

SINDH PUBLIC PROCUREMENT REGULATORY AUTHORITY

CONTRACT EVALUATION FORM

TO BE FILLED IN BY ALL PROCURING AGENCIES FOR PUBLIC CONTRACTS OF WORKS, SERVICES & GOODS

- 1) NAME OF THE ORGANIZATION / DEPTT. SINDH BANK LIMITED/ADMINISTRATION
- 2) PROVINCIAL / LOCAL GOVT./ OTHER SCHEDULED BANK
- 3) TITLE OF CONTRACT Procurement of SIEM / Log Management System
- 4) TENDER NUMBER SNDB/COK/ADMIN/T/1173/2020
- 5) BRIEF DESCRIPTION OF CONTRACT Same as Above
- 6) FORUM THAT APPROVED THE SCHEME Competent Authority
- 7) TENDER ESTIMATED VALUE Rs. 25,000,000/-
- 8) ENGINEER'S ESTIMATE
(For civil works only) -
- 9) ESTIMATED COMPLETION PERIOD (AS PER CONTRACT) 03 Years
- 10) TENDER OPENED ON (DATE & TIME) 18/09/2020 At 1100 Hours
- 11) NUMBER OF TENDER DOCUMENTS SOLD 03
(Attach list of buyers)
- 12) NUMBER OF BIDS RECEIVED 03
- 13) NUMBER OF BIDDERS PRESENT AT THE TIME OF OPENING OF BIDS 02
- 14) BID EVALUATION REPORT
(Enclose a copy) 02/10/2020 Attached
- 15) NAME AND ADDRESS OF THE SUCCESSFUL BIDDER M/s Trillium Information Systems
5th Floor, AWT Plaza, S-7th Street
Mall, Kamalpur
- 16) CONTRACT AWARD PRICE Rs.15,563,510/-
- 17) RANKING OF SUCCESSFUL BIDDER IN EVALUATION REPORT
(i.e. 1st, 2nd, 3rd EVALUATION BID).
1) M/s.Trillium Information Security Sytems (Pvt) Ltd
2) Systems Limited

18) METHOD OF PROCUREMENT USED :- (Tick one)

- a) SINGLE STAGE – ONE ENVELOPE PROCEDURE ☒ Domestic/ Local
- b) SINGLE STAGE – TWO ENVELOPE PROCEDURE ☐
- c) TWO STAGE BIDDING PROCEDURE ☐
- d) TWO STAGE – TWO ENVELOPE BIDDING PROCEDURE ☐

PLEASE SPECIFY IF ANY OTHER METHOD OF PROCUREMENT WAS ADOPTED i.e.
EMERGENCY, DIRECT CONTRACTING ETC. WITH BRIEF REASONS:

19) APPROVING AUTHORITY FOR AWARD OF CONTRACT COMPETENT AUTHORITY

20) WHETHER THE PROCUREMENT WAS INCLUDED IN ANNUAL PROCUREMENT PLAN?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

21) ADVERTISEMENT :

i) SPPRA Website
(If yes, give date and SPPRA Identification No.)

Yes	SPPRA S. No: T00531-20-0004
No	

ii) News Papers
(If yes, give names of newspapers and dates)

Yes	Express Tribune, Daily Express & Sindh <i>Express</i> 18/09/2020
No	

22) NATURE OF CONTRACT

Domestic/ Local	<input checked="" type="checkbox"/>	Int.	<input type="checkbox"/>
--------------------	-------------------------------------	------	--------------------------

23) WHETHER QUALIFICATION CRITERIA
WAS INCLUDED IN BIDDING / TENDER DOCUMENTS?
(If yes, enclose a copy)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

24) WHETHER BID EVALUATION CRITERIA
WAS INCLUDED IN BIDDING / TENDER DOCUMENTS?
(If yes, enclose a copy)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

25) WHETHER APPROVAL OF COMPETENT AUTHORITY WAS OBTAINED FOR USING A
METHOD OTHER THAN OPEN COMPETITIVE BIDDING?

Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
-----	--------------------------	----	-------------------------------------

26) WAS BID SECURITY OBTAINED FROM ALL THE BIDDERS?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

27) WHETHER THE SUCCESSFUL BID WAS LOWEST EVALUATED
BID / BEST EVALUATED BID (in case of Consultancies)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

28) WHETHER THE SUCCESSFUL BIDDER WAS TECHNICALLY
COMPLIANT?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

29) WHETHER NAMES OF THE BIDDERS AND THEIR QUOTED PRICES WERE READ OUT AT
THE TIME OF OPENING OF BIDS?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

30) WHETHER EVALUATION REPORT GIVEN TO BIDDERS BEFORE THE AWARD OF
CONTRACT?
(Attach copy of the bid evaluation report)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

31) ANY COMPLAINTS RECEIVED
(If yes, result thereof)

Yes	
No	No

32) ANY DEVIATION FROM SPECIFICATIONS GIVEN IN THE TENDER NOTICE / DOCUMENTS
(If yes, give details)

Yes	
No	No

33) WAS THE EXTENSION MADE IN RESPONSE TIME?
(If yes, give reasons)

Yes	
No	No

34) DEVIATION FROM QUALIFICATION CRITERIA
(If yes, give detailed reasons.)

Yes	
No	No

35) WAS IT ASSURED BY THE PROCURING AGENCY THAT THE SELECTED FIRM IS NOT
BLACK LISTED?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

36) WAS A VISIT MADE BY ANY OFFICER/OFFICIAL OF THE PROCURING AGENCY TO THE
SUPPLIER'S PREMISES IN CONNECTION WITH THE PROCUREMENT? IF SO, DETAILS TO
BE ASCERTAINED REGARDING FINANCING OF VISIT, IF ABROAD:
(If yes, enclose a copy)

Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
-----	--------------------------	----	-------------------------------------

37) WERE PROPER SAFEGUARDS PROVIDED ON MOBILIZATION ADVANCE PAYMENT IN
THE CONTRACT (BANK GUARANTEE ETC.)?

Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
-----	--------------------------	----	-------------------------------------

38) SPECIAL CONDITIONS, IF ANY
(If yes, give Brief Description)

Yes	
No	No

39) Date of Award of Contract: 31/12/2020

Signature & Official Stamp of
Authorized Officer

FOR OFFICE USE ONLY

Lt Col (R) Shahzad Begg
EVP/Head of Administration
SINDH BANK LIMITED

SPPRA, Block. No.8, Sindh Secretariat No.4-A, Court Road, Karachi

Tele: 021-9205356; 021-9205369 & Fax: 021-9206291

Print

Save

Reset

Procurement of SIEM / LOG Management System (1173/2020)					
S.NO	COMPANY NAME	AMOUNT (Rs)	PAY ORDER NO	NAME OF BANK	
01	Trillium	300	00260046	Askari Bnak	
02	System Limited	300	14193672	Habib Metropolitan Bank Ltd	
03	Siliconst (Pvt.) Ltd	300	04613029	Askari Bnak	
Total			900/-		

PURCHASE ORDER

PO No: 199

Date: 03-12-2020

M/s Trillium Information Security System,
10th Floor, AWT Plaza,
5 The Mall,
Rawalpindi,
Pakistan.

Subject: Procurement of SIEM/LOG Management System

Dear Sir,

With reference to the Tender Bid SNDB/COK/ADMIN/TD/1173/2020 dated 01-09-2020 for Procurement of **SIEM/LOG Management System**, submitted by you in Sindh Bank Ltd. After detail review the Sindh Bank Ltd management is pleased to inform that your Tender Bid is accepted.


Kindly proceed as per tender document. Further detail is as follows.


S. No	Product	Total Price (PKR) (Including All Taxes)
1	IBM QRadar Software/Licenses-Initial One Year	7,130,117/-
2	Professional Services -Implementation/Support Including 1x Resident Engineer for 1 Year/Local Training-Initial One Year	1,582,000/-
3	Hardware	2,000,000/-
	Total -Initial One Year	10,712,117/-
Subject to Extension of Agreement on mutual consent of both parties prices of subsequent years are as follows		
1	2 nd Year SLA (Software/Local Support including x Resident Engineer)	2,348,335/-
2	3 rd Year SLA (Software/Local Support including x Resident Engineer)	2,503,058/-
	Total	4,851,393/-
	Grand Total	15,563,510/-


Terms & Conditions

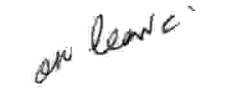
Payment Terms as per Agreement

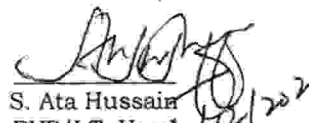
Thanks,


M. Rashid Memon
VP-I/I.T. Division


S. Zeeshan-ul-Haq
SVP-II/ I.T. Division


Naeem Muhammad
SVP-I/ CISO RM Division


Riaz Ahmed
SVP-I/I.T. Division


S. Ata Hussain
EVP/I.T. Head

SINDH BANK LIMITED
HEAD OFFICE:
3rd FLOOR, FEDERATION HOUSE,
ABDULLAH SHAH GHAZI ROAD,
CLIFTON, KARACHI-75600, PAKISTAN

UAN : +92-21-111-333-255
PHONE : +92-21-35829394
FAX : +92-21-35870543
WEB : www.sindhbankltd.com

یہ سہا : +92-21-111-333-255
فون : +92-21-358 29394
فیکس : +92-21-358 40543

سندھ بینک لمیٹڈ
ہیڈ آفس، تیسری منزل، فیڈریشن ہاؤس،
عبداللہ شاہ غازی روڈ، کلکشن، کراچی-75600 - پاکستان

Technical & Financial Proposals Evaluation Report		
Procurement of SIEM/Log Management System		
1	Name of Procuring Agency	Sindh Bank Ltd.
2	Tender Reference No.	SNDB/COK/ADMIN/TD/1173/2020
3	Tender Description	Procurement of SIEM/Log Management System
4	Method of Procurement	Single Stage One Envelop Bidding Procedure
5	Tender Published	SPPRA S. No. T00531-20-0004
6	Total Bid Documents Sold	03
7	Total Bids Received	03
8	Technical Bid Opening Date	18/09/2020
9	Financial Bid Opening Date	18/09/2020
10	No of Bid Technically Qualified	02
11	Bid(s) Rejected	01

S. No.	Name of Company	Cost Offered by Bidder	Ranking in Terms of Cost	Comparison with Estimated Cost (Rs.25,000,000/-)	Reason for Acceptance/ Rejection	Remarks
0	1	2	3	4	5	6
1	M/s Trillium Information Security Systems (Pvt) Ltd	Rs.15,563,510/-	1 st Lowest Bidder	Rs.9,436,490/- Below with the estimated cost	Accepted Being the 1 st Lowest Qualified Bidder	
2	M/s Systems Limited	Rs.22,488,066/-	2 nd Lowest Bidder	Rs.2,511,934/- Below with the estimated cost	2nd Lowest Qualified Bidder	
3	M/s Siliconst Private Ltd	Rs.41,585,418	Disqualified	Disqualified	Evaluation Criteria Not Fulfilled	

Note: M/s Trillium Information Security Systems (Pvt) Ltd is selected for the Procurement of SIEM/Log Management System to Sindh Bank Limited being the 1st Lowest Qualified Bidder.

