Common Services Division
Corporate Head Office, Dhaka

May 05, 2025

Request for Quotation (RFQ): Information Security Management System (ISMS) – ISO 27001:2022(Latest Version) End to End Certification Consultancy for Preparation, Implementation and Accreditation Service for the Bank.

Scope of bid

Bank requires "Information Security Management System (ISMS) – ISO 27001:2022 (Latest Version) End to End Certification Consultancy for Preparation, Implementation and Accreditation Service" under the following terms and conditions and technical specifications (Annexure-A of the RFQ) for the required items are given hereunder for the bidders/vendors.

1.1 Bidder's qualification

a) A well-recognized audit and legal consultancy firm with experience in building information security policy frameworks, or a company focusing on Audit GRC and Cyber Security with at least two years of similar experience, is required. The Consulting Firm should be a company focusing on Audit GRC and Cyber Security business with a minimum of 02 year's similar experience.
b) The Consulting Firm must: have a registered office in Bangladesh for at least 2 years; possesses CQI | IRCA Certified ISO 27001 Lead Auditors and Implementers, along with Project Management and Governance professionals; has at least one successful ISO 27001 certification project in a Bangladeshi Bank or NBFI; and has the legal capacity to contract under Bangladeshi law.
c) Certification must be completed within 3 months of receiving work order and surveillance I and surveillance II shall be completed on time.
d) Certificate Body engaged by the Consulting Firm shall be the member of IAF and they also have the experience to audit ISO 27001 in the banking or NBFI domain in Bangladesh.
e) Consulting Firm shall not be permitted to do joint venture with other Consulting Firm.
f) Consulting Firm shall ensure necessary audits by Certificate Body if needed by the bank with free of cost during the Certification and two Surveillances audit tenors.

1.2 Documents comprising the bid

a) Name of Company.
b) Contact Person(s):
c) Submission of supporting documents (e.g. Consultancy, Implementation and Certification experience in ISO27001 project) is mandatory.
d) Telephone (including land phone number), Fax, e-mail
e) Constitution and year of establishment (certificate of incorporation)
f) Registered Office/Corporate Office/Mailing Address
g) Names & Addresses of the Partners if applicable
h) Name, designation, qualifications and experience of the technical and management personnel to be engaged with this project
i) Trade License;
j) E-TIN, VAT and BIN Certificate
k) Letter of GIR/TIN Certificate;
l) Letter of Income Tax certificate and VAT registration certificate;
m) Other licenses/certificates as may be applicable;
n) List of deliverables with detailed timeline;
o) The number of Security Assessors who would be involved in the information security assessment, mock audit, and remediation processes, also a brief description of them comprising names, valid bidder certificates, academic and professional experience.
p) The number of ISO 27001:2022 (Latest Version) Lead Auditor from Certificate Body who would be involved in the stage 1, stage 2 and surveillance audits, also a brief description of them comprising names, valid bidder certificates, academic and professional experience.
q) The number of employees, certified auditor, certified security expert, Licensed Penetration Tester, etc. in the company.
r) Any other related information, not mentioned above, which the Certificate Body wishes to furnish.

1.3 Bid prices

Bidders shall quote the price **excluding VAT and including Tax (VAT to be borne by the Bank)** in Bangladeshi Taka (BDT) for the service. Quoted rates (figures and words) and total costs in BDT must match the Bill of Materials. The Bank won't cover additional items not in the Bill of Materials. The Consulting Firm must provide rate analysis if requested. In case of discrepancies between figures and words, the lower amount prevails. If there are calculation errors between the quoted rate and amount, the quoted rate is valid, and the Bank will correct the total. The Consulting Firm must specify the costs for the 1st and 2nd surveillance audits.

1.4 Bid validity

Bid shall remain valid for a period of **120** 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.

1.5 Bid Security / Earnest Money

The bidder shall submit 2.5 % of their bid price in the form of Payment Order/Bank Guarantee as bid security in favor of Shahjalal Islami Bank PLC. The Bid Security/ Earnest Money should be enclosed on the top of the financial offer. Any bid not accompanied by an acceptable bid security shall be rejected as non-responsive. The bid security of unsuccessful bidders will be returned within 120 days from the date of bid opening. Selected bidder will get back the Bid Security/ earnest money on submission of performance security.

