شاه جلال اسلامی بنك بی ال سی

Shahjalal Islami Bank PLC. শাহজালাল ইসলামী ব্যাংক পিএলসি.

Common Services Division
Corporate Head Office, Dhaka

January 11, 2026

Request for Quotation (RFQ): Sealed Quotation for End to End consultancy, implementation and certification of Payment Card Industry Data Security Standard (PCI DSS) for Card operation of the bank.

Scope of bid

Shahjalal Islami Bank PLC. (Hereinafter referred to as "the **Bank**") wishes to receive bids from the bona fide firms for End to End consultancy, implementation and certification of **Payment Card Industry Data Security Standard (PCI DSS)** for Card operation of the bank.

Terms and Conditions:

1.1 Bidder's qualification

- The Consulting Firm should have registered office in Bangladesh at least for the last 02 years.
- Existence as PCI QSA for at least 02 (two years) in Bangladesh (local/international firm).
- The Consulting **Firm should have PCI QSA from PCI SSC, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, CISA, OSCP, LPT, OEM certification.**
- The Bidder should have 02 (two) years of experience of providing Consultation/Implementation/ Certification services for various PCI DSS disciplines. (Bank/merchant/service provider/issuing authority etc.)
- As a valid PCI QSA firm, the Bidder should have minimum 01 (One) Bank/NBFI working experience in providing Consultation Services E.g. Scoping & Gap Assessment (at least)/Implementation/Certification services for various PCI DSS. Completion Certificate and related document must be submitted.
- PCI QSA must be actively enlisted under PCI SSC, USA website.
- The Consulting Firm must have the legal capacity to enter into the contract under the applicable law of Bangladesh.
- The Consulting Firm should be legal entities and registered national organization/government organization/Public sector unit/PLC. Company that in its name or its other names or also in the case of its Persons in different names shall not be under a declaration of ineligibility for corrupt, fraudulent, collusive or coercive practices and have not been also prohibited by Bangladeshi or international court(s) to enter into contracts. In the case of a government organization, it must have permission for participating in the bidding process from the competent authority.
- The bank should have no record of negative or adverse reputational issues regarding the bidder.

1.2 Documents comprising the bid

a. Technical Description of the deliverables to demonstrate the specified technical requirement as per **Annexure-A**.
b. Schedule for financial proposal as per **Annexure-B.**
c. Photocopy of following documents may be submitted with the offer:
   i. Valid Trade License and Company Profile.
   ii. E-TIN and VAT Certificate
   iii. Business Identification Number (BIN) Details
   iv. Name, contact number and e-mail address of the Contact person
   v. Proof of Experience (all relevant documents required in detail).
   vi. List of corporate clients (Global and Local).
d. No of Employees and Description of their support team with experts' profile.
e. Day wise Project Implementation Plan along with chart according to product delivery.

1.3 Bid prices

Bidders shall quote the price excluding VAT and including Tax in US Dollars (USD). Vendors must submit the quotation with year wise breakdown of Price. Related VAT to be borne by the bank.

1.4 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.

1.5 Bid Security / Earnest Money

The bidder shall submit 2 % (Two) 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 technical 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:

1. Be addressed to the Bank at the following address: **Head of CSD, 2nd floor, Shahjalal Islami Bank Tower, plot#4, Block- CWN(C), Gulshan Avenue, Gulshan, Dhaka.**
2. 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.
3. Bid Security/ Earnest Money should be enveloped into the technical offer
4. 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.
5. 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 **3:00 p.m. on Tuesday, January 27, 2026.**

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 will be more comprehensive and that conform the relevant required product. The Bank will carry out technical as well as financial evaluation according to the criteria of the bank. Bank will give emphasis on quality and the richness of the product as well as experience of the vendor during evaluation.

1.10 Price Negotiation

The Bank may request technically qualified bidders to negotiate the price or any other relevant queries. Representative of the Bidders must have authorization for price negotiation. Bank is no way responsible to award 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 vendor will have to deposit an amount equivalent to 5% (Five) of the total work order/contract value as performance security in the form of Payment Order / unconditional Bank Guarantee in favor of Shahjalal Islami Bank PLC. for the period of 3(three) years (It may be extended) while accepting the Work Order. Performance security will be returned after successful completion of 2nd year recertification.

These clauses maybe added while issuing the unconditional bank guarantee as 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 Product Delivery

Successful bidder is responsible for successfully completion of certification within 3 (three) months from the date of receiving the Work Order. Bidder also have to complete each year recertifications (1st and 2nd year) within 12(twelve) months from the date of receiving certification of PCI DSS.

1.16 Penalty

In case of failure or any kind of delay regarding delivery of the product within due time, vendor will be liable to pay 1% of the total Notification of Award /work order value, as penalty, to the bank for delaying 15 days after the due date. Upon reaching the penalty to 2% of total Notification of Award / Work Order, the performance security as well as the Notification of Award / Work Order may be forfeited on sending a letter to the vendor.

However, the Bank must be informed for any foreseeable delay 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.

1.17 Payment

No advance payment will be made. Payment will be made after successfully completion of **certification and recertification**. Performance security will be returned to the vendor after successful completion of 2nd year recertification. After certification, vendor will get 40% of the total payment, moving on 30% payment of the remaining amount will be made after the 1st recertification and the last 30% payment will be made after the 2nd recertification.

1.18 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.