Members – Procurement Committee

(Mr. Saeed Jamal) Chief Financial Officer – EVP – Chairperson

(Col. Shahzad Begg) Head of Administration – EVP – Member

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

Signature

Eligibility Criteria

S. No.	Requisite	*Evidence required to be attached	Compliance / Proof	
1	Minimum 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 3 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	The proposed solution / product in the bid must be currently used by atleast three Bank in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate (attach as Annexure "4")	Yes	No
5	The proposed solution / product must be currently deployed by the vendor atleast in two Bank in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate (attach as Annexure "5")	Yes	No
Qualified / Disqualified				

ELIGIBILITY CRITERIA NOTE

1. There can be subsequent clarification to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd & SPPRA websites regularly.
2. Attachment of relevant evidence in eligibility criteria is mandatory. In case of non-provision of evidence in any of the requisite, bidder will be disqualified

MANDATORY

1. GST/Income Tax Registration/Sindh Revenue Board.
2. Attachment of Affidavit (specimen attached as Annexure "H") on stamp paper from the owner of the company.
3. Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
4. Writing of tender reference as given in the NIT on the Envelop, carrying tender document is must or the bank will not be responsible if the documents are not received by the Procurement Committee on time

DISQUALIFICATION

The bidder will be considered disqualified during technical/financial evaluation process or after award contract if:

1. On black list of SPPRA & Sindh Bank Ltd.
2. Issued with two (2) warning letters/emails by the Sindh Bank Ltd in the past to the bidder for unsatisfactory performances.
3. Not GST/Income Tax Registered.
4. Alternate bid is offered.
5. Non - Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
6. The qualified bidder sublets the contract in any form/stage to any other agency.
7. The tender is deposited without Tender Fee.
8. Warranty of supplied items is less than 1 year.
9. In Eligibility Criteria, a single non-compliance of a requisite will make the bidder disqualify.
(Single Stage-One Envelope Procedure).
10. If during verification process of the client list the response by any of the bank is unsatisfactory/on account on account of previous performance.

Taimoor Ghousi
AVP/ Finance Division,

Ahsan Ali
VP/ Operations Div

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

Eligibility Criteria

System Ltd

S. No.	Requisite	*Evidence required to be attached	Compliance / Proof	
1	Minimum 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 3 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	The proposed solution / product in the bid must be currently used by atleast three Bank in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate (attach as Annexure "4")	Yes	No
5	The proposed solution / product must be currently deployed by the vendor atleast in two Bank in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate (attach as Annexure "5")	Yes	No
Qualified / Disqualified				

ELIGIBILITY CRITERIA NOTE

- There can be subsequent clarification to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd & SPPRA websites regularly.
- Attachment of relevant evidence in eligibility criteria is mandatory. In case of non-provision of evidence in any of the requisite, bidder will be disqualified

MANDATORY

- GST/Income Tax Registration/Sindh Revenue Board.
- Attachment of Affidavit (specimen attached as Annexure "H") on stamp paper from the owner of the company.
- Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
- Writing of tender reference as given in the NIT on the Envelope, carrying tender document is must or the bank will not be responsible if the documents are not received by the Procurement Committee on time

DISQUALIFICATION

The bidder will be considered disqualified during technical/financial evaluation process or after award contract if:

- On black list of SPPRA & Sindh Bank Ltd.
- Issued with two (2) warning letters/emails by the Sindh Bank Ltd in the past to the bidder for unsatisfactory performances.
- Not GST/Income Tax Registered.
- Alternate bid is offered.
- Non - Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
- The qualified bidder sublets the contract in any form/stage to any other agency.
- The tender is deposited without Tender Fee.
- Warranty of supplied items is less than 1 year.
- In Eligibility Criteria, a single non-compliance of a requisite will make the bidder disqualify.
(Single Stage-One Envelope Procedure).
- If during verification process of the client list the response by any of the bank is unsatisfactory on account on account of previous performance.

Taimoor Ghausi
AVP/ Finance Division.

Ahsan Ali
VP/ Operations Div

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

SINDH PUBLIC PROCUREMENT REGULATORY AUTHORITY

CONTRACT EVALUATION FORM

TO BE FILLED IN BY ALL PROCURING AGENCIES FOR PUBLIC CONTRACTS OF WORKS, SERVICES & GOODS

- 1) NAME OF THE ORGANIZATION / DEPTT. SINDH BANK LIMITED/ADMINISTRATION
- 2) PROVINCIAL / LOCAL GOVT./ OTHER SCHEDULED BANK
- 3) TITLE OF CONTRACT Procurement of SIEM / Log Management System
- 4) TENDER NUMBER SNDB/COK/ADMIN/T/1173/2020
- 5) BRIEF DESCRIPTION OF CONTRACT Same as Above
- 6) FORUM THAT APPROVED THE SCHEME Competent Authority
- 7) TENDER ESTIMATED VALUE Rs. 25,000,000/-
- 8) ENGINEER'S ESTIMATE
(For civil works only) -
- 9) ESTIMATED COMPLETION PERIOD (AS PER CONTRACT) 03 Years
- 10) TENDER OPENED ON (DATE & TIME) 18/09/2020 At 1100 Hours
- 11) NUMBER OF TENDER DOCUMENTS SOLD 03
(Attach list of buyers)
- 12) NUMBER OF BIDS RECEIVED 03
- 13) NUMBER OF BIDDERS PRESENT AT THE TIME OF OPENING OF BIDS 02
- 14) BID EVALUATION REPORT
(Enclose a copy) 02/10/2020 Attached
- 15) NAME AND ADDRESS OF THE SUCCESSFUL BIDDER M/s. Trillium Information Systems
1st Floor, AWT Plaza, S-ghy UMD
Mall, Karachi
- 16) CONTRACT AWARD PRICE Rs.15,563,510/-
- 17) RANKING OF SUCCESSFUL BIDDER IN EVALUATION REPORT
(i.e. 1st, 2nd, 3rd EVALUATION BID).
1) M/s.Trillium Information Security Systems (Pvt) Ltd
2) Systems Limited

18) METHOD OF PROCUREMENT USED : - (Tick one)

- a) SINGLE STAGE – ONE ENVELOPE PROCEDURE ☒ Domestic/ Local
- b) SINGLE STAGE – TWO ENVELOPE PROCEDURE ☐
- c) TWO STAGE BIDDING PROCEDURE ☐
- d) TWO STAGE – TWO ENVELOPE BIDDING PROCEDURE ☐

PLEASE SPECIFY IF ANY OTHER METHOD OF PROCUREMENT WAS ADOPTED i.e. EMERGENCY, DIRECT CONTRACTING ETC. WITH BRIEF REASONS:

1/3

9. In Eligibility Criteria, a single non-compliance of a requisite will make the bidder disqualify.
(Single Stage-One Envelope Procedure).
10. If during verification process of the cliental list the response by any of the bank is un satisfactory on account on account of previous performance.
- Taimoor Ghausi
AVP/ Finance Division.
- Ahsan Ali
VP/ Operations Div.
- Syed Zeeshan-ul-Haq
SVP/ I.T. Division

SIGNATURE MEMBERS PC-ADMIN
 FINANCIAL PROPOSAL Fin Div. _____
PRICE SCHEDULE Head - Admin Div. _____
 (Applicable for the year 2020-21) Member-IDBL. _____

Name of Bidder Trillium Information Security Systems

Date: _____

Serial #	Description	One Time Cost (A)- Year1	Recurring Charges- Year 2 & Year 3 (B)
1	Procurement of SIEM/Log Management System	PKR 10,712,117	PKR 4,851,393
*Total Amount = One Time Cost -Year 1 (A) + Recurring Charges(B) – Year 2 & Year 3			PKR 15,563,510

Note: The lowest bid will be calculated as per the formula above. However initial contract will be given for one year only, which may be extended mutually as per SPPRA Rule.

Terms & Conditions

- Prices quoted above valid for 90 days after date of bid opening i.e. 18 September 2020.
- Detailed BOQ and price breakup is also attached with the financial proposal. Payment milestone proposed on detailed BOQ/price breakup.
- Prices do not include any taxes that may become applicable after the date of submission of proposal
- Project Timelines (Delivery/Implementation/Operational Acceptance): 6 months or earlier line with tender requirements.
- Pre-required software (if applicable) necessary to operate the quoted solution shall be provided by Sindh Bank
- The support/subscription/warranty period of IBM Software shall commence from the date of order processed in IBM systems and not after Operational Acceptance in line with IBM policy
- **Payment Term – Initial One Year:**
 1. IBM Software: 100% to be made on delivery of IBM Proof of Entitlement
 2. Hardware: 100% to be made on Delivery
 3. Implementation: 100% to be made on implementation completion
 4. Resident Engineer/Local Support: 100% to be made on start of resident engineer services
 5. Training (If Applicable): 100% to be made on completion of training
- **Payment Term – Subsequent Year SLA:**
 1. IBM Software: 100% to be made on delivery of renewal Proof of Entitlement
 2. Resident Engineer/Local Support: 100% on delivery renewal Proof of Entitlement



SIGNATURE MEMBERS PC-ADMIN

Head - Fin Div.

Head - Admin Div.

Member-IDBL

4 FINANCIAL PROPOSAL

PRICE SCHEDULE

(Applicable for the year 2020-21) Date: _____

Name of Bidder SILICONST PVT LTD

S #	Description	One Time Cost (In Pak Rupee) (A)	Monthly Recurring Charges (In Pak Rupee) (B)
1	Procurement of SIEM/Log Management System	-	1,155,151.00
	*Total Amount = One Time Cost (A) + Monthly Recurring Charges(B) x 36 (In Pak Rupee)	41,585,418.00	

Note: The lowest bid will be calculated as per formula above. However initial contract will be given for one year only, which may be extended mutually as per SPPRA Rule.

*This Total Amount will be taken as price offered by the vendor.

Note

- In case of over writing/cutting/use of Blanco is found in the Financial Bid document, the bid will be taken as null & void however if the figures are readable and are also duly signed only then, bid will be accepted.
- If the item is not provide/installed on due date (date given on supply order) a fine of Rs.500/-per day will be deducted from the bill.
- The cost must include all taxes, stamp duty (as applicable under Stamp Act 1989) duly stamped on the contract agreement, installation, commissioning, transportation and labour charges.
- No advance payment for the supply of equipment will be made, bills are only be processed for necessary payment on receipt of certificate of delivery/satisfaction from the concerned officer.
- Calculation of bid security, 5% of the *(Total Amount) will be submitted with the tender document as bid security in shape of Pay Order/Demand Draft /Bank Guarantee in favour of Sindh Bank Ltd.
- The successful bidder will be the one whose total sum of cost is the lowest. As it is package tender, so no partial lowest cost will be considered for award of any work.
- The tender will be considered cancelled if the contract agreement/performance security after due signature are not submitted with Admin Office after 5 days of completion of bid evaluation report hoisting period (7 days) on SPPRA website.
- The Tender will stand cancelled if the item are not supply/installed within 8 weeks of issue of supply order.
- In case financial bids are the same, the successful bidder will be the one who has highest turnover of the two.
- If the obligation of warranty period are not met or delayed, the repair etc. requirement on this account will be carried out by the bank & the billed amount will be deducted from the performance security/ upcoming payment due to supplier. Risk & subsequent cost to this effect if any will be liability of the vendor and any subsequent expenses on the equipment will also be borne by the supplier.
- Qualified company will also be bound to sign a bond/undertaking that in case of any observation arising in respect of quality of the equipment within the warranty period, the company will be liable to address it at his own cost, non- compliance of the same will result into initiation of a case against the company for non-commitment.
- All terms & conditions of the Contract Agreement (Annexure "G") are part of tender document.
- The tender will stand cancelled if any of the given condition of the tender is not met in strictly as per the requisite of the tender document.
- Pre Bid Meeting: Within one week (For Any Clarification)
- Note: There can be subsequent clarification to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd. & SPPRA website regularly.
- Payment will be made in Pak Rupee.