The bid security may be forfeited if

(a) The bidder withdraws its bid during the period of bid validity.
(b) A successful bidder fails to sign the contract.
(c) A successful bidder fails to furnish the performance security

1.6 Sealing and marking of bid

The envelope shall:

a) Be addressed to the Bank at the following address: **The Member Secretary, Procurement Committee, Shahjalal Islami Bank PLC, Croporate Head Office, Shahjalal Islami Bank Tower, 2nd floor, plot#4, Block- CWN(C), Gulshan Avenue, Dhaka-1212.**
b) Bidder(s) should submit the financial and technical offer in separate envelope mentioning the name of the offer and both envelopes must be submitted together in a single envelope.
c) 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 1.8.
d) 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.

1.7 Deadline of bid

The bidder must submit the bids in original (sealed), duly marking the envelope as addressed at the following no later than **5:00 p.m. on Monday, 12th May, 2025.**

1.8 Late Bids

Any bid received by the Bank after the deadline may be rejected and returned unopened to the bidder.

1.9 Evaluation of proposals

The Bank will choose the offer that is more comprehensive and that conforms to the relevant required service. The Bank will carry out technical as well as financial evaluations according to the criteria of the bank. The Bank will give emphasis to quality and the richness of the product, as well as the experience of the vendor while evaluating.

1.10 Price Negotiation
The Bank may request technically qualified bidders to negotiate the price or any other relevant queries. Representatives of the Bidders must have authorization for price negotiation. Bank is in no way bound to notification of award to the contract to the lowest price bidder(s).

1.11 Award of Contract
The Bank will award the Contract to the successful bidder as per clause 1.9 and 1.10.

1.12 Bank's right to accept any bid and to reject any or all bids
Notwithstanding Clause 1.10, 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.

1.13 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.

1.14 Performance Security
The successful bidder will have to provide 5% of the Work Order Value in the form of Pay Order/ Unconditional Bank Guarantee as Performance Security in favor of Shahjalal Islami Bank PLC. The validity of the submitted Performance Security should be extended up to the achievement of ISO 27001 Certification from a Globally Recognized Certification Body subject to acceptance by the Bank.

These clauses maybe added while issuing the Performance Security,

a. *At the request of the supplier, we, (issuing Bank),...(address).... hereby irrevocably undertake to pay you, without cavil or argument, any sum or sums not exceeding in total amount of Taka .....only upon receipt by us of your (Shahjalal Islami Bank PLC) first written demand.*

b. *Any such demand made by Shahjalal Islami Bank PLC on us (issuing Bank) shall be conclusive and binding notwithstanding any difference between you and the supplier or any dispute pending any Court, Tribunal, Arbitrator or any other authority.*

1.15 Penalty
If the successful bidder fails to complete the project in time without any valid reason accepted by SJIBPLC, the successful bidder will be subject to penalty charges of (1%) per week on the work order amount and shall be deducted from the Work Order Value during the payment of the bill.
If certification would not achieve within the project stipulated time without any valid reason accepted by SJIBPLC, 10% of work order/value will be deducted from the successful bidder. Most of the remarkable issues from the Certification Body audit need to be remediated before 1st surveillance audit otherwise no payment will be made for Phase- 4 and all the issues need to be remediated before 2nd surveillance audit otherwise no payment will be made for Phase- 5.
However, Bank must be informed for any foreseeable delay or any other logical justification due to uncontrolled situation prior to exceed the delivery deadline which may be considered by the bank if situation justify such delay and the decision of purchase committee of the bank will be final.

