

Bid Evaluation Report**Procurement of Managed Security Service (MSS) for Security Operation Centre (SOC)**

1	Name of Procuring Agency	Sindh Bank Ltd.
2	Tender Reference No.	SNDB/COK/ADMIN/TD/1370/2024
3	Tender Description	Procurement of Managed Security Service (MSS) for Security Operation Centre (SOC)
4	Method of Procurement	Single Stage One Envelop Bidding Procedure
5	Tender Published & SPPRA S. No.	SPPRA S. No. T00531-23-0017 Express Tribune, Sindh Express, Daily Express (14/05/2024)
6	Total Bid Documents Sold	02
7	Total Bids Received	02
8	Technical/Financial Bid Opening Date	16/04/2024 Time: 11:30 Hours
9	No of Bid Technically Qualified	2
10	Bid(s) Rejected	0

S. No.	Name of Company	Cost Offered by Bidder	Ranking in Terms of Cost	Comparison with Estimated Cost (Rs.13,000,000/-)	Reason for Acceptance/ Rejection	Remarks
0	1	2	3	4	5	6
1	M/s Rewterz Information Security	Rs.10,699,992/-	1 st Lowest Bidder	Rs. 2,300,008/- Below with the estimated cost	Accepted Being the most advantageous bid	
2	M/s Trillium Information Security Systems	Rs.17,935,134/-	2 nd Lowest Bidder	Rs.4,935,134/- Above with the estimated cost	2 nd Lowest Qualified Bidder	

Note: Accordingly, going through the Technical/Financial evaluation criteria laid down in the tender document, M/s Rewterz Information Security is the most advantageous bid and hence recommended for Managed Security Service (MSS) for Security Operation Centre (SOC) to Sindh Bank Ltd.

Members – Procurement Committee

(Mr. Dilshad Hussain Khan) Chief Financial Officer – EVP – Chairperson

(Mr. Arshad Abbas Soomro) Head of Administration-SVP-Member

(Mr. Syed Muhammad Aqeel) Chief Manager, IDBL, KHI –AVP – Member

Signature

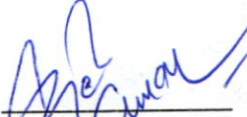
OFFICE ORDER


SUBJECT: EXTENSION FOR BID VALIDITY PERIOD


As per SPPRA Rule 38 (2), approval is solicited for further Ninety (90) days extension of "Bid Validity Period" for the following tender having SPPRA NIT ID No: **T00531-23-0017**


1. Procurement of Managed Security Service (MSS) for Security Operation Centre (SOC).

The reason for extension is M/s Rewterz Information Security is requested to extend the bid validity period to 90 days due to terms & Conditions are being discussed.


 S. Khurram Waheed
 AVP-II / IT Division


 Farhan a Siddiqui
 AVP-I/Admin Division


 Ather Iqbal
 VP-II/Admin Division


 S. Zeeshan ul Haq
 SVP/IT Division

Members – Procurement Committee

(Mr. Dilshad Hussain Khan) Chief Financial Officer – EVP – Chairperson

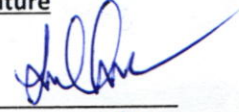
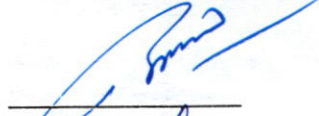
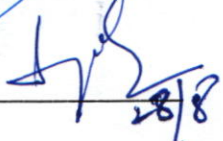
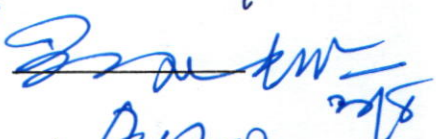
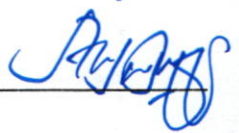
(Mr. Arshad Abbas Soomro) Head of Administration – SVP – Member

