FIRST WOMEN BANK LIMITED (FWBL)

First Women Bank
Limited (FWBL)

Request for Proposal

Implementation of SIEM Solution and 24/7 Security Operations Center

Publish date: 28 May 2022

Reference # FWBL/HO/IT/KK/2022/03

Proposal Submission deadline date & time: 13 June 2022 10:00 am

Opening of technical bid date & time: 13 June 2022 10:30 am

Contents

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

Submission Details:

All proposal submissions for responding to this request must be submitted on or before 13 June 2022 10:00 am in a single sealed envelope containing two separate sealed envelopes distinctly marked as Technical and Financial Proposal.

Submission will be valid if:
- Responses to RFP are submitted no later than 13 June 2022 10:00 am at FWBL, Head Office GF-2 Reception Area, S.T.S.M Foundation Building, CL-10/20/2, Beaumont Road, Civil Line, Karachi.
- Bids are submitted in a Single sealed envelope containing two separate sealed envelopes with separate marking "Technical Proposal" & "Financial Proposal".

Submission Questions & Clarifications

You may contact the following person if you have any questions or require clarification on any topics covered in this Request for Proposal:

Name: Naveed Ali
Email: ali.naveed@fwbl.com.pk

FIRST WOMEN BANK LIMITED (FWBL)

FWBL is requesting Technical and Financial Proposal from qualified bidders for implementation of SIEM solution along with 24/7 Security Operations Center. Bidders may provide solution for:

- Completely Outsourced ("**Managed Services**") solution with Technology stack deployed in bidder's proposed data center along with 24/7 Security Operations Center.
- "**Hybrid Solution**" where technology stack will be deployed in FWBL data center (Primary and DR site) along with outsourced along with 24/7 Security Operations Center either at bidder's premises or FWBL Head Office. Location to be proposed by the bidder.
- Bidder's will have the option to provide technical and financial proposed for either one of the above options or both. FWBL, after evaluation of technical and financial proposal (as per terms of this RFP) will decide on the implementation model i.e. "Managed Services" or "Hybrid Solution". Evaluated Bid will be calculated using the financial proposal provided for the selected implementation model i.e. if FWBL decides to opt for "Hybrid Solution", then financial bids will only be calculated for those bidder's that have submitted proposal for implementation of "Hybrid Solution". Similarly, if FWBL decides to opt for "Managed Services", then financial bids will be only calculated for this bidder's that have submitted proposal for implementation of "Managed Services".

Eligibility Criteria:

The bidder MUST comply with the following minimum criteria. The bid document shall be rejected if the vendor fails to meet the following minimum criteria and submission of the require documents.

- The bidder should be **NTN** and **Sales Tax** registered company in Pakistan.

- Bidder to provide an affidavit on a stamp paper confirming compliance with the following terms in order to be eligible for participation against this RFP.

  - Bidder or any of its associated Partner / Affiliated / Subsidiary company should not have been blacklisted from participating in any public sector bids / RFPs / tenders.

  - Bidder and/or its Owners, Directors, or Partners should not be listed in any of the International/Local Sanctions or ATA list, as required by the local regulator.

- The bidder should have minimum annual gross revenue of Rs. 50 M during the last year. Bidder is required to submit either Income Tax Returns or audited financial statements for last three financial years.

- The bidder must have been in operation for at least three years related to implementation of SIEM solutions and Security Operations Center.

- The proposed SIEM solution must be listed as a "Leader" in the latest "Gartner Magic Quadrant for SIEM".

- For "**Managed Services**" proposals:

  o Bidder must be an MSSP of the proposed solution for at-least one year.

  o Bidder must have completed at-least two implementations with at-least 500 Events per Second (or equivalent).

  o Hosting of the proposed technology solution for proposed services must be within OEM certified data center located within Pakistan. Bidder to provide details regarding this requirement in their respective technical proposal.