Signature & Stamp of Bidder

[Signature]



This document contains 59 pages



SIGNATURE MEMBERS PG ADMIN
 Head - Fin Div. [Signature] syst
 Head - Admin Div. [Signature]
 Member-IDBL. [Signature]

2 Price Schedule

(Applicable for the Year 2020-2021)

Name of the Bidder: Systems Limited

S #	Description	One Time Cost (in Pak Rupee) (A)	Monthly Recurring Charges (in Pak Rupee) (B)
Procurement of SIEM/Log Management System			
1.	SIEM Software Licenses		
1.1	SIEM Software Licenses (1 st year) – 12 Month Subscription	7,016,215	
1.2	SIEM Software Licenses (2 nd and 3 rd year)		142,840
2.	SIEM Implementation Cost	1,617,075	
3.	01 Certified and skilled resident engineer/SLA – 01 Year Cost **	3,293,143	
4.	OEM accredited training for 5 resources (system/solution operation management, security analyst and Cyber SOC management) – Virtual Learning	Free of Cost (FOC)	
5.	Hardware Cost with 3 Year Standard Warranty	7,133,473	
	Sum of Respective One time & recurring cost (2 nd and 3 rd year)	19,059,906	142,840 X 24 Months = 3,428,160
	*Total Amount = One Time Cost (A) + Monthly Recurring Charges(B) x 36 { Calculated as A+ (1.1Bx12)+(1.2Bx24) } (In Pak Rupee)		22,488,066

** - If SLA is preferred and resident engineer is not required then the price for Yearly SLA would be PKR 4,644,000 – Inclusive of Taxes with Quarterly Payment Terms

Circular

SNDB/CO/ADMIN/BIDDING/CIRC/1173/2020

Date: 18-09-2020

Opening of Tender for Selection of Procurement of SIEM/LOGS Management
System

Bidders have been called upon to participate for the subject purpose. Members of the procurement committee are requested to attend the event as per the given schedule:

Bid Opening Date: 18-09-2020

Bid Opening Time: 11:00 Hours

Venue : Board Room

Ather Iqbal
Ather Iqbal
Incharge Procurement

Signature –Procurement Committee Members

Head of Administration

Chief Financial Officer

Chief Manager (IDBL)

[Signature]
[Signature]
[Signature]

ATTENDANCE SHEET
BID OPENING -

FOR SELECTION OF Procurement of SEM/COO Management System

Date: 18-09-2020

S.No	Company Name	Name of Company Representative	Contact No.	Company Address	Signature
01	System limited				
02	Tritium	Hameed Shams	0331-2623799	10th Floor - AWT PLAZA, Mall Road Rawalpindi	
03	Silicon Systems Global International (Pvt) Ltd	DANISH KHAAN	0313-2415393	77-D/2, Lahore Centre, Lahore	

Signature - Procurement Committee Members

Head of Administration

Chief Financial Officer

Chief Manager (IDBL)

OPENING OF BID
 FINANCIAL PROPOSALS

FOR SELECTION OF Procurement of SIEM / LOG Management System

Date: 18-09-2020

S.No	Company Name	Total Bid Offered		Signature of Company Representative	Remarks
		Announced	Evaluated		
01	System Limited	Rs. 22,488,066/-			
02	Trillium	Rs. 15,533,570/-		<i>[Signature]</i>	
03	Siliconet Rayn Centel International (Pvt) Ltd.	Rs. 41,585,418/-		<i>[Signature]</i>	

Signature –Procurement Committee Members

Head of Administration

Chief Financial Officer

Chief Manager (IDBL)

[Signature]
[Signature]
[Signature]

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

TYPE OF PROCUREMENT

ADMIN / IT / CONSULTANT / MEDIA

TENDER NAME

Procurement of SEM / LCA Management System

TYPE OF TENDER

SINGLE STAGE-ONE ENVELOPE / SINGLE STAGE-TWO ENVELOPE / TWO STAGE / TWO STAGE-TWO ENVELOPE

OPENING DATE

18-09-2020

OPENING TIME

11:00 Hours

ATTENDANCE (MEMBER PC)

NAME

FIRM

ATTENDANCE (REPS. OF BIDDERS)

①	<u>System Limited</u>	
②	<u>Trillion</u>	
③	<u>Geeked / Gintan (Pvt) Ltd</u>	
	<u>Solutionist Pvt. Ltd</u>	

TOTAL BIDS ACCEPTED FOR EVALUATION

TOTAL BIDS REJECTED

REMARKS

SIGNATURE MEMBERS PC-ADMIN

Head - Fin Div. _____

Head - Admin Div. _____

Member-IDBL _____

Date: _____

3 SCOPE OF WORK / TECHNICAL SPECIFICATION

Technical Specification

3.1 Objective:

- The proposed system is one of ways to maintain situational awareness and security posture of organizational identified critical automated systems and infrastructure components in support of the Risk Management.
- The proposed system will increase the efficiency of the cyber security team, Information technology and systems operation teams besides fostering a broader awareness and a culture of IT Security and risk management.
- Institution's risk posture identification, reduction and improvement in Banking and Enterprise systems and associated critical Infrastructure components.
- The system will be served as a nerve center towards establishing a Cyber Security Operation Center (SOC).
- The proposed system is an actionable, preemptive, and enabling approach and measures through an independent and unbiased entity.
- The system provides a centralized platform and real-time actionable and comprehensive security insight and contextual information for managing cyber risks and threats from detection and protection through remediation.
- The proposed system provide real-time centralized repository or platform of monitoring and detection of cyber security events, logs, traces, footprints left by hackers / malicious insiders and privileged users activities and subsequent reporting of cyber threats, attacks and breaches to IT Operation teams and Management for mitigation and/or elimination.
- The proposed system will provide insight in Policies, Controls and Threats compliance. It will provide a controlled IT environment in terms of change and configuration management.

3.2 Project Management

Sr. No.	Approach
1.	As part of the bid submission, the bidder must include the complete high-level and detailed tentative project plan clearly highlighting the milestones – Schedule, Timelines, Methodology, Roles and responsibility related to different activities like, but not limited to, Ordering, Delivery, Sizing, Designing, Training, Integration, Configuration, Implementation, Customization, Testing, Optimization, Archiving, Maintenance Support and Services of the proposed solution.
2.	Once the contract is awarded to the successful bidder, the kick off meeting(s) will be conducted in the bank premises for the actual project plan with the successful bidder
3.	After the notification of award to the successful bidder, will provide the name of Project Team Lead and team resources those will be assigned to SNDB Security Intelligence and Threat Management System implementation and roll-out.

4.	Successful bidder must provide detailed CVs of project resources assigned to SNDB Security Intelligence and Threat Management System implementation and roll-out.
5.	The successful bidder nominated Project Team Lead/Manager will be responsible for handling the communications and coordination with their management, technical team and SNDB. Project Team Lead/Manager will also be responsible for providing the project status on regular basis.
6.	Change or removal of any resource from the Project team during execution of the project will be subject to SNDB approval. The supplier will submit the CV of the proposed resource(s) for SNDB review. In case of any change in the supplier's allocated Project Team Lead/Manager or team member, the supplier will provide the resource immediately of equivalent or higher qualification and experience.
7.	SNDB may request to change any project resource, in case their performance is not up to the mark or as per institution satisfaction.
8.	Project Supplier may engage foreign / local experts/consultants should they feel it is necessary for the project at their own cost.
9.	The Project Supplier may perform the implementation through Professional Implementation Services from the principal/OEM effectively and efficiently.
10.	The Project Supplier will also provide the Post Implementation Optimization, customization, upgrade, health-check services of the system and also assist the SNDB till acceptance of the system.
11.	During the project, the supplier should provide information on help desk support levels arrangements, End of Life and End of Support information for the proposed product/solution, software support, release management, on-site and remote support, on-line services self-diagnostics tools, ticket and case escalation etc.
12.	Project supplier support and guidance for the IT/Cyber security operation center (IT/Cy.SOC) to SNDB including but not limited to SOC requirement analysis/processes, design/strategy, Implementation of additional tools to supplement SOC capability and threat intelligence, incident handling, investigation, forensics and response.

3.3 Project Timeline

The targeted Project Timeline is 6 (Six) months or earlier including the delivery, implementation and operational acceptance from the date of signing of contract.

3.3.1 Delivery

Delivery will be considered accomplished when all the software and allied components have been delivered at designated location and installed in accordance to the contract.

All related hardware, storage, software licensing shall be in the name of SNDB – registered with OEM where applicable.

3.3.2 Implementation / Deployment

The supplier shall, with due care, diligence and attention implement and deploy the complete system with warranty and technical support and professional services according to the requirements and maximum satisfaction of the SNDB by assigning properly qualified and competent personnel having related product maintenance experience and exercising all reasonable means required in ensuring quality services in accordance with this Agreement.

The On-premises implementation phase / criteria must include but not limited to:

Sr. No.	Implementation phase / criteria
1.	Installation and configuration of server/appliance, applications and associated modules etc.
2.	OEM based accredited training for the system/solution operation management, security analyst and Cyber SOC management
3.	Network configurations - dedicated high speed network interfaces for load balancing (i) system administration, (ii) logs and events push/pull and collection, (iii) network flows.
4.	Integration and configuration of agent and agentless log sources as per requirements to achieve the objectives.
5.	Integration and configuration of network flows (Information will be provided at this stage of implementation)

6.	Normalization/Parsing of logs/events
7.	Aggregation and correlation for analytic of logs/events
8.	Centralized (Security Operation) and specialized dashboards (Networks, Databases, Hosting Systems, Applications, Privileged Users Activity, Executive Management, Audit & Compliance, System Health Check, Work flows/Ticket escalation, progress, status etc.) development and customization
9.	Use / Misuse cases development and deployment, alarms, alerts and reporting
10.	Integration of open source or proprietary threat intelligence feeds
11.	Ticket escalation/workflow configuration to support incident response
12.	Integration and configuration with Vulnerability and Patch management system if required
13.	Testing and Optimization (Health Check)
14.	The implementation, integration, configuration, customization and service related tasks done by supplier will be checked and validated by OEM professional services

The supplier backed by OEM must provide the **best technical and security analytical implementation solution** effective for SNDB IT security until operational acceptance

3.4 Training

SNDB consider training and technology transfer as an integral part of the project. The supplier is required to provide comprehensive and hands on technical training for five (05) SNDB Resources on the complete supplied solution/products and allied equipment by OEM Certified Trainers.

The cost of training should be included in the price schedule of the bidding document. The supplier will provide all necessary installation, technical, troubleshooting, maintenance and preventive maintenance manuals and documentation, CDs, Award of training completion certificates to SNDB staff etc. and keep on updating SNDB for all related technical updates.

The training should be a part of complete solution offering by the supplier that should include but not limited to the following:

1. Complete product introduction, architecture, functionality, technical features, limitations etc.
2. Implementation Installation, configuration, integration, customization, fine tuning, maintenance and services, reporting etc. with respect to the SNDB IT security requirements.
3. Day to day Operation management with available tools, backup and restore procedures in case of product malfunctioning and failure etc.
4. Security operation center monitoring, detection, analytics, reporting, incident handling and ticket escalation etc.
5. Troubleshooting and Maintenance of the System.

3.5 Operational Acceptance

Operational Acceptance means that the supplies and services in the contract have been installed and run in operations after testing in accordance with the products' parameters mentioned in the technical specifications and features meeting the technical requirements of the project.

At least One (01) months of successful operations of the installed system, in accordance with the SNDB required configuration, will confirm the Operational Acceptance of all the supplies under this contract. Also the supplier will ensure dedicated on-site support till operational acceptance.

Any component identified and confirmed through OEM/Distributor or Dealer or by Physical Inspection or performance to be non-genuine, copy or refurbished will be rejected for acceptance and it will be suppliers responsibility to replace that component or system or the entire lot failing which the SNDB may terminate the contract.

For testing any cost associated with test equipment shall be borne by the supplier.

During the course of the project until the operational acceptance of the last installation is signed any cost associated with the repair and/or replacement of the supplies in this contract will remain covered in Warranty and SLA and will be borne by the supplier.