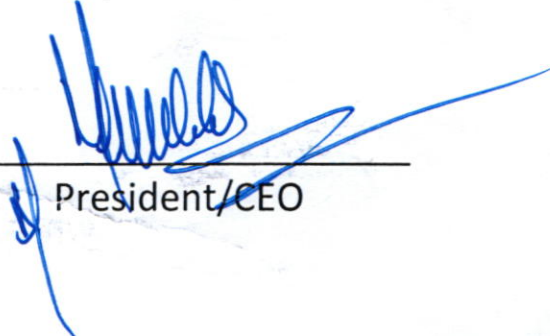
(Mr. Syed Muhammad Aqeel) Chief Manager, IDBL, KHI –AVP – Member

(Mr. Syed Assad Ali Shah) RGM Sindh-SEVP-Co-opted Member

(Mr. Syed Ata Hussain) EVP-I.T. Head- Co-opted Member

Signature


 President/CEO

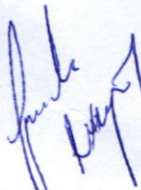
Bid Validity Extension

Dear Sir/Madam,

In reference to the bid security submitted to Sindh Bank against the tender “**Procurement of Managed Security Service (MSS) For Security Operation Centre (SOC)**”, Rewterz Information Security is requesting to grant us the extension of bid validity for another 90 days as the contract is still under review.

Looking forward to your corporation,

Regards,

 **REWTERZ**
Information Security

Areeba Najam
Manager Sales Operations
Rewterz Information Security

M/S Trillion Information Security System.

Scope of Work

Sindh bank is planning to acquire Security Operation Center (SOC) Services to improve its cyber security posture and fulfil its security requirements.

The bidder's team is required to accurately detect and prioritize threats, and provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents by consolidating log events and network flow data from the devices, and applications with the help of SIEM.

Bank is envisaging a resource-sharing model that will be an onsite monitoring services on a 24*7*365 basis offered by the vendor. Onsite service shall include deployment of resources as per demand of bank mentioned in schedule of requirement, at Sindh bank Head Office, Karachi.

The vendor should provide the following SOC related services by deploying their resources in Sindh bank, as per below details.

(The below details of activities to be performed by On- Premises deployed SOC Level 1/Level 2 / and Level 3 Engineers (as ongoing activity).

1. SOC Level 1 Engineer to be deployed in Sindh Bank Premises

SOC L1 Engineers should at least 2 Years of experience of SOC, having bachelor degree in relevant field.

The key responsibilities of L1 resource include but not limited to the following:

a. Monitoring and Analysis:


- i. Continuously monitor security alerts and events generated by SIEM Solutions/security systems.
- ii. Analyze security alerts and incidents to determine their severity and potential impact on the organization.

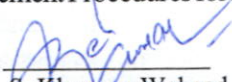
b. Incident Triage:

- i. Conduct initial triage of security incidents to assess the scope and urgency.
- ii. Classify and prioritize incidents based on predefined criteria.

c. Alert Handling:

- i. Respond to security alerts and incidents in a timely manner.
- ii. Execute Information Security Incident Management Procedures for handling common


Faraz Ahmed
VP/Admin. Div.


S. Khurram Waheed
AVP/ I.T. Division

MEMBERS PC-ADMIN

Head - Fin Div. _____

Head - Admin Div. _____

Head - IT/IRL. _____

security incidents.

d. Escalation:

- i. Escalate incidents to higher-level analysts or incident response teams as necessary.
- ii. Provide detailed and accurate information for escalated incidents.

e. Documentation:

- i. Maintain detailed and accurate records of all security incidents, including actions taken and outcomes.
- ii. Document incident handling as per Information Security Incident Management Procedures and contribute to knowledge base development.

f. Collaboration:

- i. Collaborate with other SOC team members to share information and insights.
- ii. Communicate effectively with relevant stakeholders during incident response.

g. Tool Utilization:

- i. Utilize available security tools and technologies to investigate and respond to incidents.
- ii. Report any issues or gaps in security tools to senior analysts for resolution.

h. Compliance Monitoring:

- i. Monitor security controls with respect to compliance with approved policies and regulations.
- ii. Report any deviations from compliance standards to senior analysts or management.

i. Shift Handover:

- i. Provide comprehensive shift handover to ensure smooth transitions between SOC shifts.
- ii. Share critical information with incoming analysts regarding ongoing incidents and noteworthy activities.

j. Basic Incident Mitigation:


- i. Help/Implement basic incident mitigation measures as per predefined procedures.
- ii. Follow established protocols for isolating affected systems or networks.