- For "**Hybrid Solution**" proposals:

  o Bidder must be an authorized reseller of the of the proposed technology solution(s).

  o Bidder must have active contracts (within Pakistan) with at-least two corporate entities providing services similar to scope of work defined in this RFP.

- Proposed SOC team must be based in bidder's Karachi office.
- Bidder is required to submit Purchase order(s) or work order or any other document demonstrating contractual engagement with respect to these criteria.
- The bidder company should propose a team that has required certifications and experience to provide required services as per scope of work defined in this document. CVs of such person(s) showing project wise experience should be submitted.

FIRST WOMEN BANK LIMITED (FWBL)

Terms of Reference

1. Proposed solution must have following capabilities:

   - The proposed solution must have easy to use, GUI-driven interface for creating real-time advanced analytics rules. Also solution should have ability to correlate threats in real time.
   - In case, bidder is proposing "Hybrid Solution", then
     a. Proposed architecture should support scalability with the addition of hardware (along with existing hardware/VM) & licenses.
     b. Licenses should be perpetual (only support should be renewable on yearly basis).
   - In case, bidder is proposing "Managed Services", then
     a. Availability of Disaster Recovery site for continuity of services
     b. Transfer of Log files (data) from FWBL to MSSP data center should be encrypted
   - Point to Point secure network connectivity between FWBL and service provider site will have to be established and all data communication must be encrypted.

2. The Proposed solution must include:
   - Log management
   - Next Generation SIEM
   - User and entity behavior Analytics
   - Security Analytics
   - File Integrity Monitoring & Registry Integrity Monitoring. In case, proposed SIEM solution does not provide an integrated module/component, then bidders may propose an Add-On for this requirement. Proposed add-on must be deployed in at-least three commercial banks within Pakistan and being actively used for this requirement. Bidder's must provide reference along with implementation details for this requirement, in case of add-on being proposed.
   - Incident Management. In case, proposed SIEM solution does not provide an integrated module/component, then bidders may propose an Add-On for this requirement. Proposed add-on must be deployed in at-least three commercial banks within Pakistan and being actively used for this requirement. Bidder's must provide reference along with implementation details for this requirement, in case of add-on being proposed.
   - Security Orchestration Automation, and Response (SOAR)- In case, proposed SIEM solution does not provide an integrated module/component, then bidders may propose an Add-On for this requirement. Proposed add-on must be deployed in at-least three commercial banks within Pakistan and being actively used for this requirement. Bidder's must provide reference along with implementation details for this requirement, in case of add-on being proposed.

3. Solution must have the ability to correlate the events (and generate alerts) to identify attacks like:
   - Intrusions
   - Worms, Malwares, Viruses & Trojans based activity
   - Anomalous network activity
   - Internal vulnerability threats
   - Breach of access
   - Abnormal trends
   - User specific activities

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

4. Proposed SIEM Solution must support the integration with following devices / applications:

    - Virtualization (VMware & Hyper-V etc.)
    - Sophos XG Firewall
    - End-point Protection, Detection and Response (EPP & EDR) Solutions
    - UNIX/Linux & CentOS including other open source OS.
    - Windows Servers, Active Directory Servers
    - Email Server (MDaemon, & Microsoft Exchange Servers)
    - Web Servers (Tomcat, Apache, IIS etc.)
    - DCC & AAA Servers
    - Storages (DELL EMC, HP & Huawei etc.)
    - Customized logs, Sys log feeds (Third party developed applications)
    - Privileged Access & Monitoring (PAM) / Identity and Access Management Systems
    - Vulnerability Management Solution
    - Databases (Oracle, MySQL, MS SQL Server)
    - Cisco, Huawei, H3C, Juniper & Fortinet Network equipment (LAN & SAN Switches, Routers, Firewalls, IDS, IPS, etc.)
    - Multi-Factor Authentication (MFA) Solutions
    - Internet / Mobile Banking Applications, Middleware's

5. The proposed SIEM Solution must provide central management of all components and administrative functions from a single web based user interface.

6. Proposed SIEM Solution must provide Real-time event management including events correlation and alerting.

7. Proposed SIEM Solution should have User friendly GUI dashboards for security analysts to monitor on a regular basis for suspect or malicious activity and for reporting.

8. Proposed SIEM Solution should have ability to specify filters to include or exclude data events from being gathered, processed or retained.

9. The administrator must be able to define role-based access to various functional areas of the proposed SIEM Solution. This includes being able to restrict a user's access to specific functions of the solution that is not within the scope of a user's role including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing.

10. The proposed SIEM Solution must integrate with 3rd party directory systems as an authentication method e.g. LDAP or AD solution.

11. Proposed SIEM Solution must have ability to define assets based on IP addresses, IP ranges, asset types, asset groups, asset attributes, asset owners, external and internal IP ranges, trusted and un-trusted ranges, etc.

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

12. Proposed SIEM Solution should provide audit trails of all users (including administrator) and generate reports of activities.

13. Proposed SIEM Solution should have the capability for both the agent-less & agent-based logs collection.

14. Proposed SIEM Solution must have Capability of detecting events based on pattern recognition and internal/external threats through strong correlation engine.

15. Proposed SIEM Solution should have ability to schedule reports and distribute to respective team leads through email and other alert channels. The solution shall have the ability to export reports to standard formats like CSV, HTML, PDF, XLS, DOC etc.

16. Proposed SIEM Solution should provide customized alerts generation and intimation through SMS & email.

17. Proposed SIEM Solution must be capable for detection of DOS/DDOS attacks, malwares / botnets Command & Control (C&C) servers and malicious IP/URL addresses etc.

18. Proposed SIEM Solution should have SSHv2 and Secure Web (HTTPS) for remote management interfaces.

19. Proposed solution should include Threat Intelligence feed from OEM with regular updates to detect threats, Indicators of Compromises (IOCs), speed-up breach detection and accelerate response.

20. Proposed SIEM Solution must be able to integrate with external third-party, cloud-based threat intelligence feeds and use this information to detect threats, indicators of compromises (IOCs), speed-up breach detection and accelerate response.

21. Proposed SIEM Solution should have comprehensive customizable operational security dashboards and reports.

22. Proposed SIEM Solution must archive the data in compressed and encrypted format on separate systems and can only be opened by same application.

23. Proposed SIEM Solution must have capability to create multiple policies for the automated retention and disposal of log data.

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

24. Proposed SIEM Solution should have Intuitive log management and search capabilities including log aggregation, log data retention and log analysis.

25. Proposed SIEM Solution must have ability for Security Analysts and Administrators to input internally developed Indicators of Compromise (IOCs) for detection and alerting.

26. Proposed SIEM Solution must have capability to parse the data of non-supported applications and devices.

27. Proposed SIEM Solution should maintain a central repository of log data, in its native and normalized forms for a period not less than 1 (one) year.

28. Proposed SIEM Solution should have capability to provide out-of-the-box compliance packages for GDPR, ISO 27001, PCI, NIST, etc.

29. Proposed SIEM Solution must have capability to reduce identical events data by filtering or aggregation before it is sent to log management or SIEM System.

30. Proposed SIEM Solution must be able to provide out-of-the-box correlation rules to automate the incident detection and workflow process.

31. Proposed SIEM Solution must be capable of monitoring attacks history against critical assets, applications or by particular users.

32. Proposed SIEM Solution must automate internal health checks and notify the user when problems arise.

33. Proposed SIEM Solution must deliver customizable dashboard widgets that can present relevant security information to the users of the system (i.e. event views, network activity views, incident views, etc.).

34. Proposed SIEM Solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, FTP, etc.).

35. Proposed SIEM Solution should be capable of implementation of industry best use-cases for financial industry & etc.

36. Proposed SIEM Solution should be capable of use case mapping with (Cyber Kill Change) CKC and Mitre-Att@ck Framework.

37. Support for auditing / monitoring of DBMS including session monitoring/analysis; preferably the solution be able to capture DB audit trail.