The documentation is a part of operational acceptance that comprised all SNDB specific project related system (hardware, storage, software, Applications) documentation. The supplier will provide following documentation including but not limited to the:

- 1) System Installations, Configuration and Administration
- 2) User guides
- 3) Operation & maintenance (O&M) manual that will cover all components and systems in a way that is easily understood.
- 4) Troubleshooting, backup and recovery
- 5) Standard Operating Procedure with snapshots, diagrams, commands etc.

3.6 Technical Requirements

The technical requirements are categorized as under:

1. Architectural and Deployment Requirements
2. Operational Requirements (Administration & Configuration)
3. Logs/Events/Use or Misuse cases Management Requirements
4. Security Intelligence (Real-time monitoring and prevention, Event Correlation, Analysis and Alerting)
5. Network Activity Monitoring
6. Advanced Threat Management
7. Incident Response and Management
8. Information/Logs/Events Source Requirements
9. Reporting
10. Product/Solution Roadmap

3.6.1 Architectural and Deployment Requirements

The following are the architectural and deployment requirements of the system:

Sr. No.	Requirements
1.	The bidder should include the hardware, software/database, The bidder need to supply, install & configure all the required servers, application/software, OS, middleware, back-up software etc for implementation. Hardware storage must be sufficient for 3 years logs. The bid price must include all relevant costs.
2.	The application should have comprehensive predefined security configuration assessment check (settings) for different supported platforms as per industry standards such as ISO27001, PCI-DSS, OWASP, CIS etc
3.	The application should allow search of assets based on IP, Location, Owner and Department
4.	The application should support multiple approaches for vulnerability assessment. <ol style="list-style-type: none"> 1. Automated Vulnerability Assessment (over the network) 2. Manual Vulnerability Assessment in case automated VA is not allowed
5.	Highly scalable and able to support centralized and distributed environments across multiple sites

6.	Appliance based solution or supplier should propose associated hardware
----	---

	and storage to meet and optimized technical requirements as per OEM recommendation.
7.	The solution should support high availability of hardware and storage solution preferably automatic failover for both hardware and software level
8.	Support multiple deployment options (on-premises, all-in-one appliances, virtual appliances, software, virtual image)
9.	Minimum support 1000 EPS/MPS/EPC/MPC or similar with scalability up to 10,000 EPS/MPS/EPC/MPC or similar
10.	Minimum support 10000 network flow/m with scalability up to 100,000 network flow/m
11.	The solution architecture support heavy load from different IT assets for logs collection with no major performance degradation
12.	Support multiple network interface support i.e. dedicated interface for logs/events collection, dedicated interface for network flows, dedicated interface for system administration etc.
13.	Support integration of open source and closed loop applications
14.	Support healthy database for logs, events and network activities collection and processing such that all information can be access from a single GUI in efficient manner.
15.	Ensure the integrity and confidentiality of the information collected from log sources
16.	Robust analytical risk and threat based intelligence engine for event correlation, use cases from multiple collectors and associated log sources
17.	Provision of flexible and ease of integration, retrieval/collection, aggregation, sorting, filtering, searching, correlation and analysis of events, logs or data across all distributed components.
18.	Support Offline Storage and compressed backup for SAN (FC and/or IP)
19.	Support integration with vulnerability and patch management, Identity Access module, Network Admission Control, WLAN Controller, AAA, IPS and Threat intelligence etc. solutions.
20.	Integration with Core Banking of SNDB i.e. ABII System and its alternative system such as ATM Host, Switch, Avanza etc for log collection and rule based alert generation
21.	System should be able to involve remedial process based on rules defined by SNDB
22.	All standard rules as defined by international good practices must be included
23.	Additions of rules should be easy and manageable
24.	Should provide compliance reports as per SBP Guidelines
25.	Should full stack monitoring & management

3.6.2 Moving Forward

License for EPS/MPS/EPC/MPC and Network Flow/m /FPM can be increased as per the requirement

3.6.3 Operational Requirements (Administration & Configuration)

Operational requirements are an integral part of any security intelligence solution.

Sr. No.	Requirements
1	Friendly and Ease of use interfaces (i.e. icons, menu bar, tips & help, drill downs, wizards, command short cuts, favorites etc.)
2	Support both manual and automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, rule updates, device support, upgrades, patches etc.
3	Support protected web-based GUI to perform central management of all components, monitored assets, system administration, analysis and reporting tasks.
4	The system ensures all associated system components continue to operate when any other part of the system fails or loses connectivity (i.e., management console goes off-line all separate collectors continue to capture logs).
5	Automated and manual backup/recovery process.
6	Real time dashboard of proposed system internal health checks and performance indicators statistics, i.e. memory, storage, CPU, I/Os, network traffic etc. and notify the system administrator when problems arise.
7	Provide the ability to deliver multiple dashboards that can be customized to meet the specific functional requirements of different users of the system and to achieve and implement the right segregation of duty.
8	The system administrator is able to define role base access to the system by log source, assets group, functional area or dashboard. This includes being able to restrict a user's access to information to only those systems from a specific group or functions or dashboard including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing.
9	The solution deliver customizable dashboards (i.e. for Security Operation Center, threat management, compliance management, privileged users monitoring, monitored assets view, top security events view, network activities and attacks view, use cases view, malware/virus views, suspicious/malicious activities view, incidents and alarms views etc.).
10	Support and provide predefined templates for dashboards and wizard to build new ones dashboards as per customer requirement or institution IT or business environment.
11	The solution provide intuitive mechanisms for system troubleshooting such as proactive notifications, command line, GUI utilities etc.
12	The solution support versatile and diversified built-in rules for use cases / policies / scenarios implementation
13	The solution supports the selection of built-in and customized dashboards from the UI for use in SOC or NOC deployments.
14	The solution provides the ability to encrypt communications between components. (Data in transit)
15	The solution generate and record audit logs of all administrator / user actions across monitored assets including SIEM system, Core Banking, ADC etc.
16	The solution must not initially drop any events if the license exceeds the purchased license volume and also alert for this situation in advance
17	The solution is able to use the same management console to restore the archived logs to be re-processed, re-normalized and re-classified.

18	The solution maintains a database of all assets discovered on the network. The user should be able to search this database.
19	Support standard protocols (like DNS, NetBIOS, SNMP, NTP, SMTP, HTTPS, SSH).
20	The solution supports manual and/or automated classification and inventory of assets i.e. criticality, location, department, ownership/custodian, H/w & S/w details, etc. that are being monitored and protected.
21	The solution provides integration with Microsoft active directory system
22	The solution supports file integrity monitoring across monitored assets.

3.6.4 Logs/Events/Use or Misuse cases Management Requirements

Sr. No.	Requirements
1	Log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage.
2	The solution support industry log collection methods (Syslog, Windows Management Instrumentation (WMI), Remote Procedure Call (RPC), Windows Events Collection, FTP, SFTP, SNMP, SMTP, JDBC, SDEE etc.)
3	The solution also support non industry log collection methods like Single-line Flat Files, Multi-line Flat Files, Proprietary and customized APIs etc.
4	The solution provide agent-less collection of event logs whenever possible.
5	The solution support long-term access to detailed security event and network flow data for analysis. The system must be able to provide access to at least 12 months' worth of online/active detailed information and additional 12 months offline/passive information and scalable up to 5 years of offline/passive information.
6	The solution / system generate audit logs of all administrator / user actions within system/SIEM Accounting Audit including logs/event tamper monitoring.
7	The solution support custom applications or non-supported devices logs parsing / normalization.
8	The solution supports diversified agent and agent less log collection mechanism.
9	The solution supports and maintains a history of user authentication event on per asset basis.
10	The solution supports built-in use cases as per threat detection, flow analysis, network & application behavioral analysis, incident etc.
11	The solution categorizes log data into a human-readable format to eliminate the need to know OEM specific event IDs.
12	The solution normalizes common event fields (i.e. usernames, IP addresses, hostnames, log source device, commands, time and date stamping etc.) from disparate devices across a multi-OEM network. Specialized parsing/normalization requirements also be supported.
13	The solution provides APIs, GUIs and wizards for parser creation to support the integration of unsupported data sources.
14	The solution provides common taxonomy /categories of events.
15	The solution provides the ability to store/retain both normalized and the original raw format of the event log for forensic purposes.
16	The solution provides the ability to normalize and aggregate event fields.
17	The solution supports normalize event time stamps across multiple time zones.

18	The solution supports the collector/agent send the log over TCP and encrypted from remote locations or secure zone.
19	The solution supports integrity of logs/events collected from all monitored assets

3.6.5 Security Intelligence (Real-time monitoring, Event Correlation, Analytics and Alerting / Alarms)

Sr. No.	Requirements
1	The solution support and provide real-time monitoring of users and networks activities, data access, intrusion, threats and attacks detection, behavioral profiling, suspicious/malicious activities, malware/virus proliferation, affected/compromised hosts, use cases anomalies, monitored assets anomalies, IPs and hostnames reputation, geo locations sessions, advanced persistent threats etc.
2	The solution provides alerting based on observed security events, threats, indicators of compromise from monitored devices.
3	The solution provides alerting based on observed anomalies and behavioral changes in network flow and associated security events and threats. Solution should provide alerts based on rules defined/required by SNDB
4	The solution generates an alert when a system license goes beyond the given threshold in terms of count or percentage and notifies the system administrator.
5	The solution supports alerts on internal health checks and performance indicators statistics beyond given threshold level, i.e. memory, storage, CPU, I/Os, network traffic etc. and notify the system administrator when problems arise.
6	The solution supports an alert mechanism if any SIEM system service / component / monitored asset goes in to non-responsive /stop / hang state and restored back to normal state. The alerts should be customizable as per requirements of SNDB
7	The solution provides the ability to correlate information across potentially disparate devices.
8	The solution supports risk based weighted alerts to allow for prioritization. Weightages must be assignable based on multiple characteristics such as asset type, asset value, threat/attack type, activities type, protocol, application, etc.
9	The solution provides a mechanism, to optimize rule tuning, and customized rule development as per the institution use cases requirements.
10	The solution provides the ability to aggregate and analyze events based on a user specified filter.
11	The solution limits and summarized the presentation of multiple similar events and alerts.
12	The solution supports the ability to correlate against intelligence feed, security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These intelligence feeds should be updated automatically by the solution.
13	The solution supports real time monitor and alert when there is a disruption or disconnection in log collection from an asset or log source.
14	The solution provides a real-time event view of monitored information in raw/original as well as processed/parsed format.
15	The solution provides alerting based upon established policy or rule.
16	The solution supports and provides behavioral white lists and baselines trend from hosts, applications, user activities, networks etc.
17	The solution should be capable of taking automatic actions upon receiving an alert/alarm through email or by ticket/case escalation.

3.6.6 Network Activity Monitoring

Sr. No.	Requirements
1	The solution supports local and remote network traffic collection architecture and analysis.
2	The solution supports up to layer 7 visibility of application definition protocols and ports. The system must support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP, TOR, P2P etc.)
3	The solution dynamically learns network behavioral norms and exposes changes as they occur.
4	The solution detects denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.
5	The solution detects and present views of traffic pertaining to observed threats in the network (e.g. brute force attack, reconnaissance, P2P, command and control communication, SQL injection etc.)
6	The solution identifies inbound/outbound network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, malware etc.)
7	The solution displays traffic profiles in terms of packet rate. This capability must be available for simple TCP analysis (TCP Flags, etc)
8	The solution maintains network profile and present information in multiple timeframes.
9	The solution is able to profile communication originating from or destined to the internet by geographic regions in real-time.
10	The solution provides the ability to extract specific, user defined, fields from network data and use the fields in correlation rules.
11	The solution supports in display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats across each configured monitoring point in the network and VLAN.
12	The solution is able to generate useable Metadata for network packets content such as source IP, Destination IP, source and destination Protocols, Database queries, Session Size, Session content including filenames, usernames etc. API should be available for processing the logs by other application as required
13	The solution allows the user to create custom profiles and views using any property of a flow, log, data source or already profiled traffic, IP addresses, groups of IP addresses, source/destination IP pairs etc.

