surveillance Audit for third (3rd) year	

GENERAL INFORMATION:

Bidder Name: _____

Phone: _____ **Fax:** _____

Mailing Address_____

City: _____ **Division:** _____ **Zip:** _____

Tax Identification Number _____

OWNERSHIP AND CONTROL:

Bidder's Legal Structure:

_____ **Sole Proprietorship** _____ **General**
_____ **Partnership** _____ **Corporation**
_____ **Limited Partnership** _____ **Limited Liability**
_____ **Other** _____

If Bidder is a sole proprietorship, list:

Bidder Name_____

Phone: _____ **Fax:** _____

Mailing Address: _____

City: _____ **Division:** _____ **Zip:** _____

Tax Identification Number _____

Beginning date as owner of sole proprietorship_____

Provide the names of all individuals authorized to sign for the Bidder:

NAME (printed or typed)	**TITLE**
_____	_____
_____	_____
_____	_____
_____	_____

VERIFICATION

I certify under penalty of perjury, that I am a responsible official (as identified above) for the business entity described above as Bidder, that I have personally examined and am familiar with the information submitted in this disclosure and all attachments and that the information is true, accurate and complete. I am aware that there are significant penalties for submitting false information, including criminal sanctions which can lead to imposition of a fine.

_____ _____

(Seal & Signature) (Date)