38. Proposed SIEM solution architecture should be flexible to handle future EPS growth

Minimum Requirement for Security Operations Center

1. Bidder should have at least two security analyst level (or equivalent) certified resources for proposed SIEM solution.
2. Bidder should have at least one platform administration level (or equivalent) certified resources for proposed SIEM solution.
3. Bidder should propose the following team structure to work on FWBL in 24/7 operations.
   - At-least 5 L1 resources
   - At-least 3 L2 resources
   - At-least 1 L3 resources.
4. Bidder will be responsible for:
   - Solution design
   - Log source integration with SIEM
   - AI rules configuration
   - Use case implementation
   - 24/7 monitoring, analysis, investigation and remediation support
   - Hardware plus software platform health maintenance
   - Ongoing customizations
5. Bidder should be able to provide responses over queries/ observations/ any recommendations sought by FWBL in a timely manner
6. Bidder should be able to provide knowledge regarding the rule sets/ dashboards/reports and correlating the events as and when required by FWBL.
7. Bidder should provide recommendations to enhance the visibility of SIEM
8. Monitoring and analyzing events generated to ensure all security events are timely highlighted based on their risk/threat levels and timely addressed/actioned to mitigate the impact/risk.
9. Optimize SIEM to generate only critical events whose incident management lifecycle needs to be performed. Gradually with time these events collection will be revised to add more event sources as per best practices and operational efficiency of the overall SOC.
10. Develop standard operating procedures (SOPs) for day-to-day SOC operations. Consisting of the overall incident management lifecycle.
11. Provide threat landscape by providing Global Threat Intelligence feeds

12. Coordinate with FWBL SOC Manager to indirectly get involved with relevant custodian and owner department(s) in case of an incident.

Bill of Quantity

1. SIEM Solution with 500 Events Per Second License.
2. File Integrity Monitoring (FIM) and Registry Integrity Monitoring - 35 Licenses
3. SOAR/incident Management- 10 Users
4. Custom log parsing - 10 Applications

Proposal

This is single stage two envelope bidding procedure as per PPRA rules. The bidders shall submit their proposals in one sealed envelope containing two different separate sealed envelopes marked as "Technical Proposal" and "Financial Proposal" . Only Technical proposal envelope will be opened in the presence of bidders and Financial proposal envelops will stay in FWBL custody till the opening of Financial bids.

Financial proposals from bidders that met the minimum technical score will be opened in front of bidders. Final date of opening of Financial Bids which will be communicated to all the bidders in advance.

Further final evaluation reports containing the combination of marks including technical and financials will be published on FWBL website and PPRA as well.

Successful bidder who qualifies with the combined evaluation, a meeting with the FWBL's management will be held to discuss in details the exact requirements and procedures to be followed in conducting this assignment.

After the finalization of combined evaluation the qualifying organization will be issued "Letter of Intent" which will be followed by the Service agreement and Service order.

Contract Term

Managed Services

SIEM and Integrated Technology Solution

FWBL will sign a contract with the successful bidder for a period of three years, which may be subsequently renewed for additional period based on mutual consent.

24/7 Security Operations Center

FWBL will sign a contract with the successful bidder for a period of one year, which may be subsequently renewed for additional period based on mutual consent.

Hybrid Solution

24/7 Security Operations Center

FWBL will sign a contract with the successful bidder for a period of one year, which may be subsequently renewed for additional period based on mutual consent.

Annual Software SLA Support from OEM & Implementation services SLA

FWBL will sign a contract with the successful bidder for a period of one year, which may be subsequently renewed for additional period based on mutual consent

Above mentioned contractual terms are subject to performance and compliance of the contract signed between FWBL and Bidder.

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

FIRST WOMEN BANK LIMITED (FWBL)

Submission Timeline and Location

FWBL reserves the right to modify below timeline at any time. Should the due date for proposals be changed, all prospective respondents shall be notified. The proposal must follow as per the following high level schedule.