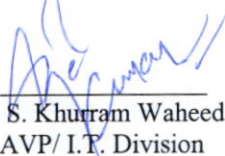
k. Threat Intelligence Process:

- i. Integrate threat intelligence feeds into daily monitoring activities.
- ii. Leverage threat intelligence to enhance incident analysis and response.

l. Adherence to Policies:

- i. Ensure adherence to security policies and procedures with respect to Security Incidences/Monitoring.
- ii. Report any policy violations or weaknesses to senior analysts and management.


Faraz Ahmed
VP/Admin. Div.

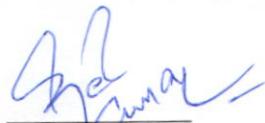

S. Khurram Waheed
AVP/ I.T. Division

MEMBERS PC-ADMIN
VIO n14 - 2021
VIO n1m5A - 2021
J2021...

M/s Trillion Information Security Systems.

Eligibility Criteria

S. No.	Requisite	*Evidence required to be attached	Compliance / Proof	
1	Minimum Three (03) Years in business in the relevant field	Letter of Incorporation / Company Registration Letter / Letter or Declaration of Commencement of Business / NTN. (attach as Annexure "1")	✓ Yes	No
2	Turn Over in last Three (03) Years should be at least 50 million	Audit Report / Tax Return (attach as Annexure "2")	✓ Yes	No
3	Registration with Income Tax , SRB and Sales Tax	NTN , SRB & GST Certificates (attach as Annexure "3")	✓ Yes	No
4	Bidder must be providing 24x7x365 days on-site/offsite SOC service to at least three (03) Banks in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate (attach as Annexure "4")	✓ Yes	No
5	Bidder must be providing 24x7x365 days on-site/offsite SOC and Cyber security consultancy services in Pakistan for at least three (03) years	Attach Documentary Evidence/Certificate (attach as Annexure "5")	✓ Yes	No
✓ Qualified / Disqualified				


S. Khurram Waheed
AVP/ I.T. Division.

on Leave
Hassan Raza
VP/ Finance Division

Syed Zeeshan-ul-Haq
SVP/ I.T. Division


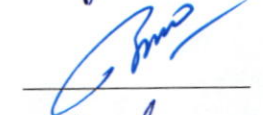
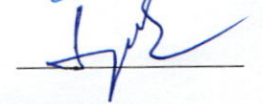
Members – Procurement Committee

(Mr. Dilshad Hussain Khan) Chief Financial Officer – EVP – Chairperson

(Mr. Arshad Abbas Soomro) Head of Administration-SVP-Member

(Mr. Syed Muhammad Aqeel) Chief Manager, IDBL, KHI –AVP – Member

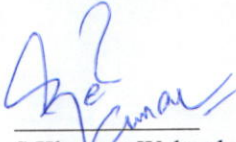
Signature

M/S Reuters Information Security

Eligibility Criteria

S. No.	Requisite	*Evidence required to be attached	Compliance / Proof	
1	Minimum Three (03) Years in business in the relevant field	Letter of Incorporation / Company Registration Letter / Letter or Declaration of Commencement of Business / NTN. (attach as Annexure "1")	Yes	No
2	Turn Over in last Three (03) Years should be at least 50 million	Audit Report / Tax Return (attach as Annexure "2")	Yes	No
3	Registration with Income Tax , SRB and Sales Tax	NTN , SRB & GST Certificates (attach as Annexure "3")	Yes	No
4	Bidder must be providing 24x7x365 days on-site/offsite SOC service to at least three (03) Banks in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate (attach as Annexure "4")	Yes	No
5	Bidder must be providing 24x7x365 days on-site/offsite SOC and Cyber security consultancy services in Pakistan for at least three (03) years	Attach Documentary Evidence/Certificate (attach as Annexure "5")	Yes	No
Qualified / Disqualified				