1.16 Payment
a) No advance payment would be made to the successful bidder.
b) Any delay in Stage of completion as per schedule or deliverables will automatically result in a delay and penalty of the corresponding payment as per Clause No. 1.15
c) The schedule of payment calculated as a percentage of the total work order value will be as follows:

Sl.	Phase	Price (BDT) Excluding VAT (VAT to be borne by the bank)	Remarks
A	**Phase-1:** Gap analysis and Mitigation support, Documentation support, Training for the internal team (20 Persons), Lead Auditor (02 Persons) and Lead Implementer (02 Persons) Training with respective certifications & Workshop.	20% of the Work Order Amount	
B	**Phase-2:** Remediation, Risk Assessment, Mock Audit, Stage 1 Audit	50% of the Work Order Amount	
C	**Phase-3:** Stage 1 Non-compliance Remediation, Workshop, Stage 2 Audit, Engage Accredited Certification Body and Certification by Globally Recognized ISO Certification Body		
D	**Phase-4** 1st surveillance audit, Workshop Revalidation Audit by Globally Recognized Certification Body	15% of the Work Order Amount	
E	**Phase-5** 2nd surveillance audit, Workshop and Revalidation Audit by Globally Recognized Certification Body	15% of the Work Order Amount	
	Total	100%	

d) All the phases of 1.16 Table (A-E) must be ensured by the bidder within the same Work Order value and no extra payment will be given other than the mentioned phase-wise payment according to the above table.

e) If the bank fails to achieve ISO 27001 Certification, then the bidder will have to follow Plan-Do-Check-Act for relevant phases until the issue is resolved and then the bidder will have to arrange the ISO 27001 certification audit again by the Certification Body without any additional cost. The process will be followed by the Plan-Do-Check-Act method for relevant phases, Certification and Surveillance Audit without any additional cost until the optimum outcome of the said project.

f) All Change Management situations and additional issues must be addressed and remediated by the bidders without any additional cost during the project.

g) On submission of the bills duly vetted and approved by the Bank or its appointed Consultant after which the payment shall be made by the Bank.

h) Payment against all items will be made as per bill subject to necessary certification by the Bank or its representative(s) after deducting security deposit, AIT, etc. as per terms & conditions of the RFP and NBR rules & regulations whatever applicable under the scope of this document and related VAT to be borne by the bank.

i) All the payment against work done shall be made in Bangladeshi Currency (in Taka) on submission of bill properly approved by the Bank as mentioned in the Schedule of Items and Bill of Quantity under the Financial Propos

1.17 Withholding Sales Tax & VAT:

The bidder is hereby informed that the Government 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 Taxes, then it is requested to provide the relevant documents with the proposal.

1.18 Terms and Conditions

Followings are the Terms & Conditions to be applicable for this tender:'

a) The Consulting Firm's offer shall be filled-in with permanent ink and shall not contain any stipulation, erasures or strike over, corrections or revisions may be made by neatly marking through the figures or words and writing the correction above.
b) No additions, alterations shall be made by the Consulting Firm in the Schedule of Item of Works & Bill of Materials. A separate sheet shall be used for any additional item, which may be required to complete the work. Alteration of tender document may lead to the cancellation of the submitted Proposal by the Tenderer.
c) A Non-Disclosure Agreement (NDA) will be signed between Consulting Firm and Shahjalal Islami Bank PLC. for implementation of the project.
d) The Consulting Firm must sign and seal each and every page of the Proposal if the hard copy is required by the Bank.
e) The Tender Amount shall include Tax, Duties etc. as per applicable rules.
f) The Consulting Firm will be completely responsible for all applicable taxes, duties, levies, charges and license fees in connection with the delivery of products/services at the site.
g) The Consulting Firm must provide the validity for the offered products/service for One hundred twenty (120) calendar days from the date of opening of the financial offer.
h) Shahjalal Islami Bank PLC reserves the right to ask for any modification, amendment, adjustment and/or alteration of the proposal submitted by a participant and in such case, the participant may be required to submit the proposal again.
i) Shahjalal Islami Bank PLC may seek clarification of Technical and/or Financial proposals from the respective participant for proper examination and evaluation of the proposals. The request for clarification by Shahjalal Islami PLC and the response from the participants shall be in writing or bye-mail.
j) Shahjalal Islami Bank PLC at its sole discretion shall have the right to accept or reject any part or entire proposal.
k) Consulting Firm must provide a summarized offer in their proposal which require to be aligned with the tender requirement for the project.
l) Consulting Firm must provide requested information in its proposal mentioned in the tender document and provide their confirmation on the acceptance of requested deliverables. Contact Person

The bidder may contract with below mentioned official(s) for any queries.