Location and Timing

Bids/Proposals must be delivered to the FWBL, on or before, 13 June 2022 10:00 am and only technical proposals will be opened on the same date at FWBL, Head Office GF-2 Reception Area, S.T.S.M Foundation Building, CL-10/20/2, Beaumont Road, Civil Lines, Karachi.

Milestone	Date & Time
RFP Released	28 May 2022
RFP Bid Submission Date and Time	13 June 2022 10:00 am
Opening of Technical Bids	13 June 2022 10:30 am
Opening of Financial Bids	To be decided

As a result of this Request for Proposal, FWBL may do one of the following at its discretion:

1. Award a contract for this Request for Proposal on the basis of prescribed evaluation criteria.

2. Cancel the whole process.

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

Proposal Evaluation Criteria

- Evaluation of the firms shall be based on information provided in Proposals.

- On the basis of technical evaluation, the financial proposal of only technically responsive bidders (qualified bidders) will be opened in the presence of their Representatives who choose to attend.

- Financial proposals of technically non-responsive vendors will be returned unopened.

- Proposals will be evaluated on the basis of 60 – 40 i.e.

    o 60% of the proposal strength will be measured in Technical evaluation

    o 40% of the proposal strength will be measured in Financial evaluation

Technical Score

Technical evaluation of the proposals will be given weight through the below mentioned factors based on the below formula.

$$\frac{\text{Bidders Technical Score}}{\text{Total Technical Score}} \times \text{Weight}$$

Minimum score of 70% on evaluation criteria specified in "Annexure A" is required to qualify for financial evaluation.

Financial Score

Bid Price will be calculated as:
One time delivery cost of proposed consultancy services.

Please note that Annual Recurring Charge must include all charges including but not limited to service based recurring charges and support fees.

$$\frac{\text{Lowest Bid Price}}{\text{Bidder's Price}} \times \text{Weight}$$

Combined Evaluation will be calculated by adding the Technical and Financial Evaluation as below:

$$\left[\frac{\text{Bidders Technical Score}}{\text{Total Technical Score}} \times \text{Weight} \right] + \left[\frac{\text{Lowest Bid Price}}{\text{Bidder's Price}} \times \text{Weight} \right]$$

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

Format for Financial Bid

The financial bid should be quoted as per the format. The financial bid should be accompanied by Financial bid cover letter. The Bidder shall bear all costs associated with the preparation and submission of its bid, including cost of presentation for the purposes of clarification of the bid, if so desired by the Bank. The Bank will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the Tendering process, the financial bid shall include the following:

- Financial Bid - Commercial Bid Cover Letter
- Financial Bid - Commercial Bid As per Format specified in this document
- Bid Security
- Payment Terms

Bid currency and Validity

- All prices must be quoted in Pak Rupees including all applicable taxes.
- Bid validity will be 180 days after the submission of proposals

Bid Security

All bids must be accompanied by a pay order of Five percent (5%) of "Total Bid Amount" in Favor of First Women Bank Ltd enclosed in the sealed financial envelope and must be delivered to Information Security Division, GF-2 Reception Area S.T.S.M. Foundation Building, CL/10/20/2, Beaumont Road Civil Lines, Karachi – 75530 on or before 13 June 2022 10:00 am

Pre-Award presentation

The FWBL reserves the right to require presentations and/or demonstrations/ Interview from any or all of the bidders, in which they may be asked to, provide additional information.

Format for Technical Bid

Technical Bids must be made in an organized and structure manner in the following form.