1.19 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 e-mail: zabedul4463@sjiblbd.com Cell: + 88011814874480	S. M. Tarequl Islam Hyder Common Services Division e-mail: tarequl4471@sjiblbd.com Cell:+8801712480201, +8801755556361

11|01|26
Zahid Hasan
SVP & Head of ICT Security Department

Abul Bashar Md. Zafry
EVP & Head of CSD

MRH ZHC

Annexure-A

Technical Specification

End to End consultancy, implementation and certification of PCI DSS for Card operation of the Bank.

Executive Summary

The Bank has identified itself as a level 1 service provider (as an issuer) as defined by the Payment Card Industry Data Security Standard (PCI DSS) terms & conditions and is seeking to validate its compliance. Bank, at this stage has decided to engage a PCI QSA firm (enlisted & running authorized PCI QSA to operate in Bangladesh) by the PCI Security Standards Council (PCI SSC), USA to perform the PCI DSS Compliance Consultation and Validation (Compliance Certification) Services and assist/help the Bank maintain compliance, throughout this project lifetime (3 years' cycle, Phase I to Phase V).

The Bank wants the PCI QSA to deliver the services as per the below phases (05 Phase)

SL No	Phase	Certification Year	Main Activities
1	Phase – I	Consultation and Certification	Assessment
2	Phase – II		Remediation
3	Phase – III		Certification
4	Phase – IV	Certificate Maintenance (Year 1 after initial certification)	Maintenance
5	Phase – V	Certificate Maintenance (Year 2 after initial certification)	Maintenance

Service Offer includes the following:

- Compliance Validation Service (CVS) Includes but not PLC. to:

  i. Remote Validation Service(s) (Provided in Phase I, II, IV and V)
  ii. Onsite Validation Service(s) (Provided in Phase III)
  iii. Remediation Guidance(s) (Provided in Phase II, III, IV and V)
  iv. Internal Vulnerability Assessment(s)/Scanning(s) (Phase I)
  v. External Vulnerability Assessment(s)/Scanning(s) (Phase I)
  vi. Internal Penetration Testing Service(s) (Phase II)
  vii. External Penetration Testing Service(s) (Phase II)
  viii. Customer portal(s) in service provider's web (provided throughout)
  ix. Trusted Commerce Security Seal(s) (Provided in Phase III, once compliance is achieved)
  x. Other relevant support(s) and services as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.

- Other Services to be Provided:

  i. External Vulnerability Scanning Service(s) as per PCI-DSS requirements during certification and recertification periods.
  ii. PCI DSS Awareness and Implementation Training (Before Phase I)
  iii. Service Duration: Service provider must offer for a three years' cycle starting from consultation and certification, Certificate maintenance year 1 (one) and certificate maintenance for year 2 (two) after certification.
  iv. Other relevant services as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.

MRA 2HC

Functional Requirements for PCI DSS Standard

Service Provider must support SJIBPLC (concerned personnel of the bank) to be PCI DSS compliant by showcasing evidence for the following requirements:

Section / Goal	Requirements
1. Build and Maintain a Secure Network and Systems.	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system password and other security parameters
2. Protect Cardholder Data	3. Protect Stored Card Holder Data 4. Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict Physical access to cardholder data
5. Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security system and process
6. Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

*** Note: The Consulting Firm will have to provide any sort/kind of support and services for above mentioned things and other relevant support and services as and when required by the bank to achieve PCI DSS Certification and 2 Recertification.**

Objective:

Now a day's card related fraud and skimming is one of the threats for card industry. Shahjalal Islami Bank PLC. wants to protect the cardholder data and ensure security of card related transactions. The payment card industry data security standard (PCI-DSS) was developed to encourage and enhance cardholder data security and facilitate the board adoption of consistent data security measures globally.

Description of the Scope of work:

A description of the envisaged scope is enumerated as under. However, the Bank reserves its right to change the scope of the RFP so as to address the need of PCI-DSS requirements. Based on the contents for the RFP, the selected QSA shall be required to independently arrive at methodology and approach, based on PCI–DSS requirements and best practices, suitable for the Bank, after taking into consideration the effort estimate for completion of the same and the resource and equipment requirements.

The Bank expressly stipulates that the QSA's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire assignment and that delivery of the deliverables and the services in connection therewith are only a part of the assignment. The QSA shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful Completion of the entire assignment at no additional cost to the Bank.

The project scope includes the following with an objective to obtain PCI-DSS certification for Shahjalal Islamic Bank PLC. (SJIBPLC). The PCI-DSS certification, including recertification should be as per the latest version of PCI-DSS currently being the version 4.0.1 or latest which will be coming during the project implementation.

Location, Network and Systems for Card Environment

Technology	Description
Locations	1) Head Office – 2) DC, Head Office – 3) DR Site, 4) Branch -142 5) ATM-143
Network	1) Core Router – *** 2) Core Firewall – *** 3) Switch – *** 4) Router- ***
Server/System & Printer	1) Servers in mentioned locations 2) Workstations in mentioned locations
Operating Systems	
Database	
Application	

Note That: ATM switch is maintained by PCI-DSS certified 3rd party vendor.

MRH 2.11.C

Scoping Information (Card Infrastructure)

Sl No	Area	Condition/status
1.	Number of Location	
2.	PCI DSS Compliance status of the Bank	
3.	Issuer and/or Acquirer	
4.	Bank Branch receive Credit Card Payment	
5.	Number of Branch of SJIBPLC	
6.	Cash Deposit Machine (CDM) Receiving Credit Card Payment	
7.	Number of Cash Deposit Machine (CDM)	
8.	Cash Recycler Machine (CRM)	
9.	Number of ATMs	
10.	POS Acquiring status	
11.	Number of Disaster Recovery Sites	
12.	Storing, Processing and Transmitting Card Data in DR Site	
13.	Number of Router, Switches & Firewalls	
14.	Segmentation of CHD (Card Holder Data) Environment	
15.	Mode(s) of taking or capturing Credit Card Number e.g. web portal, telephone, e-mails, fax, Branch Voucher, Bill Payment Machine (BPM), etc.	
16.	List of internal IP addresses (systems) in scope	
17.	Number of Public Facing IP Address included in CHD Environment	
18.	List(s) of Payment Applications which stores, processes, or transmits CHD as part of authorization and settlement	
19.	Status of Payment Application in regard to PA DSS	
20.	Card Production Status of the Bank	
21.	Handling of Key Management of SJIBPLC (in house or outsourced)	
22.	Other relevant areas necessary for PCI DSS Certification and 2 Recertifications	

Note: All relevant information at actual (related to this project) such as DC, DRS, Card Environment information and sophisticated others information will be provided to the awarded bidder after signing of NDA.

PCI DSS Consultation & Certification:

PCI DSS Compliance Validation Service:

The minimum required qualification and experience for PCI DSS

i. Existence as PCI QSA for at least 02 (two years) in Bangladesh (local/international firm).

ii. The Bidder should have 02 (two) years of experience of providing Consultation/Implementation/ Certification services for various PCI DSS disciplines. (Bank/merchant/service provider/issuing authority etc.)

iii. As a valid PCI QSA firm, the Bidder should have minimum 01 (One) Bank/NBFI working experience in providing Consultation Services E.g. Scoping & Gap Assessment (at least)/Implementation/Certification services for various PCI DSS. Completion Certificate and related document must be submitted.

iv. PCI QSA must be actively enlisted under PCI SSC, USA website.

Phase 0: (Kickoff Meeting and Training)

PCI DSS Compliance Validation Services (CVS)/Consultation consist of Project Initiation and Compliance Validation Phases, and to ensure comprehensive and efficient service, the service provider must support Bank for fulfilling the obligations within each phase before progressing to subsequent phases.

Project Initiation:

i. Kickoff Meeting
ii. Discussion on the Project Definition Plan deliverables and responsibilities
iii. Initial engagement with Onsite Validation Services Consultant/Managing Consultant
iv. PCI DSS Training
v. Begin formal scope definition process
vi. Other relevant support(s) and service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.

Project Milestone/Outcome:

1. Project should be well communicated with the Bank and relevant stakeholder.
2. Awareness and Implementation Training Completed

Phase 1: (Scoping & Gap Assessment)

Compliance Validation Services (CVS) Phase I: Will be Performed by Managing Consultant (MC) / PCI Consultant(s).

i. Initial scope agreement
ii. Gap Assessment(s)
iii. Vulnerability Assessment(s)/Scanning(s)
   a. Internal Vulnerability Assessment(s)/Scanning(s) as per the requirement of PCI DSS for Certification and 2 Recertifications.
   b. External Vulnerability Assessment(s)/Scanning(s) as per the requirement of PCI DSS for Certification and 2 Recertifications.
iv. Asset(s) Identification
v. Draft Report(s) on Compliance (ROC) development
vi. Other relevant support(s) and service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.

MRH 2.H.C

Project Milestone/Outcome:

1. Draft ROC (Report On Compliance – Detailed Assessment(s)/Audit Report(s)) including statement of scope
2. Initial Security Assessment(s) Report

a) Additional document(s) / data collection(s)

b) Vulnerability Assessment(s)/Scanning(s) (a list of required components for VA Service is given after this section:
   1) Internal Vulnerability Assessment(s)/Scanning(s) (service provider should do this service while doing common VA and shall produce separate report(s))
   2) External Vulnerability Assessment(s)/Scanning(s) (service provider will repeat this process until Bank achieves a passing score and do this service while doing common VA(s) and will have to produce separate report(s))

c) Penetration Testing
   1) Internal Penetration Testing (service provider should do this service while doing common PT and shall produce separate report(s))
   2) External Penetration Testing (service provider should do this service while doing common PT and shall produce separate report(s))
      - (a list of required components for PT Service is given after this section)

d) Policy and procedure validation/verification (a minimum list of required "Technical Documentation is given just after this section Phase -I)

e) Draft ROC development

f) Other relevant support(s) and service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.

Project Milestone/Outcome:

1. Draft ROC including policy and procedure review
2. Security Assessment(s) Report(s) (external VA, pass or fail) and initial Penetration Testing Report(s)

1.19.1 Lists of required components to be covered in VA Services:

1. Firewalls and Routers
2. Operating Systems
3. Database Servers
4. Web Servers
5. Application Server
6. Common Web Scripts
7. Application Programming Interface (API)
8. Built-in Accounts
9. DNS Servers
10. Mail Servers
11. Virtualization components
12. Web Applications
13. Other Applications
14. Common Services
15. Wireless Access Points
16. Backdoor/ Malware
17. SSL/TLS
18. Anonymous (non- authenticated) key-agreement protocols
19. Remote Access
20. Point-of-sale (POS) Software
21. Embedded links or code from out-of- scope domains
22. Insecure Services/industry- deprecated protocols
23. Unknown services
24. etc

***Note: The Consulting Firm will have to provide any sort/kind of support(s) and service(s) for above mentioned things for VA services and other relevant services as and when required by the bank to achieve PCI DSS Certification and 2 Recertification.**

MRA Z.H.C

1.19.2 Lists of functional components required to cover in PT Services:

1. Analysis security vulnerabilities
2. Investigate Multi Threat Surface
3. Commercial- Grade Exploits
4. Vulnerability Scan Validation
5. Port Scanning
6. Configuration and Services
7. Perimeter Defense – Network Penetration Test (internal and external)
8. Host & device Testing
9. Application Penetration Testing
10. Client-Side Testing of End Users and Endpoint
11. Identity Discovery & Password Cracking
12. Wireless Network Penetration Test
13. Database
14. Mobile Device Penetration Test and Surveillance Camera Attacks
15. Cloud Penetration Testing
16. Web Application Penetration Test

    a. OWASP
       1) Injection
       2) Broken Authentication
       3) Sensitive Data Exposure
       4) XML External Entities (XXE) [NEW]
       5) Broken Access Control [Merged]
       6) Security Misconfiguration
       7) Cross-Site Scripting (XSS)
       8) Insecure Deserialization [NEW, Community]
       9) Using Components with Known Vulnerabilities
       10) Insufficient Logging & Monitoring [NEW Comm.]

    b. Directory Traversal
    c. Scripting Error
    d. Web Password Testing
    e. Identify weakness in web applications, web servers and associated databases
    f. Generate exploits that can compromise security weakness of web server and backend network.

17. ETC

***Note: The Consulting Firm will have to provide any sort/kind of support(s) and service(s) for above mentioned things for PT services and other relevant support(s) and service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertification.**

1.19.3 Deliverables

The minimum required qualification and experience for making Technical Documentation(s) for PCI DSS Support:

i. Consultant Firms must have professional(s) having hands on experience in making Technical Documentation(s) (policy, process, standard) specially in Banking Industry.

ii. Consultant Firms should have minimum 02 years' hands on experience regarding making/assisting for client(s) Technical Documentation.

iii. The policy and procedure should meet the latest standard of Bangladesh Bank ICT Security Guideline Version 4.0 (2023) or latest and latest ICT Security Policy of SJIBPLC, and mapped with other internationally accepted standards/guidelines e.g. PCI DSS 4.0.1 or higher, SWIFT, ISO

MRH

2.H.C

27001, COBIT-5, NIST (updated controls) and CIS CSC V6.1 (updated controls) and each control of this policy should have specific references like which standard's / control's which clause it is covering.

iv. Vendor should have practical experience successfully delivered similar type of Technical Documentation (policy, process, standard) to the client.

1.19.4 Lists of Technical Documentation (but not PLC. to)

A. Required Policy

P00	Overview of the Policy documents
PO1	Protection and Control of Documentation
PO2	Policy Statement [Technology] Usage Policy
PO3	Business/Cardholder Data Policy Statement
PO4	Information Security (Operational) Policy
PO5	Information Security Responsibilities Policy Statement
PO6	Digital Access Control Policy
PO7	Physical Access Control Policy
PO8	Logical Access Control Policy
PO9	Role & Privileges Policy
PO10	System Configuration Policy
PO11	Firewall and Router Policy
PO12	Wireless Access Policy
PO13	Acceptable Usage Policy
PO14	Third Parties Policy
PO15	Information Security Classification Policy
PO16	Cryptographic Key Management Policy
PO17	Physical Security Policy Statement
PO18	Application Software and System Development Policy
PO19	Data Retention and Disposal Policy
PO20	Security Testing Policy (VA & PT, Code Review, Configuration Review and Documentation Review)
PO21	Vulnerability Management Policy
PO22	PCI DSS Compliance Charter
PO23	Endpoint Protection Policy
PO24	Information Technology (IT) Audit Policy
PO25	Disaster Recovery Plan
PO26	Security Incident Response Policy
PO27	Media Protection and Management Policy
PO28	Change Control Policy
PO29	Employee Background Checking Policy
PO30	Staff Training Program
PO31	Password Policy Statement
PO32	Monitoring & Logging Policy
PO33	Network Access Policy
PO34	Internet Acceptable Use Policy
PO35	Project Management Framework

***Note: The Consulting Firm will have to provide any sort/kind of support(s) and service(s) for above mentioned policies and other relevant services as and when required by the bank to achieve PCI DSS Certification and 2 Recertification.**

2.H.C

MKH

B. Required Procedure

PR1	Procedure Control Log/Records
PR2	Log Retention Procedure
PR3	Firewall Configuration Standard Procedure
PR4	Anti-Virus & Malicious Software Procedure
PR5	Change Control Procedure (Access/Hardware/network/Software/ People/ -Process/Infrastructure
PR6	Backup & Restore Procedure
PR7	Rules for Use of E-mail
PR8	Secure coding Checklist for Code reviewer
PR9	Firewall & Router Security Procedure
PR10	Security Incident Management Procedure
PR11	Log Review Procedure
PR12	Vulnerability Assessment/Scan Procedure
PR13	Penetration Testing Procedure
PR14	Risk Analysis Procedure (Assessment, Management and communication of Risk)
PR15	Patch Management Procedure
PR16	Breach Report Procedure
PR17	Security Awareness Program
PR18	PCI Data and associated classification
PR19	User Access Management
PR20	PCI DSS Operational Security Program
PR21	Managing Service Providers

***Note: The Consulting Firm will have to provide any sort/kind of support(s) and service(s) for above mentioned procedures and Other relevant service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.**

MRH

ZHC

C. Required Forms, Logs, Checklist and Instructions (continued)

FLCI1	List of documents required for compliance
FLCI2	Inventory Template
FLCI3	Individual User Agreement
FLCI4	Firewall Ports Required for Business
FLCI5	Firewall Review Meeting Minutes
FLCI6	Change Request/Control Form
FLCI7	Change Control Logbook
FLCI8	System resources and User access list
FLCI9	Username Administration Work Instruction
FLCI10	User Access Form
FLCI11	Media Inventory Log
FLCI12	Information Security Incident Reporting Form
FLCI13	Network Access Using Mobile or Employee Owned PC's
FLCI14	Standard Application Checklist
FLCI15	Key Custodian Acceptance/Acknowledge Form
FLCI16	Key Log Form
FLCI17	Weekly Backup Register
FLCI18	Vendor Support Account/Access Log
FLCI19	Standards Matrix (PCI DSS)
FLCI20	Log Review Form
FLCI21	Daily Security Checklist
FLCI22	PCI DSS Logbook (Audit Activity)
FLCI23	Service Providers Log
FLCI24	Vulnerability Scan Logbook
FLCI25	Penetration Test Targets (Log book)
FLCI26	Pen Test Report Evaluation Checklist
FLCI27	Wireless Access Point Detection Form
FLCI28	List of approved wireless access points
FLCI29	Staff Security Training Log
FLCI30	Role Assignment/Responsibility Matrix
FLCI31	Third Party Service Provider -Agreed Responsibilities Matrix
FLCI32	Authorized Service Providers List
FLCI33	Service Provider Quarterly Security Checklist
FLCI34	Data Security Contract Appendix for Third Party suppliers/ contractors
FLCI35	PED Device List
FLCI36	Inventory and Ownership of Assets
FLCI37	SSL and TLS mitigation
FLCI38	Security Awareness Delivery form
FLCI39	Logs of inactive account process
FLCI40	Data Tracking Log
FLCI41	Password reset form
FLCI42	Form Control Log
FLCI43	Sensitive Material Access Approval Form
FLCI44	Incident Response Plan – Contact details
FLCI45	List of Industry-leading security sources and associated procedure

***Note: The Consulting Firm will have to provide any sort/kind of support(s) and service(s) for above mentioned Forms, Logs, Checklist and Instructions and other relevant service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertification.**

1.19.5 ***Note: The documents mentioned above are to be produced at minimum, along with any other documents identified as not in place, in the PCI DSS gap assessment.**

1.19.6 Phase 2 (Gap Remediation Assistance)

Compliance Validation Services (CVS) Phase II: will be Performed by Managing Consultant (MC)/ PCI Consultant(s).

2 Remediation Consultation Services (Based on Gap Analysis Report of IS Audit, VA & PT and PCI DSS):

PCI DSS Compliance Validation Services

Close consultation to remediate the gaps of total card infrastructure (debit and credit card) of the bank.

Remediation Services (Object Breakdown)

Gap Remediation

- The QSA has to conduct periodic meeting(s) with the Bank to formulate a Gap Remediation Plan. The plan should be detailed with low level implementation steps.
- The QSA has to modify or formulate requisite policies to meet the PCI-DSS requirements.
- The QSA has to provide necessary support and hand-holding assistance to the Bank in remediation of the gaps found, so as to meet the PCI-DSS requirements. The supports have to be in the form of emails, telephone and onsite visits etc. Onsite support from relevant qualified professional is mandatory if there is no national lockdown. Other forms of support have to be agreed by the Bank and the Firm.

Deliverable to the Bank

1. Modified or formulated policies and documents. Those have to be aligned with Bangladesh Bank and SJIBPLC ICT Security Policy.
2. Gap remediation plan and assist to remediate GAPs.
3. Consultancy support and hand-holding assistance to meet the PCI-DSS requirements.
4. Detail low level implementations outline to carry out the remediation.
5. Checklist for ensuring ongoing compliance.

Remediation Services (Work Breakdown)

PCI Remediation Assistance and Advisory Service

1. UnPLC. Clarification support and access to PCI Security Expert by email or phone or onsite support.
2. Ongoing PCI expert remediation advisory services during remediation phase.
3. Provide PCI Awareness & Training programs.
4. Provide Data Security Policies and Procedure Templates.
5. Provide Data Security Literature, information brochure.
6. Provide project methodology and templates.
7. **Other relevant support(s) and service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.**

MRH

Z.H.C

Perform PCI DSS Mandatory Scanning

- Automated Quarterly ASV Scans with PCI Approved Scanning Vendor Solution on relevant assets as per the requirement of PCI DSS for Certification and 2 Recertification.
- Automated Security Penetration Testing on relevant assets as per the requirement of PCI DSS for Certification and 2 Recertifications.

Service provider will extend review of the related documentation and make all the "Technical Documentations based on PCI DSS need (end to end).

a) Additional document / data collection
b) Vulnerability Assessment(s)/Scanning(s)
  1) Internal Vulnerability Assessment(s)/Scanning(s) (service provider should do this service while doing common VA and shall produce separate report(s))
  2) External Vulnerability Assessment(s)/Scanning(s) (service provider will repeat this process until bank achieves a passing score and do this service while doing common VA and shall produce separate report(s))
c) Penetration Testing
  1) Internal Penetration Testing (service provider will do this service while doing common PT and shall produce separate report(s))
  2) External Penetration Testing (service provider will do this service while doing common PT and shall produce separate report(s))
d) Policy and procedure validation/verification
e) Draft ROC development
f) **Other relevant or any sort/kind of support(s) and services(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.**

Project Milestone/Outcome:

1. Draft ROC including policy and procedure review
2. Security Assessment Report(s) (external VA, pass or fail) and initial Penetration Testing Report(s)

2.HC

MRH

2.1.1 Phase 3 (Assessment & Certification)

3 PCI DSS Compliance Certification for Shahjalal Islami Bank PLC:

The QSA has to conduct following for the certifications:

1. Business unit wise procedural guidelines for ongoing compliance.
2. Carry out ASV scans as per PCI-DSS requirements.
3. Vulnerability assessment(s), Penetration testing and other scans besides ASV scans of in-scope infrastructure as per the PCI-DSS requirements (Other than ASV scanning).
4. Carry out PCI DSS certification Audit(s).
5. **Other and any sort/kind of relevant support(s) and service(s) as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.**

Deliverable to the Bank

ASV Scans, VA, PT reports and other scans' reports.

1. Report on compliance.
2. Attestation of compliance.
3. Certificate of compliance.

Completion of Remediation

1. Conduct "On-site Assessment(s)" service
2. Complete detailed Report on Compliance (ROC) or Attestation of Compliance (AOC) as appropriate.
3. Provide Certificate of Compliance.

Compliance Validation Services (CVS) Phase III: Performed by Managing Consultant (MC)/ onsite PCI Consultant(s).

a) Onsite Assessment(s)
b) Identification of remediation action items
c) Guidance for bank - generated remediation plans (as necessary)
d) Continued development of the ROC
e) External vulnerability scan definition

Project Milestone/Outcome:

1. External Vulnerability Scanning
2. Remediation Tracking Spreadsheet (RTS), or ROC

f) Additional onsite validation (as necessary/required)
g) ROC completion and submission to Service Provider's Quality Assurance (QA) Team

Project Milestone/Outcome:

1. ROC submission to QA

h) ROC review and submission (as required)

Project Milestone/Outcome:

1. Final ROC

MRH

ZHC

3.1.1 Phase 4+5 (Recertification)

4 Recertification/Certificate maintenance for 2 years after first initial certification

POST CERTIFICATION COMPLIANCE

Post Certification ongoing compliance

- The Qualified Secure Assessor (QSA) has to conduct periodic meetings with the Bank to ensure that the post certification compliance requirements are being met by the Bank. The QSA will have to consult and advice the Bank in case of any gap found.
- Vulnerability Assessments, Penetration Testing and other scans as per the PCI-DSS requirements.

Deliverable to the Bank

Quarterly scan report(s) by ASV (Approved Scanning Vendors):

- VA, PT and other scans reports.
- Report on compliance.
- Attestation of compliance.
- Certificate of Compliance.
- Other and any sort/kind of required services not covered here for recertification.

PCI Maintenance Assistance and Advisory Service

- UnPLC. Clarification support and access to PCI Security Expert(s) by email or phone or onsite support.
- Ongoing PCI expert maintenance advisory services during maintenance period.
- Provide PCI Awareness & Training programs.
- Provide Data Security Policies and Procedure Templates.
- Provide Data Security Literature, information brochure.
- Provide project methodology and templates.

Perform PCI DSS Mandatory Scanning

- Automated Quarterly ASV Scans with PCI Approved Scanning Vendor Solution on relevant assets as per the requirement of PCI DSS for Certification and 2 Recertifications.
- Automated Security Penetration Testing on relevant assets as per the requirement of PCI DSS for Certification and 2 Recertifications.

Proactive QSA Maintenance Advisory Sessions

- Weekly or Quarterly - QSA Consulting Sessions
- Discussions with Third Party Vendors.
- Discussion with Card Schemes.
- Other activities related to Data Security / PCI Compliance.

ZHC

MNU

1. (Year 1 & Year 2 after initial Certification)

Compliance Validation Services (CVS), Recertification after initial Certification (Year 1 and so on) Phase IV (Maintain): Performed by Managing Consultant (MC)/ onsite PCI Consultant(s).

Service Provider will support for the recertification of bank's PCI DSS. For doing that service provider will do all the needful i.e. Technical Documentation Review, VA & PT and other required services for remaining compliant (except solution required- if any).

The total duration of the PCI DSS re-certification is not exceeding 4 weeks.

a) Awareness & Implementation Training: 01 Day.

b) Vulnerability Assessment/ Scanning:
- o Internal
- o External

Milestone/outcome:

1. 04 successful External VA report by PCI ASV (quarterly)- arranged by service provider as per the requirement of PCI DSS to achieve Certification and 2 Recertifications.

c) Penetration Testing
- o Internal
- o External

Milestone/outcome:

1. Yearly and half yearly segmentation testing through PT penetration testing as per the requirement of PCI DSS to achieve Certification and 2 Recertifications.
2. Besides, need PT after any significant change (if any)

d) Policy and procedure validation/ verification

e) Guidance for Remediation (if any)

f) Evidence Validation

g) Draft Report on Compliance (ROC) development

h) Additional Onsite Assessment (if necessary/required)

i) Finalize Return on Compliance (ROC) – Final Audit Report

Milestone/outcome:

3. Final ROC
4. AOC & COC

j) Other relevant support and services as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.

MRH

Consulting Firm are to provide the following services

5 1. Awareness Implementation Training, detailed Scoping and Gap Analysis:

Scoping of Detail Work

- Study the bank's debit card/credit card inclusive of all payment channels in issuance, acquiring systems and detail in-scope business processes and related systems comprising s, hardware, systems software, applications software, network devices, security devices etc.
- The third-party relationship of the bank for card issuance, card and acquiring file processing etc. has to be accounted for where the cardholder information is stored, processed and/or transmitted which need to be measured against the PCI-DSS compliance requirement.
- **Other relevant and any sort/kind of services as and when required by the bank to achieve PCI DSS Certification and 2 Recertification.**

Gap Analysis

- The Bank's systems including network components, security devices, servers, ATM, applications, business processes, third party relationships, service providers and merchants etc. will be validated for compliance this coverage needs to be comprehensive during this exercise including all types of network scans, vulnerability assessments and penetration testing of the infrastructure, applications and processes as per the PCI-DSS requirements.
- Identify and document the Gaps in Bank's systems and processes as per the PCI DSS requirement.
- List the compliant and non-compliant elements.
- Classify the non-compliant elements on the basis of priority.
- Document the Gaps by providing a suitable comprehensive document to the Bank.

Deliverables

Executive Summary

- Describe the Bank's payment card business along with details of business processes, third party relationships, network diagram, data flow diagram etc.

Summary

- Description of approach and methodology.
- Details of the environment for which GAP analysis was carried out.

Observations

- Documented results of the GAP analysis.
- Documented results of the network scanning, VA & PT.

<u>(Work Breakdown)</u>

Payment Card Data Discovery

- Discover Card Holder data on selected Servers and Desktops.
- Review Card Holder Data Flow.

Security Vulnerability Scan

- Perform PCI Approved Scanning Vendor (ASV) Vulnerability Assessment on assets which are relevant for PCI DSS.

Security Penetration Testing

- Perform Security Penetration Testing on assets which are relevant for PCI DSS.

2.4.e

MAH

Assess PCI Data Security

- Perform extensive review of current card holder environment to the PCI Data Security Standard.
- Review any third-party assessors, data storage entity involved in the card holder data storage, processing or transmission.

Assessment Report

- Deliver GAP Assessment Report providing details of the gaps found in current environment to the PCI Data Security Standard.
- Remediation and Recommendations Plan Matrix

Training

- Training to Bank Personnel on PCI-DSS 4.0.1 or higher / upcoming versions Requirement and Implementation.

*** Note: The Consulting Firm will have to provide any sort/kind of support and services for above mentioned points and other relevant support and services as and when required by the bank to achieve PCI DSS Certification and 2 Recertifications.**

MRH

Z.He

Vendor Response

Task Name: Training

This includes classroom training and on the job training, in all the phases.

a. 01 hours (One-hour) Senior Management Training on PCI DSS benefits for 20 officials (maximum)
b. 3 days PCI DSS implementation training (onsite) for ICT Security, IT Division and Card Division for 20 officials (maximum)
c. PCI ISA (Payment Card Industry Internal Security Assessor) Training (offsite) for 2 officials of ICT Security Department (optional).

Sl No	Area/Domain	Requirements / Descriptions	Document Reference & Response
01	Area to be covered	PCI DSS v4.0.1 or higher version (if applicable)	
02	Duration & number of participants	a. 01 hour (One-hour) Senior Management Training on PCI DSS benefits for 20 officials (maximum)	
		b. 3 days * 5 hours, Total 15 hours; PCI DSS implementation training (onsite) for ICT Security, IT Division and Card Division for 25 officials (maximum)	
03	Training Venue	For 01 Hour and 03 Days training mentioned in (a) and (b) respectively, under point 02- will be delivered at bank arranged location and vendor response for serial 4 to serial 6 is applicable for these training.	
04	Facilities	Bank will provide training infrastructure including training hall, projector, white board, papers, and a laser printer. And Service Provider will provide trainer, training materials, training participation certificates along with food and other relevant refreshments.	
05	Trainer's Track Record	Trainer must have track record in providing training engagement with national or international training institute/ organization.	
06	Trainer Qualification	Trainer should be running PCI QSA (enlisted in PCI SSC, USA website).	
07	Trainer Practical Knowledge	The bidder shall ensure the engagement of same QSA(s) for training.	
08	Othes (if any)	Other relevant areas which are necessary for PCI DSS Certification and 2 Recertifications.	

Service Provider will provide trainer, training materials, training participation Certificates along with food and other relevant refreshments

Task Name: Gap Analysis

Sl No	Area/Domain	Requirements / Descriptions	Document Reference & Response
01	A. Gap Analysis	I. The bidder must identify and analyze the Card Data Environment (CDE) of SJIBPLC and finalize the scope for the validation of PCI DSS compliance.	
		II. According to scope, the bidder shall conduct Gap Assessment task thoroughly.	
		III. Run data discovery tools	
02	B. Submission of Gap Analysis Report	The bidder must provide a list of the compliant and non-compliant elements of SJIBPLC which they find during their assessment and provide a classification of the non-compliant elements on the basis of priority.	
03	C. Legal Stand	I. Running/active Certified PCI QSA Professional (Payment Card Industry Qualified Security Assessor) on board with the firm.	
		II. PCI QSA company with running/active enlistment in PCI SSC (Payment Card Industry Security Standard Council) website.	
04	Experience	I. 02 (two) years of existence in Bangladesh as PCI QSA Firm (Local/Foreign).	
		II. At least 01 engagement in Local Bank (Bangladeshi) as completed/supported minimum gap assessment and given report on gap assessment).	
		II. 01 engagement in other sector in PCI DSS Service.	
05	Others (if any)	Other relevant areas which are necessary for PCI DSS Certification and 2 Recertifications.	