S. Khurram Waheed
AVP/ I.T. Division.

on Leave
Hassan Raza
VP/ Finance Division

Syed Zeeshan-ul-Haq
SVP/ I.T. Division


Members – Procurement Committee


(Mr. Dilshad Hussain Khan) Chief Financial Officer – EVP – Chairperson

(Mr. Arshad Abbas Soomro) Head of Administration-SVP-Member

(Mr. Syed Muhammad Aqeel) Chief Manager, IDBL, KHI –AVP – Member

Signature





MINUTES OF THE OPENING OF THE TENDER (TECHNICAL / FINANCIAL PHASE)

TYPE OF PROCUREMENT ADMIN / IT / CONSULTANT / MEDIA
 TENDER NAME Procurement of managed security service (MSS)
 for security operations center (SOC)
 TYPE OF TENDER SINGLE STAGE-ONE ENVELOPE / SINGLE STAGE-TWO ENVELOPE / TWO STAGE / TWO STAGE-TWO ENVELOPE
 OPENING DATE 14-5-2024
 OPENING TIME 1130 Hours

ATTENDANCE (MEMBER PC)

TYPE
 TEN
 YR

ATTENDANCE (REPS. OF BIDDERS)	NAME	FIRM	BID OFFERED
		① Jullian	R 17935134/-
		② Kenters	R 10699992/-
TOTAL BIDS ACCEPTED FOR EVALUATION	#02		
TOTAL BIDS REJECTED			
MOS			

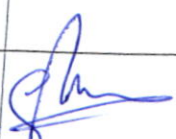
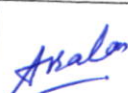
SIGNATURE MEMBERS PC-ADMIN
 Head - Fin Div. _____
 Head - Admin Div. _____
 Member-IDBL. _____
 Date: _____

ATTENDANCE SHEET

BID OPENING -

FOR SELECTION OF Procurement of Managed Security Service (MSS)
for Security - operation Centre (SOC)

Date: 14-5-2024

S.No	Company Name	Name of Company Representative	Contact No.	Company Address	Signature
1	Trillium	Shasheev	0323-2665457	Meezan bank, Ppsc branch, 101/102 7th, 8th floor	
2	Reentrez	FAISAL ARSALAN	0314-2126917	Asia Pacific Trade Center 3rd floor.	

Signature - Procurement Committee Members

Head of Administration

Chief Financial Officer

Chief Manager (IDBL)





Price Schedule

Sr NO	Item	Cost per Month in Pak Rs. (Including all govt taxes)	No of Months	Total yearly Amount in Pak Rs. (Including all govt taxes)
1	Procurement of Managed Security Service (MSS) for Security Operation Center (SOC)	891,666	12	10,699,992

SIGNATURE MEMBERS PC-ADMIN

Head - Fin Div. _____

Head - Admin Div. _____

Member-IDBL. _____

Date: _____

REWTERZ
Information Security

1. Services - Prices

SIGNATURE MEMBERS PC-ADMIN

Head - Fin Div. _____

Head - Admin Div. _____

Member-IDBL. _____

Date: _____

PRICE SCHEDULE

(Applicable for the year 2024-2025)

Name of Bidder: Trillium Information Security Systems

S. No	Item	Cost Per Month in Pak Rs. (Including all govt taxes)	No. of months	*Total yearly Amount in Pak Rs. (Including all govt taxes)
01	Procurement of Managed Security Service (MSS) For Security Operation Center (SOC)	1,356,000	12	16,272,000

VA/PT Tools

S. No	Item	Cost Per Month in Pak Rs. (Including all govt taxes)	No. of months	*Total yearly Amount in Pak Rs. (Including all govt taxes)
01	Burp Suit Professional – 01 Year Subscription	N/A	12	194,134
02	Nexpose Subscription - Licensed for number of assets: 128 IPs	N/A	N/A	1,469,000

Total = 17935134

2. Terms & Conditions:

- Prices above are in PKR valid for 90 days from the date of this proposal.
- Project Plan and Activity start date will be shared after issuance of PO.
- Payment Terms- proposed below or TBD mutually:
 - 50% at the time of project initiation
 - 50% after completion of 06 Months



Scope of Work

Sindh bank is planning to acquire Security Operation Center (SOC) Services to improve its cyber security posture and fulfil its security requirements.