1. Table of Contents
2. Technical Bid Cover letter
3. Executive Summary
4. Company Profile
5. Project Management Approach
6. Proposed Solution Delivery Approach
7. Technical Specifications - Compliance of Proposed Solution as required in this proposal
8. For "**Managed Services**", bidders to provide minimum benchmark for data center as required by OEM. Bidders to also provide information related to compliance of related criteria.
9. Proposed Implementation Timelines
10. Implementation/Technical Team Composition as mentioned in eligibility criteria
11. Reference from Financial Institutions in Pakistan with reference to similar services provided to customer. Reference information should include, but not limited to:
    a. Name of Customer
    b. Service Provided
    c. Scope of work provided by bidder
    d. Customer Reference Contact Name
    e. Customer Reference Contact Number (Office and Mobile). Office number is mandatory
    f. Designation of the Customer Reference Contact Person
    g. Year service was provided for this reference
12. Annexure – Documentary Evidences
    a. GST/NTN Certificate
    b. Organization's establishment
    c. Similar Assignments and References
    d. Team Certificates
    e. Audited Statement (Profit and Loss, Balance Sheet and Cash Flow Statements) or Income Tax Returns

Payment Terms

- Invoices will be cleared upon receiving the invoice along with necessary documentations and project milestones. Incomplete claims shall be returned to vendor.

- Taxes will be deducted at source as per government rules at the time of payment.

- If the progress of the work is not to the satisfaction of the FWBL Management, FWBL Management has the right to cancel the order, get the work done from third party selected accordance with the PPRA rules.

Payment Schedule – "Hybrid Solution"

Project Phases	Payment Plan (%age of Software Solution License and Implementation Services Cost)
Advance at the time of contract signing	20%
Delivery of the solution in UAT Environment for Testing	20%
UAT Sign off	30%
Completion of the engagement	20%
Completion of 3 Months (implementation) in Live Environment (After Go-Live)	10%

- Payments against SLA for Security Operations Center will be made against monthly invoices.
- Post Go Live OEM SLA and Implementation Services SLA will be payable at the time of renewal of such contracts.

Payment Schedule – "Managed Services"

Project Phases	Payment Plan (%age of Implementation Services Cost)
Advance at the time of contract signing	30%
Completion of Implementation Services	50%
Completion of 3 Months (implementation) in Live Environment (After Go-Live)	20%

Payments against SLA for Security Operations Center will be made against monthly invoices.

Complete Pricing

The respondent / bidder should mention all the charges in financial bid deem necessary to complete the scope of work, should include all incidental expenses in the project pricing. This includes travel expenses, printing or reproduction, communications, etc. Any invoices for expenses beyond those **itemized (listed)** in the RFP response will not be entertained by FWBL.

FWBL RFP - Implementation of SIEM Solution and 24/7 Security Operations Center

Annexure A: Evaluation Score Criteria

This section includes vendor evaluation criteria. The bidder must score at-least 70% in the following evaluation criteria to be eligible for successful bidding:

No	Evaluation Factors and Description	Total Marks	Max Marks	Total Marks and Distribution ranking
1	Experience of proposed Technical Team with proofs and certificates.	20	20	To be assigned by Technical Evaluation Committee
2	Organization Financial Strength	15	15	Firm has more than Rs. 300 million annual gross revenue for last Three (03) years
			10	Firm has more than Rs. 150 million annual gross revenue for last Three (03) years
			5	Firm has at least Rs. 50 million annual gross revenue for last Three (03) years
3	Similar SIEM projects completed along with proof and reference within last 3 years.	15	15	Firm has completed at-least six similar implementations.
			10	Firm has completed at-least three similar implementations.
			5	Firm has completed at-least two similar implementations.
4	Similar SOC services provided along with proof and reference within last 3 years.	15	15	Firm has managed at-least six off-site (outsourced) SOC engagements (clients).
			10	Firm has managed at-least three off-site (outsourced) SOC engagements (clients).
			5	Firm has managed at-least two off-site (outsourced) SOC engagements (clients).
4	Technical Bid Completeness (documentary Proof, brochures, diagrams, non-deviation material, relativity etc.)	10	10	To be assigned by Technical Evaluation Committee
5	Technical(Compliance) Evaluation of Proposed technology solution	75	75	To be assigned by Technical Evaluation Committee

6	Technical(Compliance) Evaluation of Proposed SOC Services	25	25	To be assigned by Technical Evaluation Committee

In case, single bidder has proposed "Managed Services" as well as "Hybrid Solution", above evaluation will be completed for both the proposals separately.

Annexure B: Technical Bid Documentation

Technical Bid Cover Letter

Tender Reference No:
Date:

FWBL.
Head Office, Mezzanine Floor,
STSM Foundation Building,
Civil Lines, Dr.Zia-ud-Din Ahmed Road,
Karachi.

Dear Sir,
Sub: your RFP for "Implementation of SIEM Solution and 24/7 Security Operations Center" dated DD-MM-YYYY.

With reference to your subject RFP, we have examined and understood the instructions including all annexure, terms and conditions, project scope forming part of the RFP, we hereby enclose our Technical Bid for "Implementation of SIEM Solution and 24/7 Security Operations Center" as mentioned in the RFP documents.

In the event of acceptance of our bid by The Bank (FWBL) we undertake the "Implementation of SIEM Solution and 24/7 Security Operations Center" as per your purchase orders.

We agree to abide by the terms and conditions of this bid offer till 180 days from the date of opening of bids and our offer shall remain binding upon us which may be accepted by the Bank any time before expiry of 180 days.

Until a formal contract is executed, this tender offer, together with The Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us.

Dated this day of _____ 2022
Signature: (In the Capacity of) _____

Duly authorized to sign the tender offer for and on behalf of

FIRST WOMEN BANK LIMITED (FWBL)

Bid Particulars

Name of the Bidder.	
Is the Bidder the OEM of the solution or an Authorized Partner / Re-seller	
Registered Address of the Bidder.	
Name and designation of the person to whom all references shall be made regarding this tender.	
Address of the person to whom all references shall be made regarding this tender.	
Telephone No. (With country and area code).	
E-Mail of the contact person:	
Fax No. (With country and area code).	

Name: _____

Location: _____

Date: _____

_____
Company Seal & Bidder's Signature

FIRST WOMEN BANK LIMITED (FWBL)

Bidder/OEM Owner/ Authorized Partner/ Other Consortium Member Profile:

S. No.	Name of the Company	
01.	Indicate whether the Company is the lead Bidder and whether the Company is the OEM Owner, Authorized Partner or Other consortium member	
02.	Year Established	
03.	Turnover (in PKR)	**FY 2019:** **FY 2020:** **FY 2021:**
04.	Profit After Tax (in PKR)	**FY 2019:** **FY 2020:** **FY 2021:**
05.	Proposed role of the member in the project	
07.	Head Office Address	
08	Telephone No. (with country and area code)	
09	Fax No. (with country and area code)	
10	E-mail Address	
11	Name of the Key representative for this project	
12	Any accreditations / Certifications of organization and resources	

The Bidder should fill this Annexure for the Bidder and any other member of the consortium separately (including the OEM Owner, Partner and any other member of the consortium)

As of this Date, the information furnished in all parts of this form is accurate and true to the best of my knowledge.

Name: _____

Location: _____

Date: _____

_____
Company Seal & Bidder's Signature

FIRST WOMEN BANK LIMITED (FWBL)

Details of Prior Experience

Please provide details of prior experience of the Bidder / OEM Owner / Authorized Partner / other Consortium members in implementation of Security Information and Event Management Solution.

For each prior experience reference that the Bidder wants to highlight, one sheet in the below template should be submitted in the proposal and should be supported by a copy of the purchase order as documentary evidence in **"Annexure – Documentary Evidences"** of the proposal.

Name of the client bank:	
Country:	
Client address:	
Assignment Type	
Description of the assignment and the scope of services delivered by the Bidder to the clients	
Description of the solution. Also indicate whether it is the same as the solution proposed to the bank	
Assignment Duration (in months)	
Assignment Start Date and End Date (Month & Year)	
Total No. of staff in the assignment	
Approximate value of contract (PKR or USD)	PKR / USD
Client Reference 1	Name: Designation: Address: Phone No. Mobile No. Email Address:
Client Reference 2	Name: Designation: Address: Phone No. Mobile No. Email Address:

Name: _____

Location: _____

Date: _____

_____
Company Seal & Bidder's Signature

FIRST WOMEN BANK LIMITED (FWBL)

Annexure C: Financial Bid Documentation

Financial Bid Cover Letter

Tender Reference No:
Date:

FWBL,
Head Office, Mezzanine Floor, STSM Foundation Building,
Civil Lines, Dr. Zia-ud-Din Ahmed Road,
Karachi, Pakistan

Dear Sir,

Sub: your RFP for "Implementation of SIEM Solution and 24/7 Security Operations Center" dated DD - MM-YYYY.

Having examined the RFP including all mention requirements, we, the undersigned, offer to deliver services in conformity with the said RFP and in accordance with our proposal and total cost indicated in the enclosed Commercial Bid for Implementation of SIEM Solution and 24/7 Security Operations Center mentioned in the RFP document.

All the prices mentioned in our bid are in accordance with the terms as specified in the bidding documents. We agree to abide by this bid for the period of 180 days from the date of bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in bidding documents.

If our bid is accepted, FWBL will retain BID Security (as requirement in RFP document and submitted along financial proposal) for a period of engagement (implementation phase) in favor of First Women Bank Ltd. for the due performance of the Contract.

Until a formal contract is prepared and executed, this bid, together with the bank's written acceptance thereof and bank's notification of award, shall constitute a binding Contract between us.

Dated this day of _____ 2022
Signature: (In the Capacity of) _____

Duly authorized to sign the tender offer for and on behalf of
Name: _____
Location: _____

_____
Company Seal & Bidder's Signature & Date

FIRST WOMEN BANK LIMITED (FWBL)

Financial Bid

Bidder's must use the following format to provide financial proposals:

Following format should be used for "**Managed Services**" financial proposal:

Item DESCRIPTION	COST (PKR)	APPLICABLE TAX (PKR)	Total Cost
One-time implementation services cost (if any)			
Annual Services Cost for Hosted SIEM Solution (as per requirements in this RFP)[a]			
Annual Services Cost for 24/7 SOC			
Total Bid Amount			

[a] In case technology solution provided by OEM is invoiced in a foreign currency, bidders must provide equivalent PKR value of this cost component. FWBL will issue a Purchase Order for the amount as proposed in financial proposal document, but will be subject to adjustment due to fluctuation in USD/PKR exchange rate every six months (from the date of Go Live). Please note that this adjustment will only be applicable to this cost component. All other quotations must be in PKR and not subject to any financial adjustment during the course of this contract.

Following format should be used for "**Hybrid Solution**" financial proposal:

Item DESCRIPTION	COST (PKR)	APPLICABLE TAX (PKR)	Total Cost
Commercial Bid For proposed SIEM Solution Licenses			
One-time implementation services cost			
Annual Services Cost for 24/7 SOC			
Annual Software SLA Support from OEM (which includes but not limited to OEM Incident support ,patches)[1]			
Implementation services SLA support post completion of GO Live warranty by bidder			
Total Bid Amount			

[1] In case OEM provides this quotation/invoice in a foreign currency, bidders may provide equivalent PKR value of this cost component. FWBL will use prevailing USD/PKR exchange rate at the time of issuance for the said purchase order. Please note that this adjustment will only be applicable to this cost component. All other quotations must be in PKR and not subject to any adjustment in financial proposal due to fluctuation in USD/PKR exchange rate.

Rates should be quoted in Pak Rupees and strictly as per the format illustrated above. Bids quoted in formats other than the illustrated format will be rejected. Applicable local taxes shall be paid over and above on actual basis on production of documentary evidence. Bank will not be making any other payment except those mentioned in the commercial bid.

In case, a single bidder is submitting a proposal for both "Managed Services" and "Hybrid Solution", then Bid Security must be calculated using higher of the two "Total Bid Amount" (as specified in table above)

Name: _____

Location: _____

_____
Company Seal & Bidder's Signature & Date