MRH 2.11.C

PCI DSS Gap Remediation

SL No	Task Name		Document Reference & Response
01	**Remediation:**		
	A. Off-Site + On-Site Policy, Procedure and Technical Implementation	I. The bidder shall provide a detailed checklist of required documentation (Policy, Process, Procedure, Standard, Forms, technical tools etc.).	
		II. The bidder shall modify/formulate the required policy and procedures of SJIBPLC as per the latest PCI-DSS v4.0.1 to all requirements.	
		III. The policy should meet the latest standard of SJIBPLC ICT Security Guideline 4.0, PCI DSS 4.0.1, SWIFT, ISO 27001, COBIT-5, NIST (updated controls) and CIS CSC V6.1(updated controls) and each control of this policy should have specific references like which standard's / control's which clause it is covering.	
		IV. The bidder shall arrange/carry out vulnerability scans to all the public facing systems of SJIBPLC by Approved Scanning Vendor (ASV) as per the PCI-DSS requirements.	
		V. The bidder shall continue this ASV scan until the passing score is achieved and shall submit the report to SJIBPLC.	
		VI. The bidder shall provide a detail methodology to perform internal and external Vulnerability Assessment and Penetration Testing (VA & PT).	
		VII. The bidder shall perform internal & external VA & PT (both on ICT Infrastructure and applications in scope) activities until the passing score is achieved and shall submit the report to SJIBPLC.	
		VIII. Other relevant areas which are necessary for PCI DSS Certification and 2 Recertifications.	
	On-site	I. The bidder shall sit with the respective departments/ divisions of SJIBPLC to work with low-level implementation plan as well as resolve the detected Gaps.	
	B. Policy & Procedure Technical Implementation Final Audit-Onsite	II. The bidder shall evaluate the necessary compensating controls (if require).	
		III. The bidder shall review the remediation life-cycle and confirm the SJIBPLC once the remediation is compiled.	
		IV. The bidder shall perform a presentation to Senior Management on the crucial findings, its consequences and remediation on high level regarding the gap assessment	

MKH

		V. Other relevant areas which are necessary for PCI DSS Certification and 2 Recertifications.	

PCI DSS Consultation and Assessment Services (Basic & General):

Sl No	Requirements	Document Reference & response
01	▪ The bidder should be a legally permitted and registered company for at least 02 (two) years. ▪ Furthermore, need to provide all necessary legal documents ▪ A Valid & up to date Trade License (2025-2026), BIN, Latest Income Tax Clearance Certificate, Certificate of Incorporation (in case of PLC. Firm), Bank Solvency Certificate.	
02	▪ The Bidder should have 02 (two) years' experience of providing Consulting, Implementation & Certification services for various PCI DSS disciplines. (Bank/merchant/service provider/issuing authority etc.)	
03	▪ The Bidder should be legally permitted to work in Bangladesh as PCI QSA firm (country list should be under the website of PCI SSC, USA)	
04	▪ The Bidder should have at least 01 (one) PCI QSA with running/active enlistment in PCI SSC (Payment Card Industry Security Standard Council), USA website.	
05	▪ In Service Provider permanent pool, must have the following qualified professionals, where at least one professional from each certification category are available any time to be engaged in the PCI DSS project ▪ In Service Provider permanent pool, must have at least ISO Professional out of which Certified ISO 27001 LA and Certified ISO 27001 LI. ▪ CISA ▪ OSCP ▪ LPT	
06	Other requirements which are necessary for PCI DSS Certification and 2 Recertifications.	

PCI DSS Certification Audit (Final Stage):

SL No	Task Name		Document Reference & Response
01.	**ROC, AOC and COC:** ROC-Offsite AOC-offsite	I. The bidder shall arrange all the necessary arrangement for the Report on Compliance (ROC), Attestation of Compliance (AOC) and Certification of Compliance (COC).	
02	**Others (if any)**	Other relevant tasks which are necessary for PCI DSS Certification and 2 Recertifications.	

MRH

PCI DSS Recertification after Initial Certification (year-1 and year-2)

SL No	Task Name		Document Reference & Response
01.	**Recertification**	I. The bidder shall submit the financial proposal by considering 02 (two) year recertification cost.	
		II. The bidder shall submit its detail implementation plan for the recertification for 1st and 2nd year.	
		III. The bidder shall also submit the detail methodology to accomplish periodic activities for the recertification for 1st & 2nd year.	
02.	**Others (if any)**	Other relevant and any sort/kind of tasks which are necessary for PCI DSS Certification and 2 Recertifications.	

Technical Documentation (Required for PCI DSS Compliance Effort)

Sl No	Sub-Domain/Functional Areas	Document Reference & Response
1.	Consultant Firms must have professional(s) having hands on experience in making Technical Documentation specially in Banking Industry.	
2.	Vendor should have minimum 02 years hands on experience regarding making/assisting for client(s) technical documentation	
3.	Vendor should have successfully delivered similar type of technical documentation (at least 80% of the total documentation) to the client specially banking sector.	
4.	Other Sub-Domain/Functional Areas which are necessary for PCI DSS Certification and 2 Recertifications.	

Project Management

The bidder must follow detailed project management during the certification.

MRH 2.11

Annexure-B

Financial Offer

End to End consultancy, implementation and certification of Payment Card Industry Data Security Standard (PCI DSS) for Card operation of the Bank.

Format for Financial Offer

SL	Product Description	Initial Certification Cost (in USD)	1st year recertification cost after initial certification (in USD)	2nd year recertification cost after initial certification and 1st year recertification (in USD)	Total Cost (in USD)
1	End to End consultancy, implementation and certification of Payment Card Industry Data Security Standard (PCI DSS) for Card operation of the bank.				

- All prices are including Tax & excluding VAT (VAT to be borne by the bank).
- All Prices are to be quoted in USD.
- The payment of the products will be made in BDT at the "Bank's USD BC selling rate" at the date of delivery of the product.