3.6.7 Advanced Threat Management

Sr. No.	Requirements
1	The solution supports and provides threat intelligence feeds include supporting protocols and formats.
2	The solution allows integration with the threat intelligence source/feed and provide real time visibility of global threat landscape automatically as per critical and severity ratings of threat.
3	The solution provides the ability to contextually correlate threat detection on the network and host with security events and real-time knowledge of the assets or network being targeted.
4	The solution provides the ability to automatically weight the priority and severity of reported security threats/events according to the relative importance of the targeted asset.
5	The solution supports IP and domain reputation, geo-location monitoring.
6	The solution supports and provide latest threats information like malware, phishing, suspicious apps, credential theft, breach of security controls, critical and high risk vulnerabilities, command & control reports, suspicious proxies and protocols, exploitation of vulnerabilities, Zero-day malware indicators/vulnerabilities, information leaks, hacktivism etc.
7	The solution supports and have built in Pattern Matching to identify advance yet granular threats e.g. User Account created and privilege escalated, Audit logs cleared and stopped, multiple authentication by single ID from different sources into single destination etc.

3.6.8 Incident Response and Management

Sr. No.	Requirements
1	The solution provides automatic contextual information for incidents and ability to perform basic forensic analysis.
2	The solution supports disparate events belonging to the same incident are automatically aggregated through correlation rules.
3	The solution provides a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, and vulnerability data.
4	The solution allows the fine tuning and reducing of false positives of the Indicator of Compromise, incident, risk scoring, alerts/alarms.
5	The solution supports operational efficiency and efficient workflows through automated and/or manual response capabilities, including automation to improve threat/incident detection and analytics, ticket escalation to the IT operation staff, easy execution, status update, follow up and closure
6	The solution supports triaging of incidents aided by tagging, commenting, annotating, audit trail and real time status tracking of ongoing incidents.
7	The solution provides a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, log source, correlation rules, user defined, time date, etc) for forensics purpose. The user must be able to filter incidents along these defined attributes.

3.6.9 Information/Logs/Events Source Requirements

Sr. No.	Requirements
1	The solution supports heterogeneous OEM and open source products like Microsoft, LINUX/UNIX Cisco, CA Technologies, Juniper, McAfee, Temenos, IBM, EMC, FireEye, RSA, APC, Oracle, Symantec, VMWare, HyperVisor, Baracuda, Avaya etc.
2	The solution supports information/logs/events collected from Microsoft based servers (Active Directory/Domain controller, Exchange, Proxy, share point, IIS, SQL, Anti-Virus/Malware, DLP, Gateways, syslogs, sandboxes etc.) and end-user systems.
3	The solution supports information/logs/events collected from Linux/Unix based servers (Apache, syslogs, etc.) and end-user systems.
4	The solution supports information/logs/events collected from enterprise class database solutions (MS SQL, Oracle SQL, JBase etc.)
5	The solution supports information/logs/events collected from proprietary applications (i.e. ERP, T24, SWIFT, Web, RTGS, e-CIB, DWH, OLAP, ABII Core Banking Application, Avanza Rendezvous etc.)
6	The solution supports information/logs/events collected from Data Leak Protection (DLP), File integrity and activity monitoring software and tools.
7	The solution supports information/logs/events collected from Authentication, Authorization and Auditing servers (Access Control Server, Network Admission Control Server, Identity and access management Server, Database Activity Monitoring Server etc.)
8	The solution supports information/logs/events collected from Network infrastructure components (i.e. switches, routers, firewalls, IDS/IPS, sandboxes etc.)
9	The solution supports information/logs/events collected from Network flows (i.e. Netflow, J-Flow, S-Flow etc.) products.
10	The solution supports information/logs/events collected from industry leading vulnerability scanners and patch management solutions.

3.6.10 Reporting

Sr. No.	Requirements
1	The solution provides reporting on high level IT security posture for management in terms of graphics, statistics, past and current trend, Top ratings/severity etc.
2	The solution provides configurable reporting engine for customized report creation.
3	The solution supports on demand and automatic scheduled report generation and distribution in electronic form via e-mail while maintain archiving of reports.
4	The solution provides templates for the easy creation and delivery of reports at multiple levels ranging from operations, business issues to the management,
5	The solution provides reports for typical contextual business and security issues through robust filtering and searching.
6	The solution supports sorting/searching/filtering of reports.
7	The solution supports monitored IT assets scope, ticket escalation and status reports.
8	The solution supports on demand and automated reports of users activities audit, use cases anomalies, networks intrusion and attacks, malware/virus across hosts, affected/compromised hosts, suspicious/illegitimate inbound/outbound network

	activities/traffic, suspicious/malicious sessions, monitored IT assets disconnection, stopped responding, heartbeat failure etc.
9	The solution provides the ability to export the internally generated reports to common file formats. i.e.html, csv, xls, pdf, doc etc. with institution monogram/logo support.
10	The solution provides optional reports for specific compliance regulations (PCI, SOX, FISMA) and control frameworks including (COBIT, ISO).
11	The solution supports real time creation and generation of reports from the dashboard.
12	The solution supports manual and/or automated report on classification and inventory of assets i.e. criticality, location, department, ownership/custodian, H/w & S/w details, installed applications, EOL etc. that are being monitored and protected.
13	The solution supports case/issue/incident management reports i.e. mean time to detect, escalation, pending, deferred, under progress, mean time to resolve/recover etc.
14	The solution supports integrity of generated reports

3.6.11 Product/Solution Roadmap

Sr. No.	Requirements
1	The solution has well established mechanisms to enhance current features, functionality and influence future features and products.
2	The solution has 24x7 well managed online support portal for problems, issues and requirements resolution, ticket escalation, knowledge base, software upgrades/patches.
3	Bidder provides comprehensive warranty, support, and maintenance services of quoted solution during pre and post warranty period.
4	The solution must have minimum 5 years or more end-of-life cycle at the time of bidding
5	At the time of bidding, the proposed solution must be in the leader's quadrant of Gartner.

3.7 Warranty and SLA

3.7.1 Warranty:

01 (one) year onsite comprehensive warranty (with free parts and labor) will commence from the date of Operational Acceptance Certificate.

3.7.2 Service Level Agreement (SLA) during and after Warranty

03 Years SLA	One (01) Year SLA during warranty with one (1) certified and skilled resident engineer and 24x7 OEM backed Maintenance and Support	SLA Will commence from the date of Operational Acceptance Certificate
--------------	--	---

	Extendable upto Two (02) Years SLA after Warranty with one (1) certified and skilled resident engineer and 24x7 OEM backed Maintenance and Support with mutual consent of both parties	till end of entire contract period.

Any component or equipment identified non-genuine, copy or refurbished during entire SLA will be rejected instantly and it will be supplier's responsibility to replace that component or equipment.

The bidders are required to include OEM warranty with SLA during the warranty period of 1 (one)-year as well as post warranty OEM backed Maintenance and Support of 4 (four) Years with the SLA as mentioned below

The SLA during and after Warranty Maintenance and Support of the supplies should be equipped with the OEM Support Packages to meet the following requirements, except any damage caused by the fire or disaster event or mishandling of the equipment against the specified and communicated standards operating and handling procedures to the SNDB by the OEM/Supplier.

The OEM Support Services will remain available to the SNDB on call 24 x 7 basis.

Telephone, Web and email based case opening for technical problems

Engineers Support (Preferably On-Site) or otherwise over email/phone/web whenever required by the SNDB.

The AHR should be carried out by the supplier for Custom clearing, transportation and on-site delivery of the hardware after Duty Delivery Paid to SNDB meeting the SLA time. The return and collection at customer site and return of faulty items to OEM and its related expenditure is also the responsibility of the supplier.

The warranty of the supplies will start from the Date of Operational Acceptance Certificate of the complete system.

The warranty, Maintenance and Support should be supported and registered by the OEM on the name of SNDB.

3.7.3 Service Level Agreement (SLA) Requirements

3.7.3.1 Scope of Services:

Supplier shall provide support services to run and maintain all the Hardware and Software proposed in the solution in compliance with the Service Level Requirements.

The Supplier shall also replace, restore, reinstall, reconfigure, integrate, customize, troubleshoot, Patch services and updates, Release (minor and major software/firmware/middleware upgrades), Backup hardware, Support case management (opening, escalation, follow up, historical analysis, reports, knowledge base, etc) through internet based web portal, OEM's Remote technical assistance from acceptable locations to SNDB, Access to technical material, documents, manuals and knowledge base, On- site support as and when required for any failed hardware, storage, software and application components for recovery to normal operational status at no cost to the customer.

3.7.3.2 Availability Requirement:

This section defines the Service Level requirements, classification of incidents, and means of reporting, and expectations for availability and response times in relation to all Hardware, Storage, Software, Application and any add-on or customization performed during implementation (if any) pertaining to their proposed solution that are to be maintained and supported by the Supplier.

Following table outlines the Incident Classification System including required Recovery Time:

3.7.3.3 Reporting Time:

It is the time duration from logging a support incident till the technical support person of the supplier contacts SNDB concerned Technical team.

3.7.3.4 Recovery Time:

It is the time duration from logging a support incident till the problem resolution for restoring faulting system from severity RED to ORANGE or from ORANGE to GREEN. This time starts from problem reported till successful completion of required corrective action, inclusive of replacement (if required).

3.7.3.5 Standard Business Hours:

Normal Business hours: 9:00AM - 5:30PM, Monday through Thursday and 9:00AM – 6:00PM on Friday.

3.7.3.6 Extended Business Hours:

24 x 7

Any change in Standard Business hours by Government of Pakistan will be followed accordingly during entire contract period.

3.8 Reporting & Resolution Time Limits Table

Severity	RED category	Orange category	Green category
Criteria	<ul style="list-style-type: none"> -Entire production system is down, or a major system component is inoperative or severely impacted - System performance has severely degraded 	<p>System is operating normally, but a redundant component or supporting feature has failed. e.g. Log source(s) stopped responding, dashboard not working/freeze, Alerts/Alarms stops, offline storage not available, backup abnormally stopped, License exceeding, Threat intelligence feed(s) not responding or stopped etc.</p> <p>- Technical issues are being faced causing interruptions to the operations or any failure in its functionality due any suspected hardware or software failure</p>	<ul style="list-style-type: none"> -The system is available and performing adequately, however performance tuning, software or firmware patch installation or software or firmware version upgrade is required during a planned activity. - Operational performance of the appliance / system is facing error(s), while the operations remain functional. -Any query towards the supplied solution raised by the SNDB to the local partner or OEM
Reporting time	Within two (02) business hours of Reported Incident	Within six (06) business hours of Reported Incident	Within twenty four (24) business hours of Reported Incident
Resolution Time	Within six (06) business hours of Reporting	Within forty eight (48) business hours of Reporting	Within five (05) business days of Reporting

Action	<ul style="list-style-type: none"> - Immediate availability of onsite engineers support for recovery options within one hour - Troubleshoot, Rectify, Repair, Replace faulty component (s), Re-configure, Re-deploy within specified - Escalation to OEM for technical support from OEM via internet or phone - Provide backup solution to continue 	<ul style="list-style-type: none"> - On-Site Technical Support on Call Basis. - Troubleshoot, Rectify, Repair, Replace, Re-install, Re-configure and Re-deploy component (s) to ensure resumption of business operations within specified hours as per requirement - Escalation to OEM for technical support from OEM via internet or phone (if required). 	<ul style="list-style-type: none"> - Technical Support on Call Basis or On-Site as per requirements. - Technical assistance from OEM via internet or phone. - Firmware/software patches updates and upgrades.
	operations until primary or actual solution is restored		
Support Coverage	<ul style="list-style-type: none"> - 24 x 7 	During business days hours (9:00AM - 5:30PM, Monday through Thursday and 9:00AM – 6:00PM on Friday) or otherwise notified by the Government of Pakistan or SNDB on special occasions.	During business days hours (9:00AM - 5:30PM, Monday through Thursday and 9:00AM – 6:00PM on Friday) or otherwise notified by the Government of Pakistan or SNDB on special occasions.