The bidder's team is required to accurately detect and prioritize threats, and provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents by consolidating log events and network flow data from the devices, and applications with the help of SIEM.

Bank is envisaging a resource-sharing model that will be an onsite monitoring services on a 24*7*365 basis offered by the vendor. Onsite service shall include deployment of resources as per demand of bank mentioned in schedule of requirement, at Sindh bank Head Office, Karachi.

The vendor should provide the following SOC related services by deploying their resources in Sindh bank, as per below details.

(The below details of activities to be performed by On- Premises deployed SOC Level 1/Level 2 / and Level 3 Engineers (as ongoing activity).

1. SOC Level 1 Engineer to be deployed in Sindh Bank Premises

SOC L1 Engineers should at least 2 Years of experience of SOC, having bachelor degree in relevant field.

The key responsibilities of L1 resource include but not limited to the following:

a. **Monitoring and Analysis:**


- i. Continuously monitor security alerts and events generated by SIEM Solutions/security systems.
- ii. Analyze security alerts and incidents to determine their severity and potential impact on the organization.

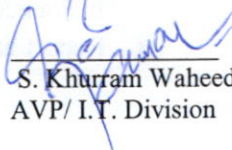
b. **Incident Triage:**

- i. Conduct initial triage of security incidents to assess the scope and urgency.
- ii. Classify and prioritize incidents based on predefined criteria.

c. **Alert Handling:**

- i. Respond to security alerts and incidents in a timely manner.
- ii. Execute Information Security Incident Management Procedures for handling common


Faraz Ahmed
VP/Admin. Div.


S. Khurram Waheed
AVP/ I.T. Division

SIGNATURE MEMBERS PC-ADMIN

Head - Fin Div. _____

Head - Admin Div. _____

Member-IDBL. _____

Date: _____

security incidents.

d. Escalation:

- i. Escalate incidents to higher-level analysts or incident response teams as necessary.
- ii. Provide detailed and accurate information for escalated incidents.

e. Documentation:

- i. Maintain detailed and accurate records of all security incidents, including actions taken and outcomes.
- ii. Document incident handling as per Information Security Incident Management Procedures and contribute to knowledge base development.

f. Collaboration:

- i. Collaborate with other SOC team members to share information and insights.
- ii. Communicate effectively with relevant stakeholders during incident response.

g. Tool Utilization:

- i. Utilize available security tools and technologies to investigate and respond to incidents.
- ii. Report any issues or gaps in security tools to senior analysts for resolution.

h. Compliance Monitoring:

- i. Monitor security controls with respect to compliance with approved policies and regulations.
- ii. Report any deviations from compliance standards to senior analysts or management.

i. Shift Handover:

- i. Provide comprehensive shift handover to ensure smooth transitions between SOC shifts.
- ii. Share critical information with incoming analysts regarding ongoing incidents and noteworthy activities.

j. Basic Incident Mitigation:

- i. Help/Implement basic incident mitigation measures as per predefined procedures.
- ii. Follow established protocols for isolating affected systems or networks.

k. Threat Intelligence Process:

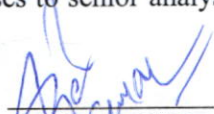
- i. Integrate threat intelligence feeds into daily monitoring activities.
- ii. Leverage threat intelligence to enhance incident analysis and response.

l. Adherence to Policies:

- i. Ensure adherence to security policies and procedures with respect to Security Incidences/Monitoring.
- ii. Report any policy violations or weaknesses to senior analysts and management.



Faraz Ahmed
VP/Admin. Div.



S. Khurram Waheed
AVP/I.T. Division

MEMBERS PC-ADMIN
Lead - Fin Div.
Lead - Admin Div.
Member-ITSL
Date: