ISLAMI BANK BANGLADESH LIMITED
OPERATIONS WING, ENGINEERING DIVISION,
PROCUREMENT OF COMPUTER HARDWARE AND ACCESSORIES DEPARTMENT,
HEAD OFFICE, DHAKA – 1000.

Date: 31.03.2019

Based on recommendation of Pre bid meeting held on 24.03.2019 the following amendments has been proposed by the ISRMD, ICTW of IBBL into the tender document to supply, installation and configuration of Security Information and Event Management (SIEM) Solution and Privileged Access Management (PAM) Solution for IBBL:

Sl. No.	Page no. of TD	Existing clause/ Terms in the Tender Document	To Be
01	Page- 12	NexGen SIEM Hardware Appliance with 10,000 EPS (Events Per Second)/MPS (Message Per Second)/GB Log Volume license for 3 years.	NexGen SIEM Hardware Appliance with 10,000 EPS (Events Per Second)/MPS (Message Per Second)/GB Log Volume license for 3 years and**scalableto 30 % additional EPS (total=13000) by increasing the License only.** **Virtual Machine may only be used for redundancy and backup and necessary hardware shall be provided by bidder.**
02	Page– 12	The solution must be able to run as a virtual machine or hardware appliance or on own hardware and in as many instances as needed to address the needs of log storage, analysis and forensics.	The solution must be able to run as a hardware appliance and must be scalable to 30% additional EPS (total=13000) by increasing the License only, to address the needs of log storage, analysis and forensics.
03	Page- 13	The solution shall support ingestion of structured and unstructured data. The solution shall have features so that devices can be grouped, logs can be set in different repositories and labels in search queries can filter which device(s) will be shown on a search.	The solution shall support ingestion of structured and unstructured data/netflow. The solution shall have features so that devices can be grouped, logs can be set in different repositories and labels in search queries can filter which device(s) will be shown on a search.
04	Page- 13	The solution architecture must support High Availability (HA) feature.	The solution architecture must support High Availability (HA) feature. The primary shall be hardware appliance and redundancy may be ensured through hardware or VM. The high availability should cater the full load of the primary appliance. **Note:**The bidder may propose separate offer for high availability solution with existing license (primary license) as per OEM specification.

05	Page- 13	The system must support remediation automation framework enables pre-defined or custom actions to be invoked by Next-Gen SIEM on third-party solution out of the box features. The system should allow users to automate actual remediation and other actions via smart remediation based on multiple-actions per alarm - this will provide 3rd parties integration with workflows.	The system must support remediation automation framework enables pre-defined or custom actions to be invoked by Next-Gen SIEM on third-party solution. The system should allow users to automate actual remediation and other actions via smart remediation based on multiple-actions per alarm - this will provide 3rd parties integration with workflows.
06	Page- 15	The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the City Bank Network as well as optimization from space, power and cooling perspective.	The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of IBBL's Network as well as optimization from space, power and cooling perspective.

Details information regarding the Tender is also available in the Tender notice at Bank's web site: www. islamibankbd.com or in the form of hard copy at the office of the undersigned.

Islami Bank My Bank
AAA Bank

Senior Vice President

Annexure: Queries from Prospective Bidders and ICTW's Reply				
Annexure	**RFP Clause**	**Type**	**Description**	**Reply**
Zara & Zaman				
Annexure I	NexGen Hardware Appliance	Suggestion	This being a relatively small EPS requirement we would suggest using either a virtual server or provide appliance using locally procured hardware. We request you to please modify this point as " solution should be Hardware/ Virtual software based appliance"	10, 000 EPS scalable up to 30 % additional EPS (total=13000) by increasing the License only. *Amendment Proposed*
	High Availability/ Redundancy	Query	Please confirm the number of appliances/ VM installation required	Virtual appliance shall only be used to ensure redundancy and backup. Bidder shall provide the necessary hardware. *Amendment Proposed*
	FIM (File Integrity Monitoring)		Please share the breakdown of 400 devices categories for proper categories of licenses	Desktop = 100; Server=300
			Separate console required or not (Y/N)	
			Number of server	
			Number of Network devices	
			Number of Desktop	
			Number of Database Instances	
			Number of exchange server	
			Number of Active directory server	
			Number of MS IIS	
			Number of VM - ESX	
			Number of VM - Hypervisor	
Annexure II - SIEM	Sizing Queries	Query	Kindly confirm the assets location we need to cover such as DC/DR/Branch etc.,	DC, DR and Branch
		Query	Kindly confirm the asset (device) count to size the collector count & their specification.	Server=25%; Network Device=25%;Desktop=15%; VM ESX= 10%; VM-Hypervisor= 5%; Others= 20%; Detailed list will be provided after signing of NDA before implementation
			Separate console required or not (Y/N)	
			Number of server	
			Number of Network devices	
			Number of Desktop	
			Number of Database Instances	
			Number of exchange server	

			Number of Active directory server	
			Number of MS IIS	
			Number of VM - ESX	
			Number of VM - Hypervisor	
		Query	Kindly confirm if proposed solution has to be in High Availability for all the layers - collector, correlation & Management.	High Availability shall be ensured for all layers.
		Query	Kindly confirm if DR solution would be in active or standby mode.	Active-Standby
		Query	Kindly confirm the EPS benchmark to be followed and expected scalability	10, 000 EPS scalable up to 30 % additional EPS (total=13000) by increasing the License only. *Amendment Proposed*
		Query	Kindly confirm the log retention requirement - Online, Offline.	As per Bangladesh Bank's requirement
	Solution should provide full support for events filtering which should be done at (when dealing with syslog) or agent side if agent is used	Suggestion	Syslog filtering cab be done at log source generation level, so we request to please modify this point as " Filtering of logs should be done at log source level, bidder shall ensure that correct level of logging is enabled at log source.	The feature already exist in the current TD
		Error	on page 15 in 2nd Row the term "city bank" should be changed to "IBBL"	Amendment proposed to the TD
Annexure III - PAM	Sizing Queries	Query	No. of days to retain the session recording	As per Bangladesh Bank's requirement
		Query	No. of concurrent sessions	30
		Query	No. of target systems is mentioned as 300, however how many are managed account's?	30
		Query	Avg No. of hours where an admin is performing activity (typically 8 hours per day)	8 hrs.
		Query	Kindly provide the complete list of target systems with OEM names like Windows, AD, Linux, network devices, Databases etc..in scope that needs to be managed through PIM solution.	Server=25%; Network Device=25%;Desktop=15%; VM ESX= 10%; VM-Hypervisor= 5%; Others= 20%; Detailed list will be provided after signing of NDA before implementation

Contessa				
	Queries	Query	Need to know the no. of devices (#of routers, #of switches, #of servers etc.)	Server=25%; Network Device=25%;Desktop=15%; VM ESX= 10%; VM-Hypervisor= 5%; Others= 20%; Detailed list will be provided after signing of NDA before implementation
		Query	How many DC and DR sites are there in IBBL	1 DC and 1 DR
		Query	Mode of Deployment of SIEM and PAM, Will it be Active/Active of Active/Standby?	Active-Standby
		Query	Is joint venture allowed? Can we participate along with another local vendor to share both of our capability and experience?	Ed will take decision regarding the matter.
			For Virtual appliance based solution IBBL will provide the Virtual Machine with necessary requirements like CPU, Memory and Storage.	Virtual appliance shall only be used to ensure redundancy and backup. Bidder shall provide the necessary hardware. Amendment Proposed
Techniche				
	Queries	Queries	Is 10,000 EPS Peck or Avarage EPS?	10, 000 EPS scalable up to 30 % additional EPS (total=13000) by increasing the License only. *Amendment Proposed*
			What are the number of localtions this SIEM will be installed ?	DC and DR
			Total Device list location wise	Server=25%; Network Device=25%;Desktop=15%; VM ESX= 10%; VM-Hypervisor= 5%; Others= 20%; Detailed list will be provided after signing of NDA before implementation.
			What is the EPS/Count/Device detail for DC and DR	10, 000 EPS scalable up to 30 % additional EPS (total=13000) by increasing the License only. *Amendment Proposed*
NHQ				
			Solution must deploy in Decentralize a multilayer Fashion	OEM specified deployment in line with IBBL's infrastructure and policies.
			Current solution should cater 10,000 EPS but must be able to address 20,000 EPS by increasing the License only	10, 000 EPS scalable up to 30 % additional EPS (total=13000) by increasing the License only. *Amendment Proposed*

			The solution must provide a unified view and correlate at real time across both packet data, logs, UEBA analysis and Endpoint detection and response solution within a single analyst console/user interface. The query must return with both network traffic and threat indicators associated to the subject (minimally IP Address, Hostname, Username, Detected threat indicators) in the same investigation view.	Bidders shall follow the compliance features already mentioned in the TD and additional features of offered solution shall be submitted with technical document.
			The solution must support dynamic editing of logs parsers, add custom log parsers and update log parser rules via the solution's user interface	Bidders shall follow the compliance features already mentioned in the TD and additional features of offered solution shall be submitted with technical document.
			The solution must support session reconstruction in the following view: a. Details b. Text c. HEX d. Packets e. Web f. Mail g. IM	Bidders shall follow the compliance features already mentioned in the TD and additional features of offered solution shall be submitted with technical document.
			The solution must provide out of the box SSL decryption capabilities for incoming or lateral network traffic	Bidders shall follow the compliance features already mentioned in the TD and additional features of offered solution shall be submitted with technical document.
			The solution must support ability to decode base64 encoded network traffic	Bidders shall follow the compliance features already mentioned in the TD and additional features of offered solution shall be submitted with technical document.
			The solution shall support ingestion of structured and unstructured log and NetFlow data . The solution shall have features so that devices can be grouped, and should support devices priorities to get threat visibility, logs can be set in different repositories and labels in search queries can filter which device(s) will be shown on a search	Amendment proposed to the TD.

			The implementation/delivery shall provide customized dashboard to help SOC analysts: Dashboard to enhance visibility and assist in analyzing different steps used in a cyber attack based on the following methodology: • Recon • Weaponization • Delivery • Exploitation • Installation • Command and Control (C&C) • Action 1. Unassigned incidents 2. Number of late incidents and representation in percentage 3. Number of new incidents and percentage increase/decrease based on previous timeframe 4. Return of investment to measure efficacy 5. Show total number of incidents segregated by incident types 6. Efficiency metrics: MTTR, Top performing analysts, Investment saved through automation"	Bidders shall follow the compliance features already mentioned in the TD.

			The system must support remediation automation framework enables pre-defined or custom actions to be invoked by Next Gen SIEM on third-party solution out of the box features. The system should allow users to automate actual remediation and other actions via smart remediation based on multiple-actions per alarm - this will provide 3rd parties integration with workflows. 1. Automate processes in data center, regardless of hardware or platform. 2. Standardize best practices to improve operational efficiency 3. Connect systems from different vendors without having to know how to use scripting and programming languages 4. Collaborative investigation and ChatOps powered war room 5. Support more than 150 partner integration for automated actions 6. Should have at last 400 automation scripts invoked for automation tasks 7. On demand logical expressions for automation supported in CLI (Meaning, on the UI, type an action/automation to be executed) 8. Bi-directional partner integration with both push and pull capabilities (Not just a 1-way integration with partner solution but 2-way for information transfer) 9. Evidence board for each incident stores key artifacts for current and future analysis	Amendment proposed to the TD.

			Use Cases Include: • Endpoint Quarantine: Identify the network port where a suspicious device is located and disable the port/device. • Suspend Users: If an account compromise is suspected, halt a user's account access— no matter what device they use. • Suspend Network Access: If data exfiltration is occurring, the incident response team can kill the connection by updating the access control list used by corporate firewalls. Also Automate and work with following solutions: Active Directory Authentication Active Directory Query Check Point Firewall VMWare vCenter Server F5 Networks McAfee Active Response McAfee Advanced Threat Defense McAfee DAM McAfee ePO McAfee ESM McAfee NSM McAfee Threat Intelligence Exchange Microsoft SQL Server MySQL Palo Alto Autofocus Palo Alto Panorama Palo Alto Wildfire PostgreSQL Nessus Qualys Rapid7 Nexpose Virus Total	Bidders shall follow the compliance features already mentioned in the TD and additional features of offered solution shall be submitted with technical document.