3.9 Terms and Conditions:

3.9.1 The Supplier shall provide details about Help Desk or Customer Support contact information including details about Call Logging Procedure to ensure recording, monitoring and reporting of support calls.

3.9.2 Supplier should provide call logging through telephone in terms of Support Levels and Escalation Procedures that should be mapped to the Severity of the incidents and should also provide telephone number which will be used after Standard Business Hours.

- 3.9.3 Supplier shall provide details about structure of Technical Support in terms of Support Levels and Escalation Procedures that should be mapped to the Severity of the incidents.
- 3.9.4 The Supplier shall provide onsite support, maintenance, replacement and update of BIOS, firmware, and all associated software supplied as part of solution covered under this agreement. The Supplier will provide latest version of firmware/software on Customer's request for up gradation purpose free of cost. In case of bug in Software/firmware Supplier will provide required patch and will perform patching, testing and verifying the changes with the coordination of the Supplier (if requested). Upgrade to Latest Version or patch fixing shall be free for the Customer.
- 3.9.5 Supplier shall submit all incident reports and quarterly summary reports for any support period as and when required.
- 3.9.6 Supplier shall perform all dispatch functions, including keeping the Customer informed about the status and eventual completion of replacements or repairs.
- 3.9.7 RED incidents should be given an escalated level of commitment from Supplier. For RED incidents, Supplier shall ask their Support Professionals to work non-standard hours, reassign critical resources from other activities, and/or ensure a Support Professional to work round-the-clock until a problem is fully resolved.
- 3.9.8 A problem that initially starts at a severity RED situation may be classified at severity ORANGE upon implementing a workaround. When a permanent solution is found and implemented, the problem might be reclassified to severity GREEN for monitoring before it is closed. However, reclassification of severity shall be accepted and signed off by the Customer.
- 3.9.9 If same fault re-occurs within 48 hours, the original call will be reopened with the same log number and the Recovery Time will continue from the time that original call was reopened.
- 3.9.10 In case the faulty item or unit is required to be sent overseas for repair or replacement services then Supplier will send the faulty equipment and deliver the replacement or repaired equipment to the Customer site at its own cost to overseas for repair and replacement.

During and after the warranty period (which means during the entire 5 (five)-years period) the supplier will have to provide support services as per the required SLA mentioned above.

The selected bidder will be essentially required to provide necessary CNIC of the Project Manager, Engineers, Technicians, labors and other logistic resources etc working within the SNDB site during the contract period.

The bidders must adhere to the rules, discipline and practices of SNDB, during the entire course of project.

Integrity Pact

Declaration of Fees, Commissions and Brokerage etc Payable by the Suppliers of Services Pursuant To Rule 89 Sindh Public Procurement Rules Act, 2010

Trillium Information Security Systems (Pvt.) Ltd. hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan (GoP) or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing, [the Supplier] represents and warrants that it has fully declared the brokerage, commission, fees etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultation fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

Trillium Information Security Systems (Pvt.) Ltd. Certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representation or warranty. [The Supplier] accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [the Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by [the Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

For and On Behalf Of

Trillium Information Security Systems (Pvt.) Ltd.

Signature: _____



Name: Mahir Mohsin Sheikh



NIC No: 61101-6425619-3

HEAD OFFICE

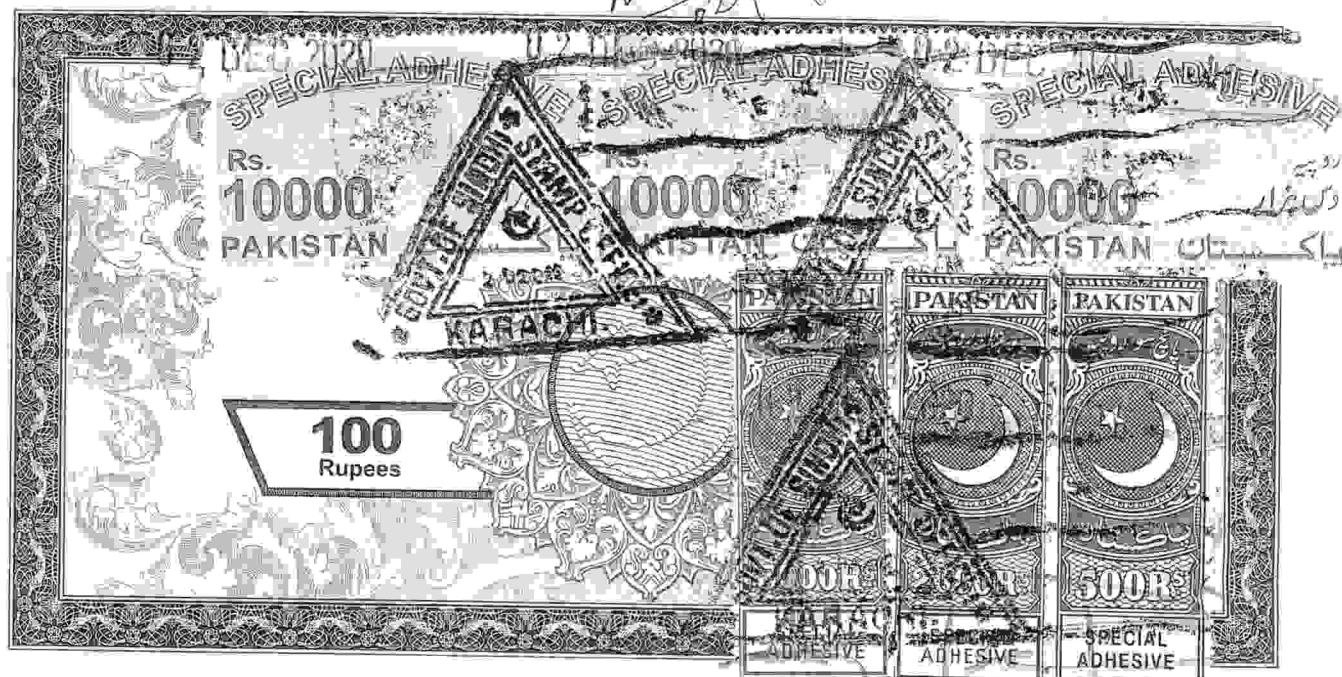
10th Floor, AWT Plaza, 5-The Mall,
Rawalpindi, Pakistan.
Tel: +92 51 5524181-2, Fax: +92 51 556 8044

KARACHI OFFICE

Office No. 802-803, Block B, 8th Floor,
Fakhri Trade Center SR-6/10,
Shara-e-Liaqat, (Frere Road), Karachi
Tel: +92 21 32277224-6 Fax: +92 21 32277227

LAHORE OFFICE

Regus Enterprise Center, 3rd Floor,
Enterprise Building, 15 KM
Multan Road, Lahore.
Tel: +92 42 35958598-698 Fax: +92 51 5568044



2-12-2020

OFFICE SUPERINTENDENT

Tender Ref. No. SNDB/COK/ADMIN/1173/2020

Karachi.

02 DEC 2020

AGREEMENT**For Procurement of SIEM/Log Management System**

This Agreement is executed made on this 3rd day of December, 2020

By & BETWEEN

Sindh Bank Limited, a banking company incorporated under the laws of the Islamic Republic of Pakistan and having its registered Head office at 3rd Floor Federation House, Abdullah Shah Ghazi Road, Karachi (hereinafter referred to as "SINDH BANK") which expression shall unless repugnant to the context include its successors-in-interest and permitted assigns) of the first part:

AND

M/s Trillium Information Security System is a private limited company incorporated under the laws of the Islamic Republic of Pakistan and having its registered office at 10th Floor, AWT Plaza, S- The Mall, Rawalpindi, Pakistan (hereinafter referred to as "M/s Trillium Information Security System"). WHEREAS the M/s Trillium Information Security System is the dealer/supplier/manufacturer of **Information Security Solution**.

WHEREAS:

"SINDH BANK" intends to procure SIEM/Log Management system from M/s Trillium Information Security System on Amounting Rs. 10,712,117/- (Ten Million Seven Hundred Twelve Thousand One Hundred Seventeen Only) as detailed below on terms and condition laid down.

Detail of Solution is as follows.

S. No	Product	Total Price (PKR) (Including All Taxes)
1	IBM QRadar Software/Licenses-Initial One Year	7,130,117/-
2	Professional Services -Implementation/Support including 1x Resident Engineer for 1 Year/Local Training-Initial One Year	1,582,000/-
3	Hardware	2,000,000/-
	Total -Initial One Year	10,712,117/-
1	2nd Year SLA (Software/Local Support including x Resident Engineer)	2,348,335/-



S. No	Product	Total Price (PKR) (Including All Taxes)
2	3 rd Year SLA (Software/Local Support including x Resident Engineer)	2,503,058/-
	Grand Total (Including All Taxes)	15,563,510/-

And M/s Trillium Information Security System agrees to provide solution to the bank, as per tender opening date 18, September 2020 along with the road map/ Schedule of payments by Sindh Bank mentioned in Financial Proposal which is attached herewith and marked as Annexure-A.

PARTIES

Collectively SINDH BANK & M/s Trillium Information Security System are referred to as "parties."

This Agreement and all terms and conditions of the tender document will remain part of this agreement.

PAYMENT SCHEDULE

The payment to be made to the M/s Trillium Information Security System under this Contract shall be made in accordance with the payment schedule mentioned below:

- a. **Software:** 100% on delivery of software Proof of entitlement (POE)
- b. **Hardware:** 100% on delivery of Hardware

Implementation/Support:

- c. 50% after completion of Phase2 of SoW
- d. 50% after implementation sign off

Year2 & Year3 Payment (Subject to Extension of Contract):

- a. 100% to be made on delivery of renewal Proof of Entitlement (PoE)

Resident Engineer/ SOC Analyst:

The resource will be deployed on-site after the request of Sindh Bank, Till one year from the day of commencement of services.

The maximum targeted Project Timeline is 6 (Six) months or earlier including the delivery and implementation sign off from the date of signing of contract.

1. Performance Guarantee:

10% of the total amount for initial year i.e. Rs. 10,712,117/- will be retained by Sindh Bank as "Performance Security" for one year and will be returned until satisfactory confirmation by SINDH BANK. In case M/s Trillium Information Security System does not fulfill its commitments, the bank reserves the right to enforce the performance security.

2. TERM OF AGREEMENT

The term of this agreement shall be for the period of 1 year commencing from the date of signing of this agreement. Extendable up to subsequent 2-Years upon mutual consent of both parties on quoted prices of subsequent years in financial bid i.e. Rs. 4,851,393/- (Four Million Eight Hundred Fifty-One Thousand Three Hundred Ninety-Three Only).


- 1. This agreement shall continue to remain in force unless terminated by either party, according to the terms and conditions as stated below.

NOW IT IS HEREBY AGREED as follows:

3. SCOPE OF WORK

This Section represents the Scope of Work (SoW) of IBM QRadar SIEM, for Sindh Bank.

[Handwritten signature]

[Handwritten signature]

 2 | Page

Terminologies:

- IBM QRadar is the tool used for Security Information & Event Management (SIEM).
- QRadar Console is used for accessing the QRadar server.
- Log Sources are end devices to be integrated with QRadar.
- Reference Set is the collection of Data Sets to be used in defining rules.
- Offenses are generated when rule conditions are met against events.

Requirements:

Following must need to be ensured by SINDH BANK for successful solution Deployment:

- Placement of hardware and Software (QRadar ISO from customer IBM Portal) as per shared specifications in prerequisites document.
- Sindh Bank shall share network diagram with M/s Trillium Information Security System to help in implementation of SIEM
- Sufficient bandwidth availability over LAN or WAN for centralized deployment.
- Network whitelisting of ports as per shared prerequisites document.
- Onsite availability of point of contacts from SINDH BANK.
- Systems to be tested are online and have connection with the Administration Server.
- The end devices (log sources), their operating system should be in good condition.
- Administrative rights and privileges are available for the deployment.

Scope of Work (SoW) Phases:

S.N.	Phases / Activities	Responsibilities	
		TISS	SINDH BANK
0	Phase 0 – Project Initiation		
0.1	Deployment kick-off session	TISS shall give an overview on the architecture and general working of the solution.	SINDH BANK shall provide the details of the team involved in deployment.
1	Phase 1 – Design Discussion		
1.1	Availability of network prerequisites	TISS shall verify the availability of network Prerequisites	SINDH BANK shall fulfill network prerequisites
1.2	Availability of SIEM Software	TISS Shall provide the link for getting the ISO file for installation.	SINDH BANK shall download the software from the provided link.
1.3	Network Connectivity Testing	TISS shall verify the Ports whitelisting as per shared prerequisite document.	SINDH BANK shall whitelist all ports mentioned in prerequisite document for efficient deployment of Solution

2.	Phase 2 – Deployment		
2.1	Installation of QRadar SIEM	✓	
2.2	System and Console Settings <ul style="list-style-type: none"> • License Installation • Configure Update Settings • Configure Users & Roles • Notification delivery Settings • Installation of QRadar Required Extensions 	✓	
	Phase 3 – Log Source Integration		
2.3.	10x Base Log Sources Integration	✓	SINDH BANK Shall provide the administration rights on the machines for
			agent installation/configuration
2.4.	2x Base Flow Source Integration	✓	SINDH BANK Shall provide the administration rights on network devices for integration
3	Phase 3 – Offense Management Rules Creation		
3.1.	Rules Creation – Enabling Standard & 5x Custom Use Cases <ul style="list-style-type: none"> • Creation & Tuning of Building Blocks • Creation & Tuning of Reference Sets • Creation & Tuning of Custom Rules 	✓	
3.2.	Detect all the unauthorized network connections to/from all systems	✓	Sindh Bank shall provide network logs for integration
3.3.	Detect unauthorized access/modification to confidential data	✓	Sindh Bank shall provide logs for integration
3.4.	Monitor for any event that results in addition, deletion, and modification of user IDs, credentials, privileges and other identifier objects	✓	Sindh Bank shall provide AD logs for integration
3.5.	Detect when anti-virus protection is not updated/disabled on the machines.	✓	Sindh Bank shall provide logs from anti-virus console for integration
3.6.	Alert when system-level objects, such as database, tables or stored procedures, are created, modified or deleted	✓	Sindh Bank shall provide database logs for integration
3.7.	Detect and generate alert when Privileged User/Administrator Password Reset Attempts, Login failures and successes	✓	Sindh Bank shall provide AD logs for integration

By



3.8.	Detect and generate alert for ACLs Creation, Deletion and Changes in switches, routers or Firewalls	✓	Sindh Bank shall provide relevant device network logs
3.9.	Detect usage of internet access, restricted websites, online streaming, chatting software and P2P software.	✓	Sindh Bank shall provide firewall or proxy logs for integration
3.10.	Ports scan activity originating from a foreign or local address(es)	✓	
3.11.	Suspicious behavior of Log Source (Unexpected Events Per Second (EPS) from Log Sources)	✓	
3.12.	Detect Malware Infection, Compromised and infected system tracking	✓	Sindh Bank shall provide logs from anti-virus deployed for integration
4	Phase 4 – Reports/ Dashboards Configuration		
4.1.	Reports Customization	✓	Sindh Bank shall share the requirement
4.2.	Dashboards Customization	✓	Sindh Bank shall share the requirement
4.3	Backup Configuration	✓	Sindh Bank shall share the address for backup location

Day-wise Breakdown:

The day-wise breakdown of onsite visits for Deployment is as follows:

Phase	Description	Man Days
1)	Phase 0 – Project Initiation	01
2)	Phase 1 – Design Discussion	03
3)	Phase 2 – Deployment	20
4)	Phase 3 – Offense Management Rules	19
5)	Phase 4 – Reports/Dashboard Customization	05
Total Man Days		48

Note:

- Total SOW to be delivered by M/s Trillium Information Security System with assistance of SINDH BANK within timelines (48 working days):
- SINDH BANK shall ensure and resolve all dependencies that need to be fixed before the specified phase initiation.

Training:

S.no.	Description	Days
01	Knowledge Transfer Session of Implemented SIEM Configurations and Features for 5x Sindh Bank Resources at HO Sindh Bank	05

 5/ Page

Hardware

The warranty of the Hardware is 3- years comprehensive onsite from the date of delivery.

The warranty will be effective while the Goods remain in the premises of the Bank and the Bank will not be responsible to send the equipment to the vendor site. In case however if any portion of equipment required to be shifted to M/s Trillium Information Security System site, vendor will provide equivalent backup during the warranty period.

Vendor should maintain adequate inventory of the parts so that the replacement is available within 24 hours, if any fault arises in the equipment during the warranty period. In case the effected part is not available, then the M/s Trillium Information Security System will provide backup equipment of the same product or better till the resolution of the fault, without any extra cost to the Bank.

If problem does not resolve within 10 days and suitable backup is also not provided then Bank will have the right to get it resolve its own from the open market and charge the actual cost to the M/s Trillium Information Security System without any further referring to the M/s Trillium Information Security System.

The vendor also undertakes to bear all kind of taxes i.e. Stamp duty/ Services Charges/Professional Tax / Sales Tax Invoice, Income Tax, Zila / Octroi Tax (if any) and all other incidental charges etc, up to the place of destination.

The Bank reserves the right to Test/Check the equipment to ensure that it is provided as per specification in the tender document. For any discrepancies, M/s Trillium Information Security System will provide remedy without any extra cost otherwise the SINDH BANK reserve the right to forfeit full security deposit/ cancel the order for the supply and bring the M/s Trillium Information Security System on black list of the Bank forever. The decision of the Bank shall be final and binding upon the M/s Trillium Information Security System.

4. Penalty

If M/s Trillium Information Security System fails to provide and implement solution within the agreed Timeline of 6 months, then Sindh Bank may be entitled to charge the penalty Rs. 5,000/per day upto maximum 10% of total project value for initial year i.e. **Rs. 10,712,117/-**

5. OTHER TERMS & CONDITIONS

- Any notice, request or consent required or permitted to be given or made pursuant to this agreement shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the given address.
- A party may change its address for notice by giving a notice to the other Party in writing of such change.
- The M/s Trillium Information Security System /contractor will not assign its job to anyone without prior permission of Sindh Bank.

6. CONFIDENTIALITY

• **Confidential Information.** For the purposes of this Agreement, the term "Confidential Information" shall mean any information comes in possession of M/s Trillium Information Security System and its personnel during normal course of business / Services shall be the property of the SINDH BANK at all times and / or any of the SINDH BANK's communications, whether in oral, written, graphic, magnetic, electronic, or other form, that is either conspicuously marked "confidential" or "proprietary," or is known to be confidential or proprietary, or is of a confidential or proprietary nature, and that is made in the course of discussions, studies, or other work undertaken shall be kept confidential by M/s Trillium Information Security System.

6 | P a g e



- M/s Trillium Information Security System acknowledges that the SINDH BANK is under strict confidentiality obligations with regard to all the information and affairs of its Customers. Therefore, M/s Trillium Information Security System shall not disclose any data, information or other affairs of SINDH BANK's customers which may come to the knowledge of M/s Trillium Information Security System in providing the above services. M/s Trillium Information Security System undertakes to obtain from its employees involved in the Services to provide written undertakings to maintain the confidentiality obligations of M/s Trillium Information Security System under this Agreement.

- In the event of breach of this clause, M/s Trillium Information Security System shall be liable to pay damages to the SINDH BANK and indemnifies the SINDH BANK against any injury arising out of any breach of this clause by the SINDH BANK.

This clause shall also survive after termination of the Agreement.

7. INDEMNIFICATION.

- M/s Trillium Information Security System (the "Indemnifier") agrees that it shall indemnify, defend, and hold harmless the SINDH BANK and its parent, subsidiaries, affiliates, successors, and assigns and their respective directors, officers, employees and agents (collectively, the "Indemnitees") from and against any and all liabilities, claims, suits, actions, demands, settlements, losses, judgments, costs, damages and expenses (including, without limitation, reasonable attorneys', accountants' and experts' fees) arising out of or resulting from, in whole or in part: (i) any act, error or omission, whether intentional or unintentional, by the Indemnifier or its officers, directors, employees, or sub-administrators, related to or arising out of the business covered by this Agreement, or (ii) an actual or alleged breach by the Indemnifier of any of its representations, warranties or covenants contained in this Agreement (including, without limitation, any failure of Indemnifier to comply with applicable local, state, provincial or federal regulations concerning Indemnifier's performance under this Agreement).

This clause shall also survive after termination of the Agreement.

8. Authorized Representative:

- Any action required or permitted to be taken, and any document required or permitted to be executed under this agreement by the Sindh Bank or the M/s Trillium Information Security System Ltd may be taken or executed by the officials.

9. Goods Faith:

The Parties undertake to act in good faith with respect to each other's rights under this agreement and to adopt all reasonable measures to ensure the realization of the objectives of this agreement.

10. Conflict of Interest:

- a) The M/s Trillium Information Security System shall hold the Bank's interests paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their own corporate interests.

11. Ensuring Access to SBP

M/s Trillium Information Security System and SINDH BANK will ensure that the State Bank of Pakistan is provided necessary access to the documentation and records in relation to the outsourced activities and right to conduct on-site to M/s Trillium Information Security System if required.

12. Anti- Money Laundering Requirement:

M/S TRILLIUM INFORMATION SECURITY SYSTEM acknowledge that they do not violate any statutory/prudential requirement on anti money laundering or record keeping procedure as per existing laws/rules and regulations of locals as well as foreign jurisdiction.

13. TERMINATION

SINDH BANK shall have the right to terminate this Agreement at any time if M/S TRILLIUM INFORMATION SECURITY SYSTEM shall default in the performance of its obligations or non compliance with any provision of this agreement hereunder; and shall fail to remedy such default (if remediable) during the three-month period following service of a written notice of default M/s Trillium Information Security System.

7/11/2023

14. Modifications and Waiver

All changes to the terms and conditions set forth in this document must be in writing and approved by both M/S TRILLIUM INFORMATION SECURITY SYSTEM and SINDH BANK; any waiver must be in writing and be signed by the party waiving its rights. -

Any failure or delay by either party on exercising any right or remedy will not constitute a waiver.

15. Governing Law Jurisdiction

This Agreement shall in all respects be constructed and be governed in the accordance with the Laws of Pakistan and both the parties i.e. SINDH BANK and M/S TRILLIUM INFORMATION SECURITY SYSTEM, hereby submits to the jurisdiction of the local courts in Karachi in any legal proceedings and as regard any claims or matter relating to this Agreement.

16. Force Majeure

Neither party shall be liable for any failure to perform or observe its obligations under this Agreement, if such failures or delays are caused by acts of God, pandemic, wars, riots, strikes, accident, explosion, fire, shortage of labor or materials, labor disputes, government restrictions, or any other cause beyond its reasonable control. In the event of the occurrence of any of the foregoing, the date of performance shall be deferred for a period of time equal to the time lost by reason of the delay. The affected party shall notify the other in writing of such events or circumstances promptly upon their occurrence.

17. Settlement of Disputes:

- The Parties agree that the avoidance or early resolution of disputes is crucial for a smooth execution of the Agreement and the success of the assignment. The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with the Agreement or its interpretation.
- If Parties fail to amicably settle any dispute arising out of or in connection with the Agreement within (10) days of commencement of such informal negotiations, the dispute shall first referred to Grievance Committee of the bank thereafter if not resolved be referred to arbitration of two arbitrators, one to be appointed by each party, in accordance with the Arbitration Act, 1940. Venue of arbitration shall be Karachi, Pakistan and proceedings of arbitration shall be conducted in English.

18. Obligation of the Contractor:

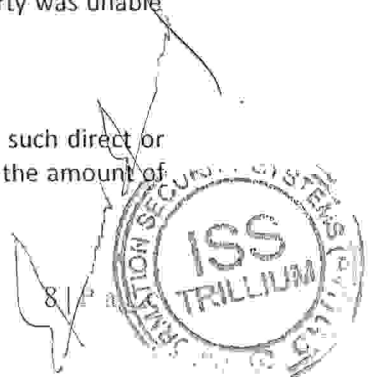
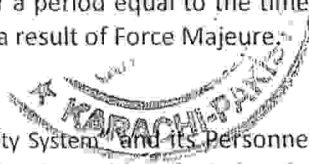
1. The M/S TRILLIUM INFORMATION SECURITY SYSTEM shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The M/S TRILLIUM INFORMATION SECURITY SYSTEM shall always act, in respect of any matter relating to this Agreement or to the Services, as faithful advisers to the Sindh Bank, and shall at all times support and safeguard the Sindh Bank legitimate interests in any dealing with third Parties.
2. If the obligation of warranty period are not met or delayed, the repair etc. requirement on this account will be carried out by the Sindh Bank & the billed amount will be deducted from the performance security/ upcoming payment due to M/s Trillium Information Security System. Risk & subsequent cost to this effect if any will be liability of the "M/s Trillium Information Security System" and any subsequent expenses on the equipment will also be borne by the M/s Trillium Information Security System.

19. Extension of Time:

- Any period within which Party shall, pursuant to this agreement, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

20. Taxes and Duties

The "M/s Trillium Information Security System" and its Personnel shall be liable to pay such direct or indirect taxes duties, fees, and other impositions levied under the Applicable Laws, the amount of which deemed to have been included in Contract Price.



21. Support Escalation Matrix:

For timely addressing of complaints given support escalation matrix will be utilized/followed: -


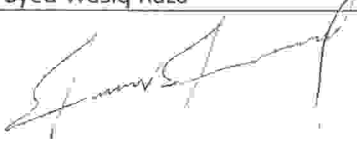

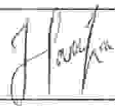
LEVEL-1	Name/Designation (support staff)	Muhammad Ali Aziz /Team Lead Cyber Security Solutions – Technical
First complain if the call is not resolved "within specified response time" (24 hours)	Landline Phone	051 5524181-2 Ext:112
	Email	muhammad.ali@infosecurity.com.pk
	Cell	03215199054
LEVEL-2	Name/Designation (Regional Head/Manager/GM)	Rehan Ahmad Khan /GM Commercial
Second complain, if the call is attended within "Specified Response Time" and not attended / or the problem still unresolved even after complaining at Level-1 (48 hours)	Landline Phone	051 5524181-2 Ext:114
	Email	rehan.khan@infosecurity.com.pk
	Cell	03085200019
LEVEL-3	Name/Designation (CEO of the firm)	Mahir Mohsin Sheikh /CEO
Third complain, if the call is attended within "Specified Response Time" and not attended /or the problem still unresolved even after complaining at Level-2	Landline Phone	051 5524181-2 051 556761
	Email	mahir@infosecurity.com.pk
	Cell	03085200001

This Agreement shall be binding upon each party to this Agreement, their successors and assigns.

In witness whereof, this has been signed on behalf of the parties hereto the day and year first above written

KARACHI



Sindh Bank Limited		Trillium Information Security Systems (Pvt.) Limited	
Address:	3rd Floor, Federation House, Clifton, Karachi, Pakistan	Address:	10th Floor, AWT Plaza, 5-The Mall, Rawalpindi, Pakistan
Name:	Naeem Muhammad	Name:	Syed Wasiq Raza
Signatures:		Signatures:	
Title:	CISO - SVP	Title:	Senior Account Manager- South
Date:		Date:	2 / 12 / 2020
Witness:		Witness:	
Name:	MAHMUD AHMAD KHAN	Name:	Muhammad Hamza Khan
Signatures:		Signatures:	
Title:	OG - IT / IT DIVISION	Title:	Product Manager- Kaspersky & Rapid7
Date:	4/12/2020	Date:	02 / Dec / 2020



ANNEX A

1 Prices Summary Table		
#	Description	Total Price - PKR (Inclusive of all Taxes)
1	IBM QRadar Software/Licenses - Initial One Year	7,130,117
2	Professional Services - Implementation/Support/Local Training - Initial One Year	1,582,000
3	Hardware as per requirement of Sindh Bank	2,000,000
	Grand Total - Initial One Year	10,712,117
Subsequent Years Cost		
1	2nd Year SLA (Software/Local Support including 1 x Resident Engineer)	2,348,335
2	3rd Year SLA (Software/Local Support including 1 x Resident Engineer)	2,503,058
3	4th Year SLA (Software/Local Support including 1 x Resident Engineer)	2,794,589
4	5th Year SLA (Software/Local Support including 1 x Resident Engineer)	3,118,880

2. Initial Year Prices - Software & Professional Services:

#	Part No.	Software Prices Description	Qty	Unit Price - PKR	Total Price - PKR
1	D1S2 JLL	IBM QRadar Software Node Install License + SW Subscription & Support 12 Months	5	70,197	350,985
2	D1R NCLL	IBM QRadar Software Install License + SW Subscription & Support 12 Months	1	762,606	762,606
3	D1R NXLL	IBM QRadar Event Capacity 1000 Events Per Second License + SW Subscription & Support 12 Months	1	5,196,247	5,196,247
		Software Net Total:			6,309,838
		General Sales Tax (GST 13%):			820,279
		Software Gross Total:			7,130,117
Professional Services - Initial Year					
4	N/A	One Time Implementation at/through Sindh Bank Head Office - Karachi	1	800,000	800,000



5	N/A	Post Implementation Support Services - Includes 1 x Resident Engineer (9 am to 5pm) Monday to Friday except public holidays as announced by Federal/Local Government - at Sindh Bank Head Office - Karachi	1	600,000	600,000
6	N/A	Local Product Training at Sindh Bank Head Office - Karachi for 5 Days - upto 5x Participants (To be conducted by QRadar Certified Resource)	1	Free of Cost	-
			Services Net Total:		1,400,000
			Services Sales Tax (GST 13%):		182,000
			Services Gross Total:		1,582,000
		Grand Total -Initial Year (Inclusive of Taxes)			10,712,117

3 Subsequent Year Prices - 2nd & 3rd Software Renewal/Professional Services:

#	Part No.	Software Prices Description	Qty	Unit Price - PKR	Total Price - PKR
Subsequent Year Pricing - 2nd Year Pricing					
1	EONE GLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months	5	15,443	77,215
2	EON BALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months	1	167,769	167,769
3	EON BGLL	IBM QRadar Event Capacity 1K Events Per Second Annual SW Subscription & Support Renewal 12 Months	1	1,143,189	1,143,189
					1,388,173
Professional Services - 2nd Year					
4	N/A	Post Implementation Support Services - Includes 1 x Resident Engineer (9 am to 5pm) Monday to Friday except public holidays as announced by Federal/Local Government - at Sindh Bank Head Office - Karachi	1	690,000	690,000
			Net Total:		2,078,173
			Services Sales Tax (GST 13%):		270,162
			Services Gross Total:		2,348,335

Qm



Subsequent Year Pricing - 3rd Year Pricing					
1	EONE GLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months	5	16,627	83,135
2	EON BALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months	1	184,525	184,525
3	EON BGLL	IBM QRadar Event Capacity 1K Events Per Second Annual SW Subscription & Support Renewal 12 Months	1	1,257,436	1,257,436
					1,525,096
Professional Services - 3rd Year:					
4	N/A	Post Implementation Support Services - Includes 1 x Resident Engineer (9 am to 5pm) Monday to Friday except public holidays as announced by Federal/Local Government - at Sindh Bank Head Office - Karachi	1	690,000	690,000
			Net Total:		2,215,096
			Services Sales Tax (GST 13%):		287,962
			Services Gross Total:		2,503,058
		Grand Total - 2nd & 3rd Years (Inclusive of Taxes)	4,851,393		

4 Subsequent Year Prices - 4th & 5th Software Renewal/Professional Services:

#	Part No	Software Prices Description	Qty	Unit Price - PKR	Total Price - PKR
Subsequent Year Pricing - 4th Year					
1	EON EGLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months	5	18,686	93,430
2	EON BALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months	1	202,978	202,978
3	EON BGLL	IBM QRadar Event Capacity 1K Events Per Second Annual SW Subscription & Support Renewal 12 Months	1	1,383,179	1,383,179
					1,679,587
Professional Services - 4th Year					
4	N/A	Post Implementation Support Services - Includes 1 x Resident Engineer (9 am to 5pm) Monday to Friday except public holidays as announced by Federal/Local Government - at Sindh Bank Head Office - Karachi	1	793,500	793,500

Signature



			Net Total:	2,473,087
			Services Sales Tax (GST 13%):	321,501
			Services Gross Total:	2,794,589
Subsequent Year Pricing - 5th Year				
1	EON EGLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months	5	20,555
2	EON BALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months	1	223,274
3	EON BGL L	IBM QRadar Event Capacity 1K Events Per Second Annual SW Subscription & Support Renewal 12 Months	1	1,521,497
				1,847,546
Professional Services - 5th Year				
4	N/A	Post Implementation Support Services - Includes 1 x Resident Engineer (9 am to 5pm) Monday to Friday except public holidays as announced by Federal/Local Government - at Sindh Bank Head Office - Karachi	1	912,525
			Services Net Total:	2,760,071
			Services Sales Tax (GST 13%):	358,809
			Services Gross Total:	3,118,880
		Grand Total - 4th & 5th Year (Inclusive of Taxes)	5,913,469	



Signature

Hardware Specifications

Dell PowerEdge R740 Server	Qty
PowerEdge R740/R740Motherboard	1
Chassis with up to 8 x 3.5" SAS/SATA Hard Drives	1
Intel Xeon Silver 4214 2.2G, 12C/24T, 9.6GT/s, 16.5M Cache, Turbo, HT (85W) DDR4 2400	2
16GB RDIMM, 2666MT/s, Dual Rank	4
2.4TB 10K RPM Self-Encrypting SAS 12Gbps 512e 2.5in Hot-plug Hard Drive,3.5in HYB CARR, FIPS140, CK	6
iDRAC9, Express	1
PERC H730P+ RAID Controller	1
Broadcom 57416 Dual Port 10GbE BASE-T Adapter, PCIe Full Height	1
Broadcom 5720 Q Port 1 GDE BASE-T, RNDG	1
Dual, Hot-plug, Redundant Power Supply (1+1), 750W	1
DVD ROM	1
Ready Rails Sliding Rails With Cable Management Arm	1
3Yr Pro support Next Business Day Onsite Service	1



[Handwritten signature]