SBAC
BANK

INVITATION OF QUOTATION FOR IMPLEMENTATION OF (I) ISO 27001 CERTIFICATION AND (II) VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

Scope of Bid:

SBAC Bank of Bangladesh wishes to receive bids from the eligible firms or companies for acquisition and implementation of ISO 27001 Certification and VAPT system and Certification.

General Terms & Conditions:

Bidder's qualification: The bidder must have experience of below-mentioned implementation.

1. Bidder need to be recognized audit and consultancy farm focusing on audit, assessment and cyber security having experience in working with cyber security and compliance for last 05 (Five years)
2. **Validity of Offer:** Offered prices must be valid for 180 days. However, prices may be reviewed quarterly by the bank with complied bidders.
3. Mode of Payment: Payment will be made step by step upon completion of deliverables and acceptance from the Bank.
4. **Warranty:** Bidders/Vendors should specify the service warranty type and period.
5. **Distribution of Tender Schedule:** Tender Schedule will be available at our Website (www.sbacbank.com/procurement) from 23.12.2021 to 05.01.2022 (during Business Hours).
6. **Submission of Tender:**

   a) Sealed envelope containing full name and address of the participant farm/company must be dropped in the tender box kept in ICT Division as on 06.01.2022 (From 10:00 AM to 4:00 PM). No late submission will be received by the Bank after opening of the Tender Box.

   b) The bidders should submit their tender, mentioning "Technical Offer" & "Financial Offer" separately in 02 (two) separate envelopes and both should be dropped in the Tender Box entering into a single bigger size envelope. Forwarding letter having contact details of bidder's contact person should be submitted with the offer. Bidders should submit the soft copy of the bid for the use of the Bank.

   c) Bidders may submit offers for any part (VAPT or ISO 27001) or all part of the schedule.
7. Opening of Tender: Tender Box will be opened on the same day, i.e. as on 06.12.2022 at 4:00 PM in presence of the bidders (if any).

   Submission of Documents: - Full particulars of the ownership, constitution, year of incorporation and main business should be submitted, Photocopy of all the relevant documents should be submitted with the offer including the followings:

   a) Valid & Up-to-Date Trade License, TIN & VAT registration Certificate.

   b) List of Corporate Clients along with respective experience certificate of successful supply and implementation mentioning name of contact person with phone number.

   c) Appraisal certificate from minimum 02 (Two) clients must be submitted.

   d) Copy of Certificate of Incorporation (in case of company)

   e) Authorization letter from certification body.

8. Local Office Address and detail of Personnel for instant support and Services: Bidders/vendors should submit their local office address, contact number and list of personnel, who will provide instant local support and Services.

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
Head Office, Dhaka

9. **Bid Security:** Bidders must submit the bid security in the form of payment order amounting BDT 3.0 lac only which is refundable after issuing work-order. If the selected vendor denies receiving work-order, The submitted bid security will be forfeited. You must submit bid security with the financial documents.

11. Bidders will quote in BDT for the offered items including applicable VAT or Tax and any other hidden cost. The payment will also be made in BDT. VAT & Tax that will be deducted from the invoice at the time of payment according to government policy.

12. Vendors will be ranked & selected on weightage basis. 70% weightage will be applicable for technical compatibility whereas 30% weightage will be applicable for financial aspects.

13. Bidder should provide details of the technical team along with profile.

14. Vendors not having a valid VAT registration number will be considered as disqualified.

15. The Bank reserves the right to relax, change or drop any of the terms and conditions of this tender schedule without any further notice.

16. The Bank reserves the right not to accept the lowest bidder and to reject any Tender or part thereof or all tenders without assigning any reason whatsoever. Any decision of the Bank in this regard shall be final, and binding on the bidders.

17. The Bank reserves the right to re-issue the Tender and or any part thereof without assigning any reason whatsoever, at the sole discretion of the Bank. Any decision in this regard shall be final, conclusive and binding on the bidder.

18. The Bank reserves the right to adjust arithmetic and other errors in any Tender in the manner in which the Bank deems fit and proper. Any decision in this regard shall be final, conclusive and binding on the bidder.

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
Head Office, Dhaka

Technical Specifications for ISO 27001 & VAPT

1. ISO 27001 Compliance and Certification

1.1 Scoping Information for Bidders:

a) Number of Location: 01 (One)
b) In Scope Division/Activities/Business functions: IT Division, Data Center, BACH, Card Division, DFID, SWIFT
c) Support functions: Risk Management and Internal Audit

1.2 Scope of the project

The whole project is under single package. Detailed scope is as follows:

- Conduct IS0 27001 Gap analysis based on the ISO 27001:2013 requirements (To be conducted by proposed Certification body)
- Develop policies, Procedure, standard & other documents required for ISMS in fulfillment of identified gap.
- Preparation of Statement of Applicability for IS0 27001
- Remediation support recommendation to implement controls by proven consultant
- Conduct risk assessment
- Support internal audit to fulfill ISMS requirements
- Certification audit by Certification body
- Perform surveillance audit
- Awareness Training for 30 personnel audience type.
- ISO Lead Auditor & Lead Implementer training with certification for 5 personnel in OEM premises.

1.3 Required Activities

This should cover the following activities:

1. Identifying and documenting the scope of ISO 27001 certification.
2. Service Provider needs to identify functional areas and processes to be covered in the scope. Documenting the scope as per ISO 27001 certification requirement.
3. Reviewing of ISMS policy, processes, systems and procedures relevant to managing risk and improving information security posture to deliver results in accordance with the organization's overall IS policies and objectives.
4. Conducting of ISO 27001 Gap assessment (To be conducted by CB). Service Provider shall conduct gap assessment against the ISO 27001 standard and provide the current status of ISMS to SBAC Bank management. The selected service provider (Bidder) is required to provide assistance to SBAC Bank's internal audit team for closure of audit findings.
5. Preparation of guidelines, procedures and other subsequent documents. The Selected Bidder would have to revise or formulate new documentation requirement such as Information Security policy, Standard & guidelines, Procedures, subsequent documents, Baseline security standard etc. The required documentation should also include the steps to be performed for ongoing IS0 27001 compliance.
6. The agreement with the bidder will be applicable for a period of 3 years which includes the first ISO 27001 certification process and subsequent surveillance audits.
7. Deliverables for Certification:
   i. Pre-certification Gap assessment followed by Audit report (To be conducted by Certification Body)
   ii. All documentation required for ISO 27001 certification and closure of audit findings,

ISO 27001 Certification audit by the approved certification body. The bidder has to mention the certification Body along with Authorization letter from certification Body in the technical bid.

1.4 Required Documentation for review/formulation

The successful bidder must review and update existing documents (where available) as needed or formulate and deliver following mandatory documents:

1. Scope of the ISMS
2. Information security policy and objectives
3. Risk assessment and risk management guidelines
4. Statement of Applicability
5. Risk remediation plan
6. Risk remediation report
7. Definition of security roles and responsibilities
8. Inventory of assets
9. Acceptable use of assets
10. Access control policy
11. SOP's for IT management
12. Supplier security policy
13. Incident management procedure
14. Change management procedure
15. LMS (Log management system) handling procedure
16. Business continuity Management procedures
17. Legal, regulatory, and contractual requirements
18. Records of training, skills, experience and qualifications
19. Monitoring and measurement results
20. Internal audit program
21. Results of internal audits
22. Results of the management review
23. Results of corrective actions
24. Review/Update/formulate Information security policy aligning with ISO 27001 and Bangladesh Bank's Guideline
25. Review/update/formulate Incident management policy and procedures for Card
26. Review/update/formulate change management procedure for Card operations
27. Review Business continuity plan relevant to card operation
28. Review/update/formulate data retention policy
29. AI (Artificial intelligence) policy
30. Cryptographic key management policy and procedures

32. Information Security monitoring systems and processes

Bidder should also review (where existing documents available) or formulate the following documents:

- Procedure for document control
- Controls for managing records
- Procedure for internal audit
- Procedure for corrective action
- Bring your own device (BYOD) policy
- Mobile device and teleworking policy
- Information classification policy
- Password policy

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
Head Office, Dhaka

- Media Disposal and destruction policy
- Procedures for working in secure areas
- Clear desk and clear screen policy
- Change management policy
- Backup policy Information transfer policy

Bidder should also formulate any other policy and procedure which is required to ensure compliance with ISO 27001.

Information security Policy should be aligned with ISO 27001 and Bangladesh Bank's ICT Security guideline.

2. Vulnerability Assessment & Penetration Testing (VAPT)

2.1 Methodology

Bidder may consider the following while conducting VA & PT:

- Dynamic vulnerability scanning.
- Security Architecture review
- External Network Vulnerability Assessment and Penetration Testing
- Internal Network Vulnerability Assessment and Penetration Testing
- Web Application Manual Penetration Testing
- Web Application Dynamic Pen Testing
- DMZ or Network Architecture Designs /Reviews
- Virtual Infrastructure Security Assessment
- Server Configuration Reviews
- Database security Assessment

Bidder should provide Separate VA and PT report. PT report must include evidence of successfully exploited vulnerability. VA report should be manually verified and false positive issues should be identified and reported accordingly.

2.2 DELIVERABLES

Include descriptions of the types of reports used to summaries and provide detailed information on security risk, vulnerabilities, and the necessary countermeasures and recommended corrective actions. Include sample reports as attachments to the proposal to provide an example of the types of reports that will be provided for this engagement. Vendors will provide reports in three separate files.

1. Executive Summary report
2. External VAPT report
3. Internal VAPT report

In 'Executive Summary' deliverables will be

a) Purpose, Methodology and Scope of work for External and Internal Penetration Testing
b) Penetration Testing tools used
c) Overall Evaluation Summary of observation risk severity (High, medium, low etc.) along with pie chart presentation.

In "External Penetration Testing" and "Internal Penetration Testing" reports, the technical details of the test will be documented. The following elements must be brought in these reports:

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
Head Office, Dhaka

a) Objective, scope, summary of findings. Risk rating and Likelihood Criteria
b) Detailed technical report for each host under the scope as required.
c) In technical details report here must be Host identification, number of vulnerabilities and type of vulnerabilities, open ports, active services by enumeration action.
d) Graphs representing risk severity level must be present
e) Vulnerability Details of hosts along with assigned risk grade and Likelihood grade will be presented
f) Remediation of each vulnerability will be presented
g) Annexure that showing up step by step penetration attempts to each vulnerability found and identity as threat.

Achievement of the following scenario would qualify as successful penetration:

- Access to internal resources (like file server, DN mail server, Web application server etc).
- Reading restricted files (reading / browsing restricted folders, Web application files, OS critical files etc).
- Reading transaction data.
- Access to any user account.
- Escalating privilege of lower privileged user account, in case of white box testing
- Gain Access to administrative accounts.
- Gaining access to network management systems.
- Demonstrating ability to control resources (like desktops, servers, devices etc).
- Exploiting any of the OWASP top 10 vulnerability.

In case of successful penetration, pen tester MUST not alter any data or do any activity which may cause unwanted disruption. Pen tester MUST keep evidence and Present it to IT Team as well as include evidence in Report.

2.3 Annual Vulnerability Assessment, Penetration Testing and Configuration review

SL	Item	Quantity
1	Server (including VM)	165
2	Router	5
3	NG Firewall	9
4	Web Application Firewall	2
5	Email Security Gateway	2
6	Core Switch	4
7	Total IP address	300

** Details can be collected from SBAC IT Division, Head Office

Bidder shall also conduct Re-validation scans/testing after mitigation of identified Vulnerabilities twice.

3 Basic Criteria for both the Projects

Interested bidder(s) must qualify for the below criteria:

1. The bidder should have registered office in Bangladesh at least for last 5 years and a reputed organization having experience in information security, Information System Audit, and Cyber security business with Minimum 05 years.
2. The bidder must have at least 02 (two) technical resources (ISO 27001 Lead Auditor) for similar service.
3. It is preferred to have at least two (2) ISO 27001/VAPT project work experience in Bank/NBFI/MNC in Bangladesh. Submission of relevant proof is mandatory

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
Head Office, Dhaka

4. Bidder(s) must have the legal capacity to enter into the contract under the applicable law of Bangladesh. Bidder(s) shall not be barred as per law of the land that may subject to legal proceedings of any kind.

3.1 Detailed criteria for Project Team and experience

1. Two technical resources of at least 5 years of Information security & IS Audit experience is preferred. (Provide experience certificate of the resources). The Bidder with resources in the domain knowledge of banking Information Security/ IS Audit will carry extra weightage in evaluation (necessary documents should be enclosed).
2. Bidder should have at least 2 (Two) experience of conducting VA & PT project in Bangladeshi Bank/multinational organization.
3. The Bidder should have Certified Professional in their team (HR resource profiles are to be attached as evidence)-
   1) Minimum 01 (one) nos. of experienced resources with CISSP or similar.
   2) Minimum 02 (Two) nos. of experienced resources with CISA or similar.
   3) Minimum 02 (Two) nos. of experienced resources with ISO 27001 Lead Auditor.
   4) Minimum 2 (two) nos. of resources with ECSA/CEH/PenTest+.

3.2 Tender Evaluation

The method of evaluation of Tenders shall follow the 'Quality and Cost Based System' (QCBS) Evaluation will be done as per prescribed marking format mentioned in the tender document.

The weightage of evaluations of Technical & Financial offer shall be 70% and 30% respectively. Technical Evaluation shall be done on 70% percent weightage. Financial evaluation shall be done on 30% percent weight-age. The technically responsive & financially lowest bidder shall get the full marks in the financial offer among the responsive bidders and the others shall be evaluated on relative grading. Finally to obtain the Ranking of the Bidders, both the Technical and Financial grades shall be summed up. To be noted, the lowest bidder will not necessarily be awarded preferential consideration.
The bank has the final decision authority without giving any explanation to any bidder.

Technical Evaluation Matrix is given below

SL	Technical Evaluation	Actionable	Marks
1	Proposal on Details Scope (requirements) as specified in the Schedule	Proposal Document	10
2	Presentations on the Methodology, project plan for the project	Presentation will be Scheduled and communicated to all Bidder	10
3	Completed more than one information security Implementation projects at Banks/NBFI/MNC in Bangladesh (10 Points to be awarded) Completed one information security Implementation projects at Banks/NBFI/MNC in Bangladesh (5 Points to be awarded)	Completion Certificate	15
4	Proposed certification body has certified ISO 27001 more than one Banking/NBFI/MNC in Bangladesh (10 Points to be awarded) Proposed certification body has certified ISO 27001 one Banking/NBFI/MNC in Bangladesh (5 Points to be awarded)	Documentary Evidence (Issued certificate/ Completion Certificate)	15

South Bangla Agriculture & Commerce Bank Ltd. IT Division Head Office, Dhaka

5	Bidder should have at least below credential holders in this project team: 1) Minimum 01 (one) nos. of experienced resources with CISSP or similar. 2) Minimum 02 (Two) nos. of experienced resources with CISA or similar. 3) Minimum 02 (Two) nos. of experienced resources with ISO 27001 Lead Auditor. 4) Minimum 2 (two) nos. of resources with ECSA/ CEH/PenTest+.	Documentary Evidence	10
9	Completed VA & PT project of Bank/NBFI/Insurance/MNC organization in Bangladesh	Documentary Evidence	10
Total			**70**

4. Financial Offer

Bidder should furnish the financial offer in following format

	Major activities	1st year price in BDT	2nd year price in BDT	3rd year price in BDT
1.	**ISO 27001 Compliance Certification**			
1.1	Gap assessment and Training		N/A	N/A
1.2	Implementation of ISMS including documents preparation, remediation consultancy, awareness & implementation.		N/A	N/A
1.3	Year 1 certification Audit & Certification		N/A	N/A
1.4	Surveillance audit (2nd& 3rd year)	N/A		
2.	**Vulnerability Assessment & penetration testing**			
2.1	VA & PT as per the given scope			
Grand Total including VAT & Tax				

5. Terms & Conditions

1. The bidder should not be blacklisted by any government institution in Bangladesh or abroad. (Self-declaration should be provided).
2. The bidder must have strong presence and registered office in Dhaka, Bangladesh for prompt support.
3. Submission of declaration regarding bidder ('s) has the legal capacity to enter into the contract under the applicable law of Bangladesh and bidder ('s) shall not be as per law of the land that may subject to legal proceeding of any kind.
4. All the pages of the tender schedule as well as all the offered document should be duty signed by the authority of the bidder.
5. The bidder must submit last 03 (Three) years financial reports audited by reputed audit firm of Bangladesh.
6. No data and information will be allowed to be taken outside of the Bank's premises in any form in e.g. paper or electronics.
7. The successful bidder must complete the deliverables within 06 (six) Months from the date of receiving work order like:
   a) Gap assessment and training.
   b) Implementation of ISMS including documents preparation, remediation consultancy, awareness & implementation.
   c) Year 1 certification audit & certification.
   d) Bidder will conduct surveillance audit for the 2nd and 3rd year.

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
Head Office, Dhaka

8. The selected bidder shall furnish a schedule of assessment/implementation of the contact of ISO 27001 certification encompassing its entire scopes, discuss the same with the bank officials and arrive finally at a mutually agreed assessment/ implementation schedule with in the overall ambit of six month' time of the first certification.
9. The terms of payment will be under:

   ISO 27001

   Year 1:

   a) 30% payment will be made after completion of Gap analysis.
   b) 30% payment will be made after submission of policy and procedure and related documents.
   c) 20% payment will be made after submission of VAPT report.
   d) Rest 20% payment will be made after year 1 certification.

   Year 2 & 3:

   a) 40% Payment after completion of 50% of Surveillance audit of ISO 27001
   b) Rest 60% after completion of surveillance audit and report submission.

   VA & PT:

   a) 50% payment after completion of Vulnerability Assessment.
   b) Rest 50% payment will be made after final report submission of VA & PT.

10. All quoted prices should be included Gap assessment, documents preparation, remediation consultancy, awareness, Training, implementation, training cost and VAT Tax or AIT etc. if any.
11. Payment will be made after delivery, successful implementation and acceptance from bank.

I/we have completely read the terms and conditions and specifications and understood the total responsibility of the job. I/we have quoted this bid taking all the responsibility and liability.

____

(Authorized Signatory)

South Bangla Agriculture & Commerce Bank Ltd.
IT Division
★ Head Office, Dhaka ★