For Technical queries:	**For Financial queries:**
Zabedul Hoque Chowdhury ICT Security Department e-mail: zabedul4463@sjiblbd.com Cell: 01814874480	S.M. Tarequl Islam Hyder Common Services Division e-mail: tarequl4471@sjiblbd.com Cell: 01712-480201

Abul Bashar Md. Zafry 5/5/25
SVP & Head of CSD

Zahid Hasan 05/5/25
SVP & Head of ICT Security Department
2HC

Annexure-A

Technical Specification

Of

Information Security Management System (ISMS) – ISO 27001:2022 (Latest Version) End to End Certification Consultancy for Preparation, Implementation and Accreditation Service for the Bank.

TECHNICAL SPECIFICATION OF ISO 27001: 2022(Latest Version), an Information Security Management System (ISMS) Standard for SJIBPLC.

OBJECTIVES OF THE RFP:

The Bank has a goal to achieve the Certification of ISO 27001:2022 (Latest Version) (ISMS). This request for proposal document ('RFP document' or RFP) has been prepared solely for the purpose of enabling SJIBPLC to select Consultant for ISO 27001: 2022(Latest Version) consultancy services to prepare and readiness to obtain ISO 27001: 2022 (Latest Version) Certificate with maintenance and surveillance audit for SJIBPLC Data Centre, DR site and IT Division of the Bank. For this "SJIBPLC" intends to select a reputed bidder /consultancy service provider to engage with the Bank's team in implementing the ISMS and assist the Bank in obtaining certification of ISO 27001:2022 (Latest Version) from an accredited certification body (CB). The Selected bidder /consultancy service provider shall assist the Bank to prepare and create a readiness to obtain the ISO 27001: 2022(Latest Version) Certificate. The selected bidder /consultancy service provider may tie-up with accredited certification bodies (CB) and has to submit an all-inclusive proposal for obtaining ISO 27001: 2022(Latest Version) Certification for the SJIBPLC.

Locations to be covered for End to End Information Security Management System (ISMS) ISO 27001: 2022(Latest Version) Certification for the Banks are:

i. Data Centre, Head Office, Gulshan
ii. Disaster Recovery Site, Gazipur
iii. IT Division, Head Office, Gulshan

SCOPE OF WORK FOR ISMS

Items	Description
Details Scope of Work	a. Conduct ISO27001 gap analysis based on the ISO 27001:2022 (Latest Version) requirements b. Develop Policies, Procedure, Standard, templates & other Documents required for ISMS c. Preparation of Statement of Applicability d. Remediation support to implement controls by proven consultant e. Conduct Risk Assessment f. Support Internal Audit & Management Review Meeting (MRM) g. Certification Audit by a Certification body h. Perform Surveillance Audit i. Awareness Training for 20 personnel j. ISO 27001 Lead Auditor training with certification for 2 personnel. k. ISO 27001 Lead Implementer training with certification for 2 personnel **l.** Any relevant scope/task to achieve ISO 27001 Certification and 2 Surveillance Audit

SCOPING INFORMATION

Items	Description
Scope Statement:	ISO 27001 Certification (ISMS) for IT Division, IT Services, Data Center and Disaster Recovery Site.

2H.C

Number of Location:	02 (Two)
Nature of the Business:	Financial Service (Banking)
Business functions:	Banking: Branch Banking, Teller, Investment, Party, Trade Service, Retail Banking, Internet Banking, Mobile Application, Cards, Remittance, Corporate Payment Module, Utilities Payment, Customer Onboarding System, Agent Banking etc.
Support functions:	HR, IT, Risk Management, Internal Audit, Common Services Division, Banking Operation Division etc.
Current Security Practices and Technology:	Access Control, Network Security, Endpoint Protection, Vulnerability Assessment, Intrusion Prevention, WAF, ISE, Application Security, Secure Configuration, Malware Protection and Content Filtering, etc.
The number of personnel in the company:	3500 +
Number of personnel to be covered by the assessment:	30
The number of personnel involved directly in ensuring the security of information:	6
External interfaces with your network:	BACH, BEFTN, SWIFT, SMS, CMS, Remittance, etc.
Description of business systems in the scope:	Core Banking, Agent Banking, Internet Banking, Mobile Application etc.
Description of the infrastructure encompassed in the scope:	Data Center and Disaster Recovery Infrastructure as well as IT Division responsible to provide services like Core Banking (includes 141 branches and 05 sub-branches), Agent Banking, 143 ATM terminals, Internet Banking, Internet Service, Mobile Applications, Remittance Service, Utility Payments etc.
Security framework currently following:	ISMS
Adoption of cloud-based service:	None

STATEMENT OF WORK (SOW)

i. Project implementation

The project shall be implemented by the following 05 (Five) phases:

Sl No	Phase/Stage	Assignment
01	Phase 1	Scoping, Planning and Gap Assessment
02	Phase 2	ISMS Preparation, Implementation and Operation
03	Phase 3	Certification
04	Phase 4	1st Surveillance Audit
05	Phase 5	2nd Surveillance Audit

Phase 1: (Scoping, Planning and Gap Assessment)

Activities (key): Consulting Firm

1. Project Kick-off and discuss the project approach, timing.
2. Establish project governance, project plans, roadmap and team
3. Understand SJIBPLC's Strategy & Governance structure
4. Understand SJIBPLC's Business, IT Service, IT Systems, Infrastructure and operations

2.H.C

5. Review existing ISMS responsibilities, IT Policies, procedures and guidelines etc. used in Shahjalal Islami Bank PLC.
6. Identify internal departments and external parties involved within Shahjalal Islami Bank PLC
7. Understand the organization, its departments, and processes
8. Physical and Logical boundaries for the scope
9. Identify legal requirements for information security for the organization
10. Conduct ISO27001 gap analysis based on the ISO 27001-2022(Latest Version) requirements
11. Understand IT landscape
12. Identification and classification of information assets and value assets based on CIA.
13. Develop an asset register and evaluate assets based on asset classification guidelines
14. Develop risk register and perform risk assessment from a people, process and technology risk point of view and identify asset wise Threat and Vulnerability, Risk rating and impact.
15. Risk Assessment should include risk tolerance and risk appetite
16. Make recommendations on suitable and cost-effective risk mitigation controls and strategies
17. Prepare an implementation plan for implementing the ISMS controls.
18. Develop Risk registers and Risk Treatment Plans (RTP)
19. Other relevant Activities (key) required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Activities: Accreditation (Certification/ISO Audit) Body:

1. Awareness Training (General) regarding ISMS Standard and Requirements.
   - Number of participants: 20 (in 01 batch)
   - Duration: 01 Day (08 Hours)

2. ISO 27001 Lead Auditor (Certification - IRCA – International Register of Certificated Auditors, UK/ CQI - The Chartered Quality Institute)
   - The number of participants: 2 (two).
   - Duration: 05 Days (40 Hours)

3. ISO 27001 Lead Implementer (Certification - IRCA – International Register of Certificated Auditors, UK/ CQI - The Chartered Quality Institute)
   - The number of participants: 2 (two).
   - Duration: 05 Days (40 Hours)

Key Deliverables:

The consulting firm will ensure through the individual team (from the bank) to build manuals and also assist the said teams to make necessary processes i.e. SOP (Standing Operation Procedure), various policies and other required documentation for achieving the required standard toward the accreditation. One set of hard copy and softcopy (in MS Word format) of the total work have to be submitted. All documentation required for tasks and otherwise related to ISO 27001:2022(Latest Version) certification needs to be completed & submitted to the Bank by the Service Provider. The key Deliverables should include, but are not limited to the following:

1. Project Team Identification and Resource Requirements
2. ISMS Scope Document (Physical and Logical and Technology)
3. Detailed Project plan
4. ISMS Policy Document (List of Applicable Policies, Procedures and best practice documents)
5. Gap Analysis combined Report, featuring gaps, recommendations, priority and owner
6. Asset Registers

2.H.C

7. Risk Treatment Plan
8. Risk Assessment Report
9. Risk Treatment Report
10. Statement of Applicability
11. Other relevant Key Deliverables as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Phase 2: ISMS Implementation and Operation

Key Activities: Consulting Firm

1. Develop/ Update ISMS policies, procedures and templates require for implementation of ISMS
2. Design and implement ISO 27001 framework communication
3. Implementation of the requirements identified from the risk treatment plan
4. Operate ISO 27001 framework
5. Conduct management review and ensure metrics are defined
6. Conduct internal audits (pre-certification) and provide a corrective action plan, review Statement of Applicability, Risk Register and other mandatory documents as per ISO 27001 standards requirement.
7. Corrective action plan for remediation of gaps
8. Facilitate to conduct a management review meeting
9. Assist for Certification Audit
10. Must follow the Plan-Do-Check-Act
11. Mock Audit
12. Register and engage of certification body
13. Certification
14. Other relevant Key Activities as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Following Key Deliverables that shall be provided from Scratch to the Final Stage by the Winning Bidder based on the requirements of SJIBPLC during Certification and 02 Surveillance Audits Period.

Policies and Mandatory Documents:

1. Information Security Policy and Objectives
2. Security Organization
3. Asset Management Policy
4. Risk Management Policy &Procedure
5. Risk Assessment and Risk Treatment Methodology
6. Statement of Applicability (SoA)
7. Risk Treatment Plan
8. Risk Assessment and Risk Treatment Report
9. Definition of Security Roles and Responsibilities
10. Inventory of Assets
11. Acceptable Use of Assets
12. Access Control Policy
13. Operating Procedures for IT Management
14. Secure system engineering principles

2.11.2

15. Communication Policy
16. Information Systems, Acquisition, Development and Maintenance Policy
17. Social Media Policy
18. Supplier Security and Relationship Policy
19. Information Security Incident Management Policy
20. Business Continuity Strategy, Policy and Plan,
21. Human Resources Security Policy
22. Physical and Environmental Security Policy
23. Statutory, Legal, Regulatory, Contractual Requirement and Compliance Policy (Requirements)
24. It can be mentioned that besides the mentioned documents, other documents as per ISMS requirement has to be developed
25. Other relevant Key Deliverables as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Mandatory Records:

1. Records of training, skills, experience and qualifications
2. Monitoring and measurement results
3. Internal audit program
4. Results of internal audits
5. Results of the management review
6. Results of corrective actions
7. Logs of user activities, exceptions, and security events
8. Other relevant Mandatory Records as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Procedures:

1. Asset Management Procedure
2. Media Handling Procedure
3. Change Management Procedure
4. Physical & Environmental Security Procedure
5. Systems Planning and Acceptance
6. Backup and Recovery
7. Business Continuity Procedures
8. Internal Audit Procedures
9. Antivirus Procedures
10. Bidder Management Procedure
11. Access Control Procedure
12. System Development Procedure
13. Network Security Procedure
14. Security Compliance Procedure
15. Information Security Incident Management Procedure
16. Other relevant Procedures as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

2.H.C

Templates:

1. NDA Format
2. Visitor Access Register
3. Media Movement Register
4. Hardware Movement Register
5. Change Control Forms
6. Incident Report
7. Access Request Forms
8. Backup Schedule
9. New User Account Requisition
10. Asset Register
11. Revocation of Access Right Form
12. Business continuity Test report formats
13. Other relevant Templates as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Most commonly used other Documents:

1. Procedure for document control
2. Controls for managing records
3. Procedure for internal audit
4. Procedure for corrective action
5. Bring your own device (BYOD) policy
6. Mobile device and teleworking policy
7. Information classification policy
8. Password policy
9. Disposal and destruction policy
10. Procedures for working in secure areas
11. Clear desk and clear screen policy
12. Change management policy
13. Backup policy
14. Information transfer policy
15. Business impact analysis
16. Exercising and testing plan
17. Maintenance and review plan
18. Business continuity strategy
19. Other relevant Commonly Used Documents as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

2.H.C

Technical Documentation:

The consulting firm will have to provide documentation on the following points as a part of the technical documentation-

1. Process approach for ISO 27001:2022(Latest Version) design and Implementation.
2. Risk Assessment process approach and methodology.
3. ISMS development activity details.
4. Pre-Audit assessment process plan and execution.
5. Statement of Applicability: approach and completion.
6. Deliverables.
7. Project timeline and completion plan.
8. Consultancy Team details including qualifications, experience, references etc.
9. Other relevant Technical Documentation as and when required by the bank to achieve ISO 27001 Certification and 2 Surveillance Audits.

Phase 3: Certification

Certification Body will perform the following activity for the purpose of certification:

Certification & Maintenance	Stage	Assignment/Activities
Relevant Scopes/Tasks and Initial Certification	Stage I (Pre-Certification Audit)	Review Documentation, process and other relevant tasks that are required for certification
	Stage II (Certification Audit)	Review the Implementation controls and effectiveness of process and other relevant tasks that are required

Phase 4: 1st Surveillance Audit

Certification Body will perform the following activity for the purpose of 1st Surveillance Audit:

Certification & Maintenance	Stage	Assignment/Activities
1st Surveillance Audit	Certification Maintenance Year 01 (after initial Certification)	Checking of the procedures and policies and other relevant tasks that are used in everyday operations

Phase 5: 2nd Surveillance Audit

Certification Body will perform the following activity for the purpose of 2nd Surveillance Audit:

Certification & Maintenance	Stage	Assignment/Activities
2nd Surveillance Audit	Certification Maintenance Year 02 (after initial Certification)	Checking of the procedures and policies and other relevant tasks that are used in everyday operations

BIDDER'S RESPONSE/STRENGTH

GENERAL

SL	Description	Bidder offer
1	Name of the Company	Please mention

2.H.C

2	Address of Registered Office	Please mention
3	Presence and locations of Offices in Bangladesh	Please mention
4	Details of Team Lead and number of persons who are proposed to be associated for executing the project. The team should be consisting of ISO 27001 Lead Implementer and Auditor Implementer having experience of conducting ISO 27001 certification project	Please submit the Resume of Team Lead and core resources
5	Number of project team Lead and their qualification and project experience	Please mention
6	Number of project team member and their qualification and project experience	Please mention
7	Number of ISO 27001 Lead Auditor/Implementer	Please mention
8	Number of ISACA, ISC2 and OSCP qualified personnel	Please mention
9	Number of Bank and NBFI Client with Name	Please mention
10	Number of Client with Name (other than Banks and NBFIs)	

Training:

a. ISO 27001 Awareness Training:

Sl No	Area/Domain	Requirements / Descriptions	Document Reference & Response
01	Area to be covered	1) Information Security and International Standards 2) Information System Security Requirements 3) Security Policy 4) Security Organization 5) Asset Classification and Control 6) Personnel Security 7) Physical and Environmental Security 8) Communication 9) Operations Management 10) Access Control 11) System Development and Maintenance 12) Business Continuity Management 13) Compliance 14) Identification of ISO 27001 Controls. 15) Other relevant areas to achieve ISO 27001 Certification and 2 Surveillance Audits.	
02	Duration	08 hours (01 Day)	
03	Participants	20	
04	Framework to Follow	Capacity Building must follow the latest international recognized/ attested framework/ syllabus i.e. ISO 27001:Latest Version (if any)	
05	Training Venue	Training will be delivered at bank arranged venue.	
06	Facilities	Bank will provide training infrastructure including training hall, projector, whiteboard, papers a laser printer, transport, food & beverage, other logistic (if any) Service Provider will provide Trainer and training materials	
07	Trainer	Must be ISO 27001 Lead Auditor/Lead Implementer (CQI|IRCA)	

2.4.e

b. ISO 27001 Lead Auditor Training

Bidder Response

Sl No	Area/Domain	Requirements / Descriptions	Document Reference & Response
01	Area to be covered	1) Information Security and International Standards 2) Information System Security Requirements 3) Security Policy 4) Security Organization 5) Asset Classification and Control 6) Personnel Security 7) Physical and Environmental Security 8) Communication 9) Operations Management 10) Access Control 11) System Development and Maintenance 12) Business Continuity Management 13) Compliance 14) Identification of ISO 27001 Controls. 15) Other relevant areas to achieve ISO 27001 Certification and 2 Surveillance Audit.	
02	Duration	5 Full Days (40 Hours)	
03	Number of Participants	2 (two)	
04	Framework to Follow	Capacity Building must follow the latest international recognized/attested framework/ syllabus i.e. ISO	
05	Training Venue	Training will be delivered at Bidder arranged venue.	
06	Trainer Qualification	The trainer should be certified on the below domain/subject: 1) ISO 27001 Certified Trainer/Certified in Information Security Management Standard (ISMS)/ISO 27001 LA	
07	Trainer's Profile	For conducting Capacity Building training, 03 profiles of the trainers must be submitted with the consent letter from the trainer.	
08	Trainer Practical Knowledge	Besides theoretical knowledge, the trainer is preferred to have hands-on practical ITES operational as well as implementation expertise in financial sector (banking and non-banking).	
09	Training as Core Activities	For training, the trainer must be a professional trainer. His/her profession must be under a similar type of organization (trainer should not be a service holder – giving training as an optional service).	
10	Certification Examination	Instructor Led (IRCA) Certification should be included for 02 participants	
11	Others (If any)	Bidder Response	

ZH.C

c. ISO 27001 Lead Implementer (LI) Training

Bidder Response

Sl No	Area/Domain	Requirements / Descriptions	Document Reference & Response
01	Area to be covered	1. Information Security and International Standards 2. Information System Security Requirements 3. Security Policy 4. Security Organization 5. Asset Classification and Control 6. Personnel Security 7. Physical and Environmental Security 8. Communication 9. Operations Management 10. Access Control 11. System Development and Maintenance 12. Business Continuity Management 13. Compliance 14. Identification of ISO 27001 Controls. 15. Other relevant areas to achieve ISO 27001 Certification and 2 Surveillance Audit.	
02	Duration	5 Full Days (40 Hours)	
03	Number of Participants	2 (two)	
04	Framework to Follow	Capacity Building must follow the latest international recognized/ attested framework/ syllabus i.e. ISO	
05	Training Venue	Training will be delivered at Bidder arranged venue.	
06	Trainer Qualification	The trainer should be certified on the below domain/subject: ISO 27001 Lead Implementer (LI) Certified Trainer /ISO 27001 Lead Auditor (LA) Certified Trainer/Certified in Information Security Management Standard (ISMS).	
07	Trainer's Profile	For conducting Capacity Building training, 03 profiles of the trainers must be submitted with the consent letter from the trainer.	
08	Trainer Practical Knowledge	Besides theoretical knowledge, the trainer is preferred to have hands-on practical ITES operational as well as implementation expertise in the financial sector (banking and non-banking).	
09	Training as Core Activities	For training, the trainer must be a professional trainer. His/her profession must be under a similar type of organization (trainer should not be a service holder – giving training as an optional service).	
10	Certification Examination	Instructor-Led (IRCA) Certification should be included for 02 participants	
11	Others (If any)	Bidder Response	

Annexure-B

Financial Offer
of

Information Security Management System (ISMS) – ISO 27001:2022 (Latest Version) End to End Certification Consultancy for Preparation, Implementation and Accreditation Service for the Bank.

Format of the Financial Offer

Financial Offer must be submitted as per following format and all other cost (if any) must be integrated into the service cost:

Service	Price (BDT) Excluding VAT (VAT to be borne by the bank)
End to End Certification Consultancy for Preparation, Implementation and Accreditation Service of (ISMS) ISO 27001:2022 (Latest Version) for the Bank which includes ISO 27001:2022 (Latest Version) Certification, 1st Surveillance Audit, 2nd Surveillance Audit and other requirements as per this RFP	BDT---------- /-

•Price excludes VAT and related VAT to be borne